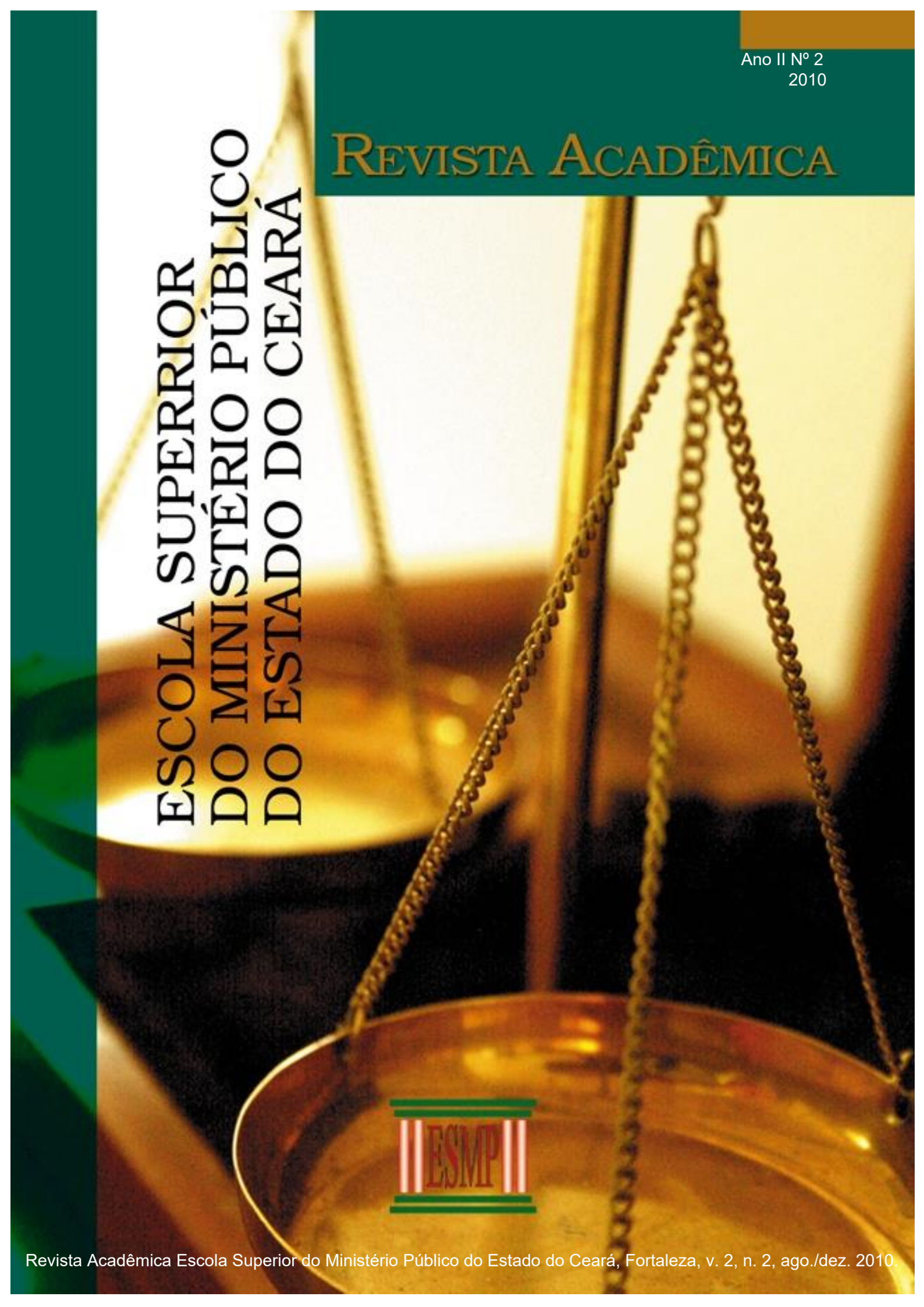
Ano II Nº 2
2010

REVISTA ACADÊMICA

ESCOLA SUPERIOR
DO MINISTÉRIO PÚBLICO
DO ESTADO DO CEARÁ



Revista Acadêmica Escola Superior do Ministério Público do Estado do Ceará, Fortaleza, v. 2, n. 2, ago./dez. 2010.

DEFICIÊNCIAS DA LEGISLAÇÃO PENAL BRASILEIRA FRENTE AOS CRIMES CIBERNÉTICOS

Claudia Lucio de Medeiros*

RESUMO

A utilização cada vez maior de novas aplicações tecnológicas, culminando com a chamada "revolução digital", contribuiu para o avanço da sociedade. Atrelado a esse contexto, entretanto, surgem usuários que utilizam tais inovações, mais especificamente a Internet, para praticar atos ilícitos, seja criando novas modalidades de crimes, seja criando novas formas de praticar crimes já tipificados na legislação penal brasileira, passando-se, com isso, a exigir soluções que o Direito não estava preparado para resolver. Este artigo apresenta um estudo sobre o impacto da tecnologia nas relações jurídicas, especialmente no âmbito do Direito Penal, além de apresentar o tratamento atualmente dado pela legislação penal brasileira aos chamados '*crimes cibernéticos'*. A metodologia utilizada deu-se por meio de um levantamento da legislação vigente e a verificação de sua eficácia ao se iniciar uma investigação criminal do tipo, bem como por meio de comparação da legislação nacional com o ordenamento jurídico de outros países. Através dos resultados, infere-se que o Brasil não apresenta uma legislação específica referente a essas modalidades de crimes, evidenciando a necessidade urgente de regulamentação definitiva dos novos tipos penais, com o intuito de evitar que tais práticas delitivas permaneçam impunes e prossigam acarretando atos lesivos à sociedade.

Palavras-chave: Crimes Cibernéticos. Legislação Brasileira. Impunidade.

1 INTRODUÇÃO

A utilização cada vez maior da tecnologia e os benefícios proporcionados pela chamada *'revolução digital'* são de fundamental importância para a evolução da sociedade. Os modernos sistemas computacionais e o aprimoramento das aplicações tecnológicas em vigor vão sendo lançados no mercado sempre na ânsia

* Servidora do Ministério Público do Estado do Ceará.
Graduada em Ciências da Computação
Universidade Estadual do Ceará
E-mail: cldmedeiros@yahoo.com.br

de melhorar e facilitar a forma de nos comunicarmos, permitindo, inclusive, que diversos países, como é o caso do Brasil, pudessem ser integrados ao mundo globalizado sob diversos aspectos.

Segundo Thiago Rosa (2007, p.3), dentre essas mudanças que ocorrem devido ao crescimento desenfreado de novas tecnologias, podemos perceber o surgimento de novos métodos de interação entre os indivíduos. Novas formas de se relacionar, entretanto, criam também novos problemas, tendo em vista o surgimento de situações que ainda não possuem previsão legal específica.

Atrelado a isso, tal contexto de inovação tecnológica igualmente propiciou o surgimento de novas modalidades de crimes, bem como a expansão de novos métodos de praticar crimes já tipificados na legislação vigente. A partir daí, os conhecimentos tecnológicos inovadores passaram a ser utilizados não apenas para beneficiar a sociedade, mas também tornaram-se perigosas ferramentas para a prática de condutas ilícitas e lesivas a diversos bens jurídicos.

O Código Penal Brasileiro foi elaborado em 1940, época em que os legisladores tipificaram de forma bem definida, diversos tipos de crimes. Desde então, várias mudanças foram ocorrendo na sociedade, principalmente no tocante ao aspecto tecnológico, como já se disse, e mais especificamente, em relação à Informática, que teve uma expansão desenfreada, a partir dos anos 80.

O surgimento da Informática, segundo Silva (2003), ocorreu no meio social de forma bastante rápida, passando-se a exigir, com a mesma rapidez, soluções que o Direito não estava preparado para resolver.

Percebemos, com isso, que tais mudanças provocadas pela informatização generalizada, acabaram não sendo acompanhadas pela legislação pátria, obrigando os aplicadores da lei, na medida do possível, a enquadrar os novos tipos de condutas lesivas nos tipos penais já existentes.

Desta forma, com a utilização inapropriada das técnicas e procedimentos informáticos, presenciamos um relevante impacto da tecnologia nas relações jurídicas, especialmente no âmbito do Direito Penal (DAOUN e LIMA, 2010, p.3).

2 CRIMES CIBERNÉTICOS

Fabrizio Rosa (2005) esclarece que existem os delitos comuns, que já se encontram previstos no Código Penal Brasileiro; crimes comuns praticados com o auxílio do computador, que igualmente se enquadram em condutas já descritas; e por fim, determinadas condutas que também necessitam da utilização do computador para alcançar o resultado desejado, mas que ainda não se encontram tipificadas na legislação. Estas últimas podem ser consideradas como os “crimes de informática” cuja caracterização necessita de legislação específica, tendo em vista não se enquadrarem na legislação penal pátria.

Segundo Gouveia (2007), dentre algumas destas condutas ainda não tipificadas, encontramos os vírus de computador, as invasões, a destruição de dados, etc. Outros delitos clássicos que vêm sendo praticados no mundo virtual - como o estelionato em todas as suas formas, a pornografia infantil, a racismo, dentre outros – igualmente seguem causando atos lesivos e prejuízos reais às pessoas. Neste último caso, os crimes já se encontram devidamente inseridos e tipificados na legislação pátria, praticados porém pelo meio informático, e a inovação consiste apenas no *modus operandi* do cometimento do crime.

Com fulcro no art. 5º, XXXIX, da CF/88, “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal*”,* temos 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. No caso, determinadas condutas criminosas ocorridas mediante a utilização de sistema informatizado, dispositivo de comunicação ou rede de computadores, igualmente devem estar expressamente definidas em lei.

Destarte, nesse contexto, embora o Poder Judiciário venha punindo os infratores com base nos tipos penais já existentes (passíveis, portanto, de imediata aplicação), vislumbramos a necessidade de se criar uma legislação específica o mais breve possível, pois a tentativa de adaptar tais crimes em leis antigas e ultrapassadas, nem sempre é possível, mostrado-se ineficaz em muitos casos, acabando por gerar impunidade.

> (...) Podemos constatar, portanto, que é imprescindível que o legislador penal elabore normas próprias para coibir tais práticas delitivas, no caso, os chamados “crimes de informática”. Para isso, é necessário, entretanto, identificá-los, diferenciá-los e conceituá-los, propiciando assim leis mais claras e específicas, de forma a alcançarem seu objetivo primordial, que é o de regulamentar o comportamento do ser humano em sua vida cotidiana. (ROSA, T., 2007, p.5)

Destacamos que, no Brasil, não há uma cultura de informática jurídica e de Direito da Informática disseminada na sociedade. Embora existam no país algumas iniciativas, por meio de projetos de lei, no sentido de regulamentais os novos tipos de condutas delitivas, muitas se encontram ainda tramitando no Congresso, sem que medidas efetivas tenham sido colocadas em prática. O ordenamento jurídico brasileiro não acompanhou, portanto, as mudanças tecnológicas ocorridas na sociedade, em contraste com a expansão cada vez maior do número de usuários que utilizam o computador e conseqüentemente a Internet.

Segundo pesquisa realizada pelo Ibope/Nielsen, em dezembro de 2009, o Brasil possui 67,5 milhões de ‘*internautas’*, enquanto em setembro do mesmo ano, contabilizava 66,3 milhões. Com isso, o país ocupa o 5º lugar do mundo com o maior número de conexões à Internet. (AGÊNCIA ESTADO, on line)

Por outro lado, as denúncias de crimes praticados pela Internet também seguem aumentando. Segundo estatísticas do Ministério Público Federal (MPF), entre 2007 e 2008 o número de procedimentos abertos na Procuradoria para investigar crimes cibernéticos cresceu 318%. Os dados da Central Nacional de Denúncias de Crimes Cibernéticos mostram que, em 2008, foram denunciadas 91.038 páginas da Internet, das quais 57.574 (63,2%) referentes ao crime de pornografia infantil. (SAFERNET BRASIL, on line)

Podemos constatar, com isso, a necessidade de regulamentar o mais breve possível a legislação penal brasileira, no tocante aos crimes ocorridos no meio virtual, adequando-a ao novo cenário tecnológico que se apresenta.

3 DESAFIOS NO PROCEDIMENTO INVESTIGATÓRIO

No decorrer de uma investigação criminal relacionada a crimes ocorridos no meio cibernético, muitos são os desafios encontrados pelo investigador na busca

de provas materiais. A dinamicidade da Internet, a possibilidade do anonimato e o alcance ilimitado em termos de espaço físico facilitam a eliminação dos indícios necessários para a comprovação do delito.

A identificação do número IP (Internet Protocol) é o passo inicial e mais importante em uma investigação relacionada a crimes cibernéticos. O IP consiste em um “endereço” atribuído exclusivamente a um determinado usuário (no caso, um computador), enquanto este estiver conectado na rede. Neste caso, o provedor de acesso (como por exemplo, *Uol*, *Terra*, *Aol*, etc, que possibilitam a conexão com a Internet) tem a obrigação de fornecer tal informação para tentar localizar e identificar o infrator. Para isto, é necessária a existência de mecanismos legais que possam obrigar os provedores de acesso a armazenar e fornecer as informações de seus usuários por um tempo determinado.

Entretanto, a regulação estatal da atuação destes provedores de acesso ainda é mínima, dificultando, com isso, as investigações criminais no Brasil, e contribuindo, conseqüentemente, para a impunidade de alguns crimes ocorridos no meio virtual. (BRASIL, M., 2006)

O principal ponto é que a legislação é omissa quanto à obtenção dos dados cadastrais dos usuários nos provedores. Como são dados cadastrais, não deveria ser necessário mandado, ou seja, mediante ordem formalizada pelo juiz. Entretanto, os provedores não fornecem tais informações sigilosas sem um *pedido de quebra de sigilo de dados telemáticos*.

Ademais, os provedores não são obrigados a guardar os registros de acesso quando um determinado indivíduo acessa a Internet. Isso dificulta bastante a persecução penal na busca da infração em crimes por computador, notadamente na Internet.

Além disto, o mecanismo de identificação das máquinas pelo IP permite identificar, em muitos casos, apenas as máquinas, mas não quem provocou o delito. Exemplo de situações em que isso ocorre são os computadores utilizados em *lan-houses*, *cybers-café* ou salas públicas de serviços de Internet, as quais não se têm controle algum sobre quem usa o computador ou com que finalidade o utiliza. Esta situação resulta em um problema a ser considerado no decorrer de uma investigação, urgindo a necessidade de se legislar o tema, no sentido de obrigar, por exemplo, o controle dos usuários que utilizam computadores em tais locais, como,

por exemplo, por meio de um cadastro, com o intuito de se haver um controle maior das pessoas que utilizam os computadores nestes casos.

Outro desafio a ser considerado trata da jurisdição, ou seja, da competência de investigação nos casos em que mais de um País é envolvido no problema. A Internet é uma rede global, sem fronteiras, e cada informação nela contida está acessível a todo o planeta, tornando-se quase impossível impor leis neste espaço. Além disto, determinar os lugares em que o crime ocorreu e gerou resultados, bem como definir autoria e materialidade, são problemas que o investigador deverá estar preparado para contornar.

A regra, neste caso, é atribuir a competência de investigação ao Estado em que ocorreu o fato, bem como aos demais territórios utilizados para a prática material de atos relacionados ao crime. Caso um site de conteúdo irregular, por exemplo, esteja hospedado no exterior, a competência da Justiça brasileira será executável apenas se houver algum vínculo com brasileiros. Se tal site, entretanto, não estiver hospedado em provedores nacionais e nem seja identificada a participação de brasileiros no crime, a competência deverá ser atribuída a outras entidades estrangeiras (BRASIL. M., 2006).

4 LEGISLAÇÃO NACIONAL E INTERNACIONAL

Em resposta ao avanço da criminalidade cibernética e na tentativa de contornar as dificuldades encontradas no decorrer do processo de investigação, diversos esforços foram empreendidos por várias nações, com a celebração de acordos internacionais, no intuito de harmonizar as legislações penais e evitar que as máquinas tradicionais dos Estados viessem a atrapalhar o processo investigatório.

Um exemplo de cooperação internacional foi a “Convenção Sobre o Cibercrime”, firmada pelo Conselho Europeu, em 23 de novembro de 2001, celebrada em Budapeste – Hungria, que teve 43 países como signatários, aberta, porém, à assinatura por todos os países do Globo. Embora o Brasil não tenha aderido a este tratado, pode ser considerado um país em harmonia com suas deliberações. (INFO. ABRIL, 2007)

Segundo Susan este tratado obriga os seus signatários a:

> 1) Elaborar leis materiais que tratem de crimes cibernéticos.
> 2) Assegurar aos aplicadores da lei autoridade suficiente para investigar efetivamente este tipo de crime, incluindo mecanismos de autorização para busca e apreensão de computadores, bem como habilitá-los a ordenar aos provedores de acesso a Internet a preservarem os registros de acesso (logs) de uma conexão que seja objeto de investigação.
> 3) Assegurar cooperação internacional a outros países signatários no combate aos crimes cibernéticos. (SUSAN, 2007, p.14-15)

A Convenção de Budapeste facilita, com isso, a punição dos "infratores virtuais", mesmo que cada país tenha sua própria legislação e soberania. Ainda que um crime tenha repercussão em mais de um país, com o auxílio mútuo entre as partes envolvidas, todas poderão proceder as devidas investigações e, caso necessário, efetuar a prisão do infrator. (NETO, 2009)

Como exemplo de legislações de alguns países, referente aos crimes de informática em geral, podemos destacar:

> **Argentina** - projeto de lei sobre crimes informáticos, tratando do acesso ilegítimo a dados, dano informático e fraude informática, entre outros tipos; arts. 183 e 184 do código penal; Decreto 165/94, relacionado ao software; Lei 11.723, direito intelectual.
> **Alemanha** - código penal, seção 202 a, seção 2; seção 303 a, seção 303b; Lei contra criminalidade econômica de 15/05/86.
> **Brasil** - nenhuma legislação penal específica; projeto de lei 84/99, da câmara dos deputados, dispõe acerca dos crimes cometidos na área de informática, suas penalidades e outras providências; Lei 9.609, de 19/02/98: lei sobre propriedade intelectual de programa de computador; Lei 9.610, de 19/02/98: lei de direitos autorais; Lei 9.800, de 26/05/99 – sistema de transmissão de dados e imagens via fax ou similar. Código penal. Estatuto da Criança e do Adolescente.
> **Canadá** - código criminal, seção 183, seção 242.2, seção 326, seção 342, seção 342.1, seção 430. (1.1), seção 487.
> **Espanha** - novo código penal, aprovado pela lei orgânica 10/1995 de 23/11/95, traz vários artigos intimamente relacionados com os crimes da informática. Ex. arts. 197 a 201, arts. 211/ 212, art. 248, arts. 255/256, art. 279, art.278, art. 400, art. 536.
> **Estados Unidos** - ato federal de abuso do computador (18 usc. sec. 1030), que modificou o ato de fraude e abuso do computador de 1986, Ato de decência de comunicações de 1995, Ato de espionagem econômico de 1996, Seção 502 do código penal relativo aos crimes da informática, Nos E.U. A, os estados têm independência para legislar sobre o assunto.
> **França** - novo código penal, seção 202 a, seção 303 a, seçã0 303 b; Projeto de lei relativo a criminalidade informática. Lei 88-19 de 05/01/88 sobre fraude informática.
> **Italia** - Código penal, art. 491, art. 615, art.616, art.617, art. 621, art. 623, art.635. Lei 547 de 23/12/93 - modifica e integra norma ao código penal e ao código de processo penal em tema de criminalidade informática. Lei 675 de 31/12/96, sobre a tutela da privacidade.

> **Japão** - tem legislação penal relacionada a crime de computadores. (ARAÚJO, 2009, p.33)

No Brasil, iniciativas ainda tímidas apontam a intenção do legislador brasileiro em adaptar o sistema jurídico ao novo contexto tecnológico, porém a legislação vigente não é suficiente e muitos projetos relevantes encontram-se ainda tramitando há anos no Congresso Nacional.

Por outro lado, também não é correto afirmar a ausência total de regulamentação em nosso país, no que tange à criminalidade informática. Muitas condutas delituosas podem ser enquadradas nos tipos penais já caracterizados em nosso ordenamento jurídico. Na ausência de uma legislação específica, o infrator deverá ser julgado dentro do próprio Código Penal, mantendo-se as devidas diferenças.

Segundo Neto,

> Algumas medidas emergenciais foram adotadas, entretanto, com o intuito de combater algumas dessas condutas delituosas. Um dos principais exemplos é o caso da pornografia infantil. Até o final de 2008, com a reforma do Estatuto da Criança e do Adolescente (ECA), não era considerado crime aquele que armazenava conteúdo digital de teor erótico / pornográfico, envolvendo crianças e (ou) adolescentes. (NETO, 2009, p.73)

Desta forma, o ECA dispôs em seu art. 241-B que:

> Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008), incorre em crime com pena de reclusão de 1 (um) a 4 (quatro) anos, além de multa.

Além disto, com a alteração legislativa, o art. 241 do ECA passou a prever expressamente o crime de publicação e divulgação por qualquer meio de comunicação, inclusive pela Internet, de fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente.

A legislação brasileira em vigor já tipifica alguns dos crimes identificados pela Convenção de Budapeste, como no caso da pedofilia, bem como trata de outros já inseridos no Código Penal. A tabela abaixo resume alguns delitos que devem ser tratados pela legislação penal de cada Estado signatário, segundo a Convenção, com a sua correspondência na legislação brasileira:

Tabela 1: As leis brasileiras e a Convenção de Budapeste (CP – Código Penal)

Recomendação da Convenção	Artigos das leis ou códigos
1. Do acesso ilegal ou não autorizado a sistemas informatizados	154-A e 155 § 4º, V do CP
2. Da interferência não autorizada sobre os dados armazenados	154-D, 163-A e 171-A do CP
3. Da falsificação em sistemas informatizados	163-A, 171-A, 298 e 298-A do CP
4. Da quebra da integridade das informações	154-B do CP
5. Das fraudes em sistemas informatizados com ou sem ganho econômico	163-A e 171-A do CP
6. Da pornografia infantil ou pedofilía	241 da Lei 8.069, de 1990, Estatuto da Criança e do Adolescente (ECA), alterado pela Lei 10.764, de 2003
7. Da quebra dos direitos de autor	Lei 9.609, de 1998, (a Lei do Software), da Lei 9.610 de 1998, (a Lei do Direito Autoral) e da Lei 10.695 de 2003, (a Lei Contra a Pirataria)
8. Das tentativas ou ajudas a condutas criminosas	154-A § 1º do CP

Fonte: (INFO. ABRIL, 2007)

Como já se disse, existem no Brasil diversos projetos de lei tramitando no Congresso, com o intuito de regulamentar o ambiente virtual. Dentre vários exemplos, podemos destacar a Lei de Crimes Cibernéticos, de autoria do senador Eduardo Azeredo, que igualmente se encontra em fase de tramitação legislativa.

Este projeto de Lei, segundo Medeiros (2009), foi inicialmente proposto no Senado Federal (PLS 76 de 2000) e ficou popularmente conhecido como Lei Azeredo, tendo como principal objetivo alterar várias leis a fim de que possam tipificar como crimes, diversas condutas ilícitas praticadas por intermédio de

sistemas informatizados, condutas estas que passariam a serem tratadas como crimes cibernéticos. Tal projeto, contudo, gerou polêmica e veio a sofrer fortes críticas.

Ainda de acordo com o mesmo autor, após vários anos de tramitação, o PLS 76, juntamente com outros dois projetos de lei (Projeto do Senado 137 de 2000 e Projeto da Câmara 89 de 2003, que igualmente tratam de crimes cibernéticos), vieram a ser substituídos por uma redação definitiva, aprovada em 2008 pelo Senado Federal, encontrando-se no momento em fase de espera de aprovação pela Câmara dos Deputados. Caso aprovado, tal texto deverá ser sancionado pelo Presidente da República e em seguida publicado, tornando-se, por fim, lei.

5 CONSIDERAÇÕES FINAIS

Não há dúvidas acerca dos benefícios ocasionados pela chamada revolução digital, permitindo que diversos países, como é o caso do Brasil, pudesse se integrar ao mundo globalizado sob diversos aspectos. Atrelado a isso, entretanto, a expansão desenfreada de novas tecnologias, e mais especificamente da Internet, igualmente propiciou o surgimento de novas modalidades de crimes, bem como a expansão de novos métodos de praticar crimes já tipificados na legislação pátria.

Embora boa parte desses delitos praticados no chamado “ambiente virtual” já estejam devidamente tutelados pela legislação brasileira, onde é possível aplicar a legislação em vigor, no que for pertinente, nem sempre é possível enquadrar esses crimes em leis antigas e ultrapassadas, apresentando-se ineficaz em muitos casos, acabando por gerar impunidade. A aprovação de leis específicas sobre o tema, bem como a reformulação das leis já existentes, permitirá aos aplicadores da lei instrumentos facilitadores para a efetivação da Justiça, mediante a responsabilização adequada e eficaz dos infratores.

Além disto, assegurar mecanismos cada vez mais eficientes de controle e segurança são tarefas igualmente fundamentais, para que a sociedade possa usufruir dos benefícios e da praticidade que a tecnologia traz consigo.

No Brasil, ainda não há uma cultura de informática jurídica e de Direito da Informática disseminada na sociedade. Embora existam no país algumas iniciativas

por meio de projetos de lei, no sentido de regulamentais os novos tipos de condutas delitivas, muitas se encontram ainda tramitando no Congresso, sem que medidas efetivas tenham sido colocadas em prática. Desta forma, é necessária a regulamentação definitiva dos novos tipos penais, para evitar que tais práticas delitivas permaneçam impunes e prossigam acarretando atos lesivos à sociedade.

Por fim, não devemos esquecer que, de uma forma geral, o Direito é uma ciência altamente dinâmica que deve acompanhar as mudanças vividas pela sociedade, adequando-se ao novo contexto que se apresenta, no caso, o do mundo virtual e o da sociedade da informação.

DEFICIENCIES OF THE BRAZILIAN CRIMINAL LEGISLATION FRONT THE CYBERCRIMES

ABSTRACT

The increasing use of new technological applications, culminating with the call “digital revolution”, contributed for the advance of the society. Together to this context, however, appears users who use such innovations, more specifically the Internet, to practise torts, either creating new modalities of crimes, either creating new forms to practise tipificados crimes already in the Brazilian criminal legislation, transferring themselves, with this, to demand solutions that the Right was not prepared to decide. This article presents a study on the impact of the technology in the legal relationships, especially in the scope of the Criminal law, beyond presenting the treatment currently given by the Brazilian criminal legislation to the calls “Cybercrimes”. The used methodology gave by means of a survey of the current law and the verification of its effectiveness to if initiating a criminal inquiry of the type, as well as by means of comparison of the national legislation with the legal system of other countries. Through the results, the urgent necessity of definitive regulation of the new criminal types is inferred that Brazil does not present a referring specific legislation to these modalities of crimes, evidencing, with intention to prevent that such practical criminal remain unpunished and continue causing harmful acts to the society.

Key-Words: Cybercrimes. Brazilian Legislation. Unpunished

REFERÊNCIAS

AGÊNCIA ESTADO: **Brasil ocupa quinta posição em mercado de celulares e internet, diz ONU.** Notícia disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL1352191-6174,00.html> em 23/10/2009. Acesso em 08 jun.2010.

ARAÚJO, Carlos Guido de. **Aspectos Nacionais e Internacionais dos Crimes de Informática**. Recife: Sociedade Pernambucana de Cultura e Ensino. Faculdade de Ciências Humanas de Pernambuco, 2009. Disponível em: <http://www.jurisway.org.br/v2/dhall.asp?id_dh=3308>. Acesso em: 08 jun.2010.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado, 2009.

BRASIL. Lei 8.069 de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. **Diário Oficial [da] República Federativa do Brasil.** Brasília, DF: Congresso Nacional, 2010.

BRASIL. Ministério Público Federal. Procuradoria da República do Estado de SP. **Crimes Cibernéticos:** manual prático de investigação. São Paulo, 2006. Disponível em: <http://www.mpdft.gov.br/portal/pdf/unidades/promotorias/pdij/TAC/Manual_de_Crimes_de__Inform%C3%A1tica_-_vers%C3%A3o_final2.pdf> Acesso em: 05 jun. 2010.

DAOUN, Alexandre Jean; LIMA, Gisele Truzzi. **Crimes Informáticos:** O Direito Penal na Era da Informação. Disponível em:<http://www.truzzi.com.br/pdf/artigo-crimes-informativos-gisele-truzzi-alexandre-daoun.pdf> Acesso em: 03 jun. 2010.

GOUVEIA, Flávia. Tecnologia a serviço do crime. **Ciência e Cultura**, vol.59, n.1, São Paulo Jan./Mar. 2007 Disponível em: <http://cienciaecultura.bvs.br/scielo.php?pid=S0009-67252007000100003&script=sci_arttext >. Acesso em: 08 jun.2010.

MEDEIROS, Nubielson. **Crimes Cibernéticos e a Segurança na Internet.** Uberlândia/MG: Faculdade de Ciências Aplicadas de Minas Gerais, 2009. 45p.

NETO, Pedro Américo de Souza. **Crimes de Informática.** [S.l]: Universidade do Vale do Itajaí, 2009. 92p.

REVISTA INFO. **Resenha didática - Tipificação e punição dos crimes de informática:** 1 PLS 76/2000 (PLC 89 de 2003 e PLS 137 de 2000). Abr. 2007. Notícia disponível em: <http://info.abril.com.br/aberto/infonews/052007/23052007-resenha1.pdf> Acesso em: 02 jun. 2010

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

ROSA, Thiago Santos. **Projeto de Monografia Científica:** A Diferença entre os crimes de Informática e Crimes Comuns cometidos Via Internet. Bebedouro, 2007. Disponível em: <http://www.fafibe.br/revistasonline/arquivos/revistajuridicafafibe/sumario/5/14042010174132.pdf> Acesso em: 08 jun.2010.

SAFERNET BRASIL: **Denúncias de Crimes pela Internet crescem**. 23/02/2009. Notícia disponível em: <http://amorordemeprogresso.blogspot.com/2009/02/safernet-recebeu-91-mil-denuncias-em.html> Acesso em: 30 mai. 2010.

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

SUSAN, N. Herman. **Os Desafios do Crime Cibernético**. REDHCP – Revista Eletrônica de Direitos Humanos e Política Criminal, Porto Alegre, nº 1, p.14-15, nov. 2007.

TOURINHO, Juliana Gama dos Santos. et al. **Crimes Informáticos**. Disponível em: <http://www.frb.br/ciente/2006.1/ADM/ADM.TOURINHO.F2.pdf> Acesso em: 05 jun. 2010.