Revista de Direito, Governança e Novas Tecnologias

Organização Comitê Científico
Double Blind Review pelo SEER/OJS
Recebido em: 03.12.2017
Aprovado em: 30.12.2017

BREVE PANORAMA SOBRE A LEGISLAÇÃO APLICADA NOS CRIMES ELETRÔNICOS

Heloísa Augusta Vieira Molitor[1]
Victor Hugo Tejerina Velazquez[2]

Resumo: Este trabalho faz explanação sobre o Marco Civil da Internet, a Lei conhecida como Carolina Dieckmann e a Lei conhecida como Azeredo, ambas contra a criminalidade no ciberespaço os denominados crimes eletrônicos e pretende verificar se há uma adequada política criminal destinada a proteger a sociedade. Basicamente analisaram-se as leis 12.965/14, 12.737/2012 e 12.735/12 sua sanção e aplicabilidade. Pode-se concluir que os crimes praticados na esfera digital, conhecidos como cyber crimes, são tipificados pelo código penal. A metodologia utilizada foi à pesquisa qualitativa, utilizando-se do método de análise de conteúdo.

Palavras-chave: Crime; Internet; Tipificação; Cybercrime; Classificação.

BRIEF OVERVIEW OF LEGISLATION APPLIED IN ELECTRONIC CRIMES

Abstract: This work makes an explanation about the Internet Civil Registry, the Law known as Carolina Dieckmann and the Law known as Azeredo, both against cybercrime so-called electronic crimes and seeks to verify if there is an adequate criminal policy aimed at protecting society. Basically the laws 12,965 / 14, 12,737 / 2012 and 12,735 / 12 were analyzed for their sanction and applicability. It can be concluded that crimes practiced in the digital sphere, known as cyber crimes, are typified by the penal code. The methodology used was qualitative research, using the content analysis method.

Keywords: Crime; Internet; Cybercrime; Typing; Classification.

[1]Advogada. Especialista em Direito e Tecnologia da informação pela POLI - USP e Mestranda em Direito pela Unimep. E-mail: heloavs@ig.com.br.

[2] Advogado. Mestre e Doutor em Direito pela Pontifícia Universidade Católica de São Paulo. Idealizador e fundador de Cadernos de Direito e da Revista Discente Interinstitucional. Professor[1], Fundador e ex-Coordenador do Programa de Pós-Graduação em Direito da UNIMEP. Coordenador do NEDAEPI. tejerina@unimep.br

INTRODUÇÃO

Com a disseminação da internet e o uso de computadores pessoais, a oferta dos mais variados produtos e serviços pela rede mundial de computadores alcança centenas de milhões de pessoas nos mais diversos países em questão de segundos.

Os modelos de negócios das empresas são resultados predominantemente de novas tecnologias - derivadas de inovação, pesquisa e desenvolvimento - que constituem um alto valor agregado na oferta de seus produtos e serviços. Essa presença onipresente das novas tecnologias introduz novas ferramentas de trabalho em um mundo virtual complexo, transformando a forma de interação entre pessoas, empresas e consumidores.

O sociólogo espanhol Manuel Castells, em seu livro "A Galáxia da Internet"[3] - que traz reflexões sobre a internet, negócios e a sociedade - afirma que a internet é, acima de tudo, uma criação cultural. Ademais, que a Internet não é uma simples tecnologia de comunicação, mas o epicentro de muitas áreas de atividade social, econômica e política, que faz parte do cotidiano da maioria da sociedade moderna.

As novas formas de interação em uma rede de computadores sem fronteiras - das quais se incluem a redes sociais tais como *Facebook, Twitter, Youtube* - se interpenetram com questões de ordem jurídicas, econômicas, sociais e morais, quer sejam por conflitos de leis entre os países, tratados internacionais, questões fiscais e tributárias, a defesa do consumidor no âmbito do comércio eletrônico entre outros.

Essas questões se apresentam diariamente em um mundo virtual globalizado, extremamente dinâmico, e nessa miscelânea virtual nos deparamos com os chamados *crimes eletrônicos*.

Vale frisar que a vulnerabilidade das pessoas e das empresas, fazem com que sejam alvos de hackers.

As breves considerações expostas neste artigo visam expor alguns aspectos relacionados aos crimes praticados na Internet, que aumentam e se diversificam a cada dia proporcionalmente ao crescimento e exploração da rede mundial de computadores.Nesse

[3] CASTELLS, Manuel. **A Galáxia da Interne**t: reflexões sobre a Internet, os negócios e a sociedade. Tradução. Maria Luiza X. de A. Borges. Rio de Janeiro: Editora Zahar, 2003. 244 p. (original: La Galaxia internet. Reflexiones sobre Internet, empresa y sociedad. Madrid: Areté. 2001.). Veja também: www.edrev.info/reviews/revp49.pdf: acesso em 09/10/2016.

contexto, esse breve estudo não pretende, nem de longe, esgotar a matéria sobre o assunto, mas visa levantar alguns questões relacionadas às ações para se regular os direitos e deveres de milhões de internautas brasileiros, através do Marco Civil da Internet, bem como as dificuldades de se delimitar e tipificar os crimes eletrônicos e as sanções punitivas sem adentrar e punir ações praticadas na rede mundial de computadores que possam ser consideradas de menor potencial ofensivo e que não devem ser abrangidas pela legislação penal.

O artigo também expõe, suscintamente, as principais evoluções no tratamento legislativo dos crimes digitais no Brasil, como as leis ordinárias e esparsas que tratam sobre a tipificação de crimes eletrônicos, bem como algumas considerações sobre a Convenção de Budapeste sobre o *cibercrimes*, ainda não aderida pelo Brasil.

1. CONCEITO CRIMES ELETRÔNICOS

Antes de discutir as leis aplicadas na esfera de crimes eletrônicos, vale trazer a baila concieto sobre crimes eletrônicos, entretanto, foi possível verificar que há diversas terminologias tratando do mesmo assunto, como crimes eletrônicos, crimes virtuais, *cybercrimes*, um conceito exato sobre crimes eletrônicos, crimes digitais, crimes informáticos, entre outros.

Para Emerson Wendt Crimes Cibernéticos são delitos praticados contra ou intermédio de computadores.[4]

Bryant, afirma que crime digital ou de alta tecnologia é aquele no qual foi utilizada a tecnologia para facilitar a atividade criminosa.[5]

Para Manuel Lopes Rocha, este define, como: *"Aqueles que tem por instrumento ou por objeto sistema de processamento eletrônico de dados, apresentando-se em múltiplas modalidades de execução e de lesão de bens jurídicos". (crimes da informática – Remy Gama Filho. Editora: CopyMarket.com, 2000)*

[4] WENT, Emerson. JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos ameaças e procedimentos de investigação. Rio de Janeiro, Brasport, 2012.
[5] BRYANT, Robin P. Investigating Digital Crime. Wiley, 2008.

Dessa forma alguns doutrinadores tentando definir esses crimes de uma forma mais simples divide os crimes cibernéticos em próprios e impróprios.

Os próprios seriam aqueles que exigem ou dependem necessariamente da utilização de ambiente computacional, exemplos destes são a disseminação de vírus, invasão e destruição de bancos de dados.[6]

Crimes impróprios são aqueles em que o ambiente computacional é utilizado como meio para a execução da conduta ilícita, são crimes que podem ser cometidos por diversos meios, exemplo crimes contra honra, ameaça, falsificação, furto, etc.[7]

2 . HISTÓRIA DOS CRIMES VIRTUAIS

Fazendo uma busca histórica sobre o tema verifica-se que os primeiros casos sobre a temática iniciou-se no século XX, quando então, se falava em manipulação de sistemas computacionais.

Já em 1970 o Hacker aparece nos crimes de invasão e furto de software e em 1980 houve explosão com a pirataria, pedofilia, invasão de sistemas, propagação de vírus, etc.

Foi então devido a essa explosão de conduta ilícita que começaram a se preocupar com a segurança nos meios informáticos, vale frisar que no Brasil isso se iniciou com a promulgação da Constituição Federal em 1988.

Atualmente ainda sem a tipificação adequada e com a facilidade de acesso a rede mundial de computadores os crimes tradicionais relacionados à informática, previstos em nossa legislação não são suficientes para classificar os crimes cometidos contra o computador ou por meio dele frente às novas modalidades criminosas que surgiram e que merecem ser definidos em lei especial, para garantia da ordem legal.

[6] VECCHIA, Evandro Della. Perícia Digital da investigação à análise forense. Campinas, Millenium, 2014.
[7] Idem 5

3 . A LEGISLAÇÃO BRASILEIRA E OS CRIMES ELETRÔNICOS

Sobre os delitos praticados pela internet, o cerne da questão é saber se a legislação brasileira, em especial a penal, é suficiente para tratar de crimes eletrônicos.

Nesse contexto, uma significativa parcela de especialistas em Direito Digital defende a aplicação mínima do Direito Penal em delitos praticados na internet, pois acreditam que a legislação penal brasileira atende 95% das demandas virtuais.[8]

Ou seja, que 95% das relações em um ambiente virtual já estão disciplinadas pela nossa lei penal. Dessa forma, o Direito Penal seria o último recurso para tratar os crimes eletrônicos e que só deveria ser aplicado quando todos os demais forem insuficientes.

No caso do crime de ameaça, por exemplo - que antes da era da internet poderia ser consumado por um bilhete ou qualquer papel escrito - hoje acontece por um e-mail ou um *scrap* postado em um site de relacionamento. O crime é tipificado pelo artigo 147 do Código Penal, sendo que a tecnologia só serviu como uma ferramenta para praticar, por meio eletrônico, um crime já tipificado em lei.

Outro crime comumente praticado pelo meio eletrônico é a fraude bancária, que pode ocorrer num simples clique de um mouse. O cavalo de tróia instalado em um computador faz a captação indevida de dados com o fim específico de subtrair o patrimônio de alguém. Tal prática pode ser tipificada como crimes já previstos em nossa lei penal.

Ou seja, os integrantes de uma organização criminosa, que praticam fraude bancária, poderão ser enquadrados, por exemplo, pelos crimes de furto qualificado mediante fraude (art. 155, § 4º, II e IV do CP), formação de quadrilha (capitulado no art. 288 do CP), interceptação telemática ilegal (art. 10 da Lei 9296/96) e violação de sigilo bancário (previsto no art. 10 da Lei Complementar 105/2001).

Uma prática ilícita - que poderia ser classificada dentro do percentual restante de 5% dos crimes eletrônicos ainda não tipificados em nossa legislação - é quando o alvo do criminoso é a supressão de dados de um sistema informatizado como, por exemplo, o sistema SAP.[9]

[8] Revista Visão Jurídica. Editora Escala Ano V. Edição 62. Junho/2011. Entrevista com Alexandre Jean Daoun. Advogado e Mestre em Direito Processual Penal.

[9] SAP é um sistema informatizado que oferece um conjunto de módulos com diversas aplicações de negócio. Os módulos são integrados e contém a maior parte das funcionalidades necessárias às grandes corporações, incluindo manufatura, finanças, vendas e distribuição e recursos humanos.. A configurabilidade do sistema é

Outras condutas que ainda não estão previstas em nosso ordenamento jurídico seriam disseminar código malicioso (vírus) ou invadir domicilio eletrônico.

Dessa forma, conforme a classificação de Rossini[8], existem os "*delitos informáticos puros*" em que o sujeito visa especificamente atingir o sistema de informática em todas as suas formas, e os "*delitos informáticos mistos*" em que o computador é mera ferramenta para a ofensa a outros bens jurídicos que não exclusivamente os do sistema informatizado.

Por outro lado, existe um corrente que defende a aplicação de penas mais severas para crimes praticados pela internet. Sob essa ótica, defendem a necessidade de uma lei específica para tratar crimes eletrônicos ou, pelo menos, o aumento das penas de determinados delitos, pois acreditam que as punições previstas na legislação vigente não são proporcionais ao impacto e prejuízo que a rapidez e amplitude da internet podem causar a uma pessoa.

Nessa assertiva, um dos crimes mais comuns são os crimes contra a honra. Uma pessoa difamada pela internet, através do envio de e-mails anônimos e mensagens ofensivas, pode ter sua imagem e reputação "registrada" de forma indelével na rede mundial de computadores. O causador poderá ser condenado pelo Crime de Difamação, previsto no artigo 139 do Código Penal que prevê pena de detenção de apenas 3 meses a um ano e multa, que viola o princípio da proporcionalidade.

Para o advogado especialista em direito digital Rony Vainzof[10], a tendência é que nosso poder judiciário esteja cada vez mais ciente de que a Internet não é uma terra sem lei e, que, enquanto o Brasil não conta com uma lei específica para crimes digitais, o fechamento de pequenas portas abertas do Código Penal brasileiro e alguns ajustes na legislação, possibilitará que o judiciário tenha mais ferramentas para enquadrar os chamados crimes cibernéticos.

Esses ajustes, que tipificam crimes eletrônicos seriam: criar o tipo penal da invasão do domicílio virtual, somente na forma dolosa; tipificação penal para a disseminação de códigos maliciosos, com intuito de causar dano ou obter vantagem indevida, somente na forma dolosa; aumentar a pena máxima para os crimes contra a honra praticados pelos meios eletrônicos e, da mesma forma, aumentar a pena máxima para o crime de concorrência desleal (art. 195 da Lei

feita por tabelas que administram desde a estrutura corporativa até a política de desconto oferecida aos clientes. Disponível em < http://www.sap.com/brazil/solutions/index.epx>. Acesso em 03/01/2017.

[10] ROSSINI, Augusto Eduardo de Souza. "Brevíssimas Considerações Sobre Delitos Informáticos". Caderno Jurídico. Julho/02. Ano 2.nº 4. ESMP.

9.279/96), se praticados através dos meios eletrônicos.

Nesse diapasão, na opinião do advogado criminalista Marco Aurélio Florêncio Filho[11], a maioria dos ilícitos praticados através das novas tecnologias pode ser enquadrada no código penal vigente, bem como nas leis específicas em vigor. Dessa forma, defende que o advento de lei específica deverá se restringir a poucas condutas ainda não tipificadas, que devem ser muito bem analisadas para se avaliar sua real necessidade.

Por outro lado, muitos defendiam que antes de qualquer alteração no Código Penal ou para se sancionar uma nova lei específica para tipificar crimes eletrônicos era necessário que, previamente, fosse aprovado o Marco Civil da internet que trata dos direitos e garantias dos internautas na esfera de uma legislação civil.

No contexto da sociedade de informação, as aspirações como o acesso à justiça nas relações sociais especialmente em função das novas condutas criminosas, há que considerar os desdobramentos da "informática jurídica" ao tratar de estabelecer tanto os fundamentos da aplicação da informática como os problemas inerentes à informatização do Direito. De modo indireto a informática jurídica considera questões de filosofia jurídica e de teoria do direito[12]. A aparição dos "sistemas expertos" "sistemas baseados em conhecimentos", demonstra que o esquema linear normativo não serve na prática, (Schneider e Schroth)[13], pois, tais desenvolvimentos revolucionam também a consideração da decisão jurídica, porque demonstram, através de estratégias de ensaio [acerto] e erro, que o transcurso da decisão jurídica é diferente do que se pensava.

Especialmente no que concerne à problemática da organização associativa de conhecimentos indica que os processos de decisão transcorrem de forma muito mais complexa do que teoricamente se supunha. A tentativa de apoiar a decisão jurídica na automatização reflete os problemas que carregam os conceitos normativos.

[11] Disponível em <http://www.nic.br/imprensa/clipping/2011/midia542.htm >. Acesso em 10/12/2016.
[12] FLORÊNCIO FILHO, Marco Aurélio. "O Princípio da Intervenção Mínima do Direito Penal e a Criminalidade Informática".
[13] SCHNEIDER Jochen; SCHROTH, Ulrich. *Perspectivas en la aplicación de las normas jurídicas: determinación, argumentación y decisión* in Kaufmann Arthur e Hassemer, Winfried. **El pensamiento jurídico contemporáneo**. Madrid: Debate, 1992, p. 419.

4. PANORAM A SOBRE AS LEIS VIGENTES

4.1 Marco Civil da Internet

O anteprojeto de lei que estabeleceu princípios, garantias, direitos e deveres para o uso da rede mundial de computadores no país, foi construído em conjunto com a sociedade, em processo que ficou conhecido como o Marco Civil da Internet.

No panorama normativo, o anteprojeto representa um primeiro passo no caminho legislativo, sob a premissa de que uma proposta legislativa transversal e convergente possibilitará um posicionamento futuro mais adequado sobre outros importantes temas relacionados à internet que ainda carecem de harmonização, como a proteção de dados pessoais, o comércio eletrônico, os crimes cibernéticos, o direito autoral, a governança da internet e a regulação da atividade dos centros públicos de acesso à internet, entre outros.[14]

Com vistas ao diálogo entre normas jurídicas e a rede mundial de computadores, partiu-se do texto constitucional e o conjunto de recomendações apresentadas pelo Comitê Gestor da Internet no Brasil - CGI.br - no documento "Princípios para a governança e uso da Internet" (Resolução CGI.br/RES/2009/003/P). Para o seu desenvolvimento, o projeto se valeu de inovador debate aberto a todos os internautas.

Uma discussão ampla foi realizada com a sociedade pela própria Internet, entre outubro de 2009 e maio de 2010, por meio de um blog hospedado na plataforma Cultura Digital (uma rede social mantida pelo Ministério da Cultura e pela Rede Nacional de Ensino e Pesquisa - RNP). Esse processo de participação popular resultou em mais de dois mil comentários diretos, incontáveis manifestações sobre o "marco civil" em ferramentas virtuais, como os microblogs Identica e Twitter, além de dezenas de documentos institucionais, oriundos do Brasil e do exterior.

A dinâmica adotada teve como meta usar a própria Internet para, desde já, conferir mais densidade à democracia. Por meio da abertura e da transparência, permitiu-se a franca expressão pública de todos os grupos sociais, por meio de um diálogo civilizado e construtivo.

Em 26/10/2011 foi criada uma Comissão Especial na Câmara dos Deputados para

[14] Todas as considerações feitas até então são as justificativas apensas ao Projeto de Lei nº 2126/2011, conhecida como Marco Civil da Internet, apresentadas por José Eduardo Martins Cardoso, Miriam Aparecida Belchior, Aloizio Mercadante Oliva e Paulo Bernardo Silva.

cuidar desse projeto de Lei e em 23 de abril de 2014 foi sancionada a lei 12.965/2014 denominada como Marco Civil da Internet.

Esta lei é importante, pois traz conceitos em seu artigo 5º do que é internet, terminal, endereço de protocolo de internet, conexão à internet, registro de conexão, registro de acesso entre outros.

Esses conceitos são utilizados para saber quem estava utilizando o endereço de IP no momento do ato ilícito por exemplo, se faz necessário o provedor ter os registros de conexões, com data, hora, fuso horário e afim.

4.2 Lei "Azeredo" – 12.735

Essa Lei ficou assim conhecida pois, o Projeto de Lei nº 84/99, de autoria do Deputado Luiz Piauhylino, sob a ementa original que "Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências".

O Projeto de Lei nº 84/99 englobou as proposições PLS 76/2000, PLS 137/2000 e PLC 89/2003. Houve um Substitutivo do Senado ao Projeto de Lei da Câmara nº 89/2003, de autoria do então Senador Eduardo Azeredo, que foi aprovado pelo Plenário do Senado Federal em 2008. Posteriormente, na Comissão de Constituição e Justiça e de Cidadania, o Deputado Regis de Oliveira acrescentou novo substitutivo modificando a redação de vários artigos.

O projeto substitutivo do senador Eduardo Azeredo agregou num único texto as propostas apresentadas no Projeto de Lei da Câmara dos Deputados 89/2003 e nos Projetos de Lei do Senado Federal 76/2000 e 137/2000. O projeto substitutivo modifica a legislação penal brasileira: Decreto-Lei 2.848/40 (Código Penal); Decreto-Lei nº 1.001/69 (Código Penal Militar) e as Leis Federais nº 7.716/89 e nº 8.069/90 (Estatuto da Criança e do Adolescente) e 10.446/02, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, ou que sejam praticadas contra sistemas informatizados e similares e dá outras providências.

O Projeto ficou conhecido como Lei "Azeredo", por causa de seu principal defensor, e apelidado de "AI5 digital" pela bancada do Partido dos Trabalhadores, projeto acusado de incitar a criação de um estado policial na internet, de censura à livre circulação de informações da ditadura militar e a criminalização em massa, em um momento que não existe uma garantia dos direitos dos internautas, através do Marco Civil na Internet.

O texto final com alterações inclui a supressão de disposições relativas a pedofilia decorrentes de sua obsolescência, uma vez que a Lei nº 11.829 de 25/11/2008 alterou a Lei 8.069/90 - referente ao Estatuto da Criança e do Adolescente - em seus artigos 240/241 e 241-A para "aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet".

Dessa forma houve a supressão do artigo 20 do Substitutivo do Senado Federal ao PL da Câmara nº 89/2003 que trazia alterações no artigo 241 do ECA e a supressão do artigo 5º do PL 84/99, da Câmara dos Deputados, que trazia alterações ao Código Penal, inserindo o art. 218-A sobre "Pornografia Infantil". Essa última, devido ao estágio do Projeto, somente poderá ser suprimido por veto da Presidente da República.

Também foram suprimidas, do Substitutivo do Senado, as expressões "dispositivo de comunicação" e "rede de computadores", que constavam na ementa e nos artigos 1º, 2º, 5º, 6º, 7º, 10, 12, 13, 16, 17, 18 e 21 e nas definições dos incisos I e III do Art. 16, para reduzir o escopo de interpretação judicial para apenas "sistemas informatizados".

Tais supressões tiveram como justificativa ampliar a segurança jurídica e impedir que condutas banais e inofensivas possam se enquadradas nesses tipos penais como, por exemplo, desbloquear um aparelho celular - considerado como "dispositivo de comunicação" de acordo com a definição do próprio projeto - ou um aparelho de DVD para assistir a um filme proveniente do exterior.

Vale frisar que esta lei traz apenas dois pontos que são: a criação de delegacia de policia especializada em crimes informáticos e inclui na legislação crimes de preconceito de raça ou cor para que a publicação seja interrompida. Originalmente o projeto contemplava como crimes condutas tais como acessar um sistema informatizado sem autorização; obter, transferir ou fornecer dados ou informações sem autorização; divulgar ou utilizar de maneira indevida informações e dados pessoais contidos em sistema informatizado, ou, falsificar dados eletrônicos ou documentos públicos; estelionato eletrônico, inserir ou difundir código malicioso seguido de dano, destruir, inutilizar ou deteriorar coisas alheias ou anos eletrônicos pertencentes a terceiros etc.

4.3 Lei Carolina Dieckmann 12.737/2012

A Lei Carolina Dieckmann é oriunda do projeto de Lei n° 2793/2011, apresentado em 29/11/2011 que tipificava criminalmente os delitos cometidos na Internet é de coautoria de deputados da base aliada do governo: Paulo Teixeira, Luiza Erundina, Manuela D´Àvila, João Arruda, Brizola Neto e Emiliano José.

A justificação dos coautores ao Projeto de Lei 2793/2011 é de que se trata de uma proposta alternativa ao Projeto de Lei 84/99 que, em sua redação atual, traz propostas de criminalização demasiadamente abertas e desproporcionais, capazes de ensejar a tipificação criminal de condutas corriqueiras praticadas por grande parte da população na Internet. Contém, também, em um diploma penal matérias - como guarda e acesso a registros de conexão - que deveriam constar de uma regulamentação da Internet que fosse mais abrangente e mais atenta aos direitos e garantias do cidadão. Ademais, que, em seu atual estágio de tramitação, por conta de questões regimentais, o Projeto de Lei 84/99 não pode mais ser emendado ou alterado.

A lei foi conhecida como Carolina Dieckmann, pois em 2012 teve fotos íntimas copiadas do computador da atriz foram postadas na rede.

A lei trata apenas de tipificações penais, não aborda questões relativas a guarda e fornecimento de registros, ou demais obrigações imputáveis a provedores de serviços de internet - questões que encontram lugar mais adequado numa regulamentação civil sobre a matéria.

A legislação buscou equilibrar as penas previstas segundo a gravidade das condutas, hierarquizando, a partir de um tipo principal, os patamares de penas aplicáveis a partir dos resultados danosos obtidos pela prática dos atos tipificados e, obviamente, buscando harmonizar as penas previstas com as já existentes no ordenamento jurídico brasileiro.

Busca, tanto quanto possível, orientar as tipificações a partir de um fim especial de agir, consistente na intenção consciente do agente em praticar determinada modalidade de atividade danosa à terceiro. Reinsere as condutas tipificadas na lógica atual dos bens jurídicos penalmente tutelados pelo ordenamento, evitando a expansão desnecessária da proteção penal para novas searas. Acrescenta como elementos básicos do tipo critérios de verificação - de modo, de meio, de finalidade - para que se verifique a conduta como efetivamente punível, buscando assim mitigar os efeitos indesejados de uma tipificação demasiadamente aberta sobre

condutas sociais corriqueiras.

5. CONVENÇÃO DE BUDAPESTE

A Convenção de Budapeste, conhecida como Convenção sobre o *Cibercrime*, é o primeiro tratado internacional que dispõe sobre os crimes cometidos através da rede mundial de computadores. Proposta pelo Conselho Europeu, em 23 de novembro de 2001, entrou em vigor em 1 de julho de 2004. Em 28 de outubro de 2010 trinta países haviam assinado, ratificado e aderido a Convenção, enquanto dezesseis países haviam assinado, porém sem ratificá-la.

O preâmbulo da Convenção destaca a necessidade de se impedir os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, assegurando a incriminação desses comportamentos e da adoção de poderes suficientes para combater eficazmente essas infrações, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infrações tanto no nível nacional como internacional e estabelecendo disposições para uma cooperação internacional rápida e eficiente.

Apesar do Brasil ainda não ser signatário da Convenção de Budapeste, já foram incorporadas várias de suas disposições na atual redação do Projeto de Lei 84/99 bem como em leis específicas já existentes como a questão da pornografia infantil cuja Lei nº 11.829 2008 alterou a Lei 8.069/90 (ECA) em seus artigos 240/241 e 241-A, para inserir condutas relacionadas à pedofilia na internet.

Temos, também, a Lei nº 10.447/2002 que dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme, para fins do disposto no inciso I do §1º do artigo 144 da Constituição. O artigo 21 do substitutivo da PL 84/99 acrescenta o inciso "V" ao artigo 1º da referida Lei, prevendo a cooperação internacional na investigação de infrações penais de delitos praticados contra ou mediante sistema informatizado quando houver repercussão internacional que exija repressão uniforme. Essas disposições estão em consonância com os artigos 23 e 25 da Convenção de Budapeste que trata dos princípios gerais relativos à cooperação internacional e auxílio mútuo.

A conservação de dados informáticos, incluindo dados relativos ao tráfego, constante no artigo 22 da PL 84/99, é prevista no artigo 16 da Convenção de Budapeste. Ademais, temos

As disposições da Lei 9296/96, que se aplica à interceptação do fluxo de comunicações em sistemas de informática e telemática, que é prevista no artigo 21 da Convenção que dispõe sobre a "interceptação de dados relativos ao conteúdo".

A adesão do Brasil à Convenção de Budapeste ainda está sob análise e discussão sendo que, sob o ponto de vista diplomático, existem restrições a sua adesão sob o argumento de que o Brasil não participou da discussão dos seus termos e não expôs seus objetivos e interesses.

Por outro lado, o acordo é considerado importante para alguns especialistas uma vez que o país ainda não dispõe de legislação especializada no assunto. O procurador da República em São Paulo, Sérgio Suiama é um dos especialistas no tema que defende a adesão do Brasil à Convenção de Budapeste. Conforme entrevista concedida a Revista Consultor Jurídico em 29/05/2008,[15] segundo o procurador a adesão traria algumas vantagens como modelo legislativo homogêneo e a adoção de mecanismos de cooperação mais ágeis que a carta rogatória, por exemplo. Lembrou que foi por causa de uma carta rogatória que o Brasil demorou dois anos para conseguir um endereço IP (Internet Protocol) para localização de um computador.

De acordo com o procurador, o Brasil também carece de conhecimentos técnicos específicos que já estão em andamento em outros países e, por meio da convenção, seria possível um intercâmbio de experiências. Ele lembrou que os provedores de internet do país também têm pouco comprometimento com o combate aos crimes cibernéticos.

Sob a ótica jurídica há necessidade de uma análise para identificar a compatibilização de todos os termos da Convenção com a nossa legislação constitucional e infraconstitucional para que o Brasil não se torne, no futuro, inadimplente com um tratado internacional que não o atenda plenamente.

[15] Reportagem de Maria Fernanda Erdelyi, correspondente da Revista Consultor Jurídico em Brasília. Revista Consultor Jurídico, 29 de maio de 2008. Disponível em <http://www.conjur.com.br/2008-mai-29/itamaraty_ainda_estuda_adesao_convencao_budapeste>.

6. CONCLUSÃO

Em uma rede mundial de computadores sem fronteiras e com o aumento da criminalidade virtual, torna-se imperativo a necessidade de harmonização da legislação internacional bem como se estabelecer os tipos penais específicos e estritamente necessários na legislação brasileira para combater os crimes cibernéticos.

A Convenção de Budapeste já foi ratificada em países que abrigam grandes provedores como o Google nos Estados Unidos.

Mesmo que o Brasil não tenha participado das discussões daquele tratado, aderindo a Convenção de Budapeste poderá ter voz ativa para influenciar rumos futuros que poderão nortear e disciplinar ainda mais as ações delituosas praticadas na internet, que tenham repercussão nacional e internacional.

Sob o ponto de vista da legislação interna, nota-se que o Brasil ainda está engatinhando com a adoção de leis específicas sobre os crimes eletrônicos, em comparação, por exemplo, com a Itália que desde 1993 tratou de incorporar em seu Código Penal os delitos relacionados com os crimes eletrônicos.

Entretanto, é possível notar algum avanço legislativo com o Marco Civil na Internet, Lei Azeredo e Lei Carolina Dieckemann.

Não obstante, nossos profissionais de direito, usando as ferramentas legais já existentes em nosso ordenamento jurídico, estão conseguindo de forma pioneira firmar jurisprudência relacionada ao combate de crimes eletrônicos - tanto na esfera penal como civil

- que, em breve, deverá nortear e balizar o advento de leis específicas sobre a matéria que ainda gera muita discussão, como analisamos nete breve estudo.

Sendo assim, finalizo com uma fala de Liliana Paesani: “se o jurista se recusar a aceitar o computador, que formula um novo modo de pensar, o mundo, que certamente não dispensará a máquina, dispensará o jurista. Será o fim do Estado de Direito e a democracia se transformará facilmente em tecnocracia”.[16]

[16] PAESANI, Liliana M. Ap. Borruso. Direito de Informática. São Paulo, Atlas, 2014.

7. REFERÊNCIAS

BRYANT, Robin P**. Investigating Digital Crime**. Wiley, 2008.

CASTELLS, Manuel. A Galáxia da Internet: reflexões sobre a Internet, os negócios e a sociedade. Tradução. Maria Luiza X. de A. Borges. Rio de Janeiro: Editora Zahar, 2003. 244 p. (original: La Galaxia Internet. Reflexiones sobre Internet, empresa y sociedad. Madrid: Areté. 2001.)

"Comentários e Sugestões sobre o substitutivo do Projeto de Lei de Crimes Eletrônicos (PL n.8499) apresentado pela Comissão de Constituição e Justiça e de Cidadania" Novembro 2010. Disponível em <http://direitorio.fgv.br/node/1238> Acesso em 03/01/2017

COSTA JUNIOR, Paulo José da, Código Penal Comentado. DPJ Editora.– São Paulo. 2005. 8ª Edição .

CRESPO, Marcelo Xavier de Freitas Crespo. "Crimes Digitais". São Paulo. Editora Saraiva. 2011.1ª Edição.

FLORÊNCIO FILHO, Marco Aurélio. "O Princípio da Intervenção Mínima do Direito Penal e a Criminalidade Informática".

Justificação apensa ao Projeto de Lei nº 2126/2011, Marco Civil da Internet, apresentadas por José Eduardo Martins Cardoso, Miriam Aparecida Belchior, Aloizio Mercadante Oliva e Paulo Bernardo Silva.

Justificação apensa ao Projeto de Lei nº 2793/2011, apresentadas pelos seus coautores Paulo Teixeira, Luiza Erundina, Manuela D´Àvila, João Arruda, Brizola Neto e Emiliano José.

PAESANI, Liliana M. Ap. Borruso. **Direito de Informática**. São Paulo, Atlas, 2014
REMY; Gama Filho, Editora: CopyMarket.com, 2000 - *Teoria do Delito*, Editora Revista dos Tribunais. *Suspensão Condicional do Processo Penal*, Editora Revista dos Tribunais.

ROSSINI, Augusto Eduardo de Souza. "Brevíssimas Considerações Sobre Delitos Informáticos". Caderno Jurídico. Julho/02. Ano 2.nº 4. ESMP.

Revista Consultor Jurídico, 29 de maio de 2008. Disponível em <http://www.conjur.com.br/2008-mai29/itamaraty_ainda_estuda_adesao_convencao_budapeste>. Acesso em 18/06/2017

Revista Visão Jurídica. Editora Escala. Edição 62 e 130. Junho/2011e julho/2017.

SCHNEIDER Jochen; SCHROTH, Ulrich. *Perspectivas en la aplicación de las normas jurídicas*: determinación, argumentación y decisión in Kaufmann Arthur e Hassemer,

Sistema SAP. Disponível em < http://www.sap.com/brazil/solutions/index.epx>. Acesso em 03/01/2017

VECCHIA, Evandro Della. **Perícia Digital da investigação à análise forense**. Campinas, Millenium, 2014.

WINFRIED. **El pensamiento jurídico contemporáneo**. Madrid: Debate, 1992.

WENT, Emerson. JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos ameaças e procedimentos de investigação**. Rio de Janeiro, Brasport, 2012.

WIKIPEDIA. A enciclopédia Livre: História da Internet Disponível em: <http://pt.wikipedia.org/wiki/Hist%C3%B3ria_da_Internet>. Acesso em 08 agosto. 2017