# CRIMES CIBERNÉTICOS: ASPECTOS LEGISLATIVOS E IMPLICAÇÕES NA PERSECUÇÃO PENAL COM BASE NAS LEGISLAÇÕES BRASILEIRA E INTERNACIONAL

# CYBERCRIMES: LEGISLATIVE ASPECTS AND IMPLICATIONS IN THE CRIMINAL PROSECUTION BASED ON THE BRAZILIAN AND INTERNATIONAL LEGISLATIONS

Jessica Fagundes Bortot [*]

**Resumo**

Este estudo teve por objetivo analisar brevemente os principais aspectos do fenômeno dos crimes cibernéticos em nosso país. Para tanto, realizou-se uma breve digressão histórica acerca da evolução da Internet e apresentou-se um rol de conceitos acerca dos crimes cibernéticos. Ainda fez-se relevante um estudo comparativo entre a legislação internacional e o ordenamento jurídico brasileiro, destacando a legislação dos Estados Unidos, a Convenção de Budapeste, a Lei Azeredo, a Lei Carolina Dieckmann e a Lei Marco Civil da Internet. Avaliou-se, ainda, o trabalho do Ministério Público de Minas Gerais e os aspectos que dificultam a persecução penal. Destarte, trata-se de um tema atual e de extrema relevância para a seara do Direito Penal.

**Palavras-chave:** Crimes Cibernéticos; Legislação; Persecução Penal; Direito Penal..

**Abstract**

This paper had the purpose of making a brief analysis of the main aspects of the cybercrime phenomenon in our country. In order to do so, a short historical digression was made on the evolution of the Internet and important concepts of cybercrimes were presented. Also, a comparative study was made between the international legislation and the Brazilian legal system, highlighting the United States legislation, the Budapest Convention, the Azeredo Law, the Carolina Dieckmann Law and the Brazilian Internet Civil Law. It was also evaluated the work

[*] Graduada em Direito pela Faculdade Mineira de Direito da Pontifícia Universidade Católica de Minas Gerais.

of the Public Prosecutor's Office of Minas Gerais and the aspects that hinder criminal prosecution. Thus, it is a current topic of extreme relevance to the field of Criminal Law.

**Key-words**: Cybercrimes; Legislation; Criminal Prosecution; Criminal Law.

# 1. INTRODUÇÃO

Hoje, o mundo é considerado predominantemente digital. Não há mais como negar que a Internet faz parte essencial do dia a dia da sociedade, no entanto, não obstante todos os seus benefícios, há também, como custo, a prática crescente de ilícitos no meio digital.

Além do aumento do número de usuários, outro ponto que influi para a grande quantidade de crimes praticados na Internet é a sensação de impunidade que ainda existe. Tal sensação ocorre, uma vez que, devido à ausência de legislação adequada, a determinação da autoria, a competência de julgamento, as provas, as perícias e até mesmo a execução das penas, se mostram prejudicadas e ineficientes.

Ao longo dos anos, vários países têm tentado adaptar suas leis para combater os crimes cibernéticos, com destaque para os Estados Unidos, primeiro país a legislar sobre o assunto, e a Europa, pela elaboração da Convenção sobre o Cibercrime, também conhecida como Convenção de Budapeste.

Enquanto isso, no Brasil, o legislativo carece de insumos no que se refere a esse combate, o que torna o solo nacional um verdadeiro oásis para os criminosos. E além do país não ser signatário da Convenção Europeia sobre o Cibercrime, o mesmo não possui agentes suficientemente capacitados para investigar e periciar os crimes virtuais, o que torna a persecução penal quase impossível.

A ocorrência desse tipo de crime aumenta a cada dia, e ao contrário do que muitas vezes se imagina, as repercussões não são apenas em face do particular. Existem também outras inúmeras consequências, para a economia ou política de um país, que podem levar até mesmo a guerras ou ao terrorismo.

Diante da relevância desse tema, o presente trabalho compromete-se com a análise desse dinâmico ramo do Direito, denominado Direito Digital, e suas repercussões no Direito Penal e Processual Penal Brasileiro.

Para tanto, não só será realizado uma breve análise sobre as legislações nacionais e internacionais que tratam do tema, como também sobre alguns aspectos técnicos da Internet, de forma clara para profissionais do Direito, uma vez que não há como discutir novas regulamentações sobre o mundo cibernético sem compreender seu funcionamento.

Por fim, ao analisar os desafios enfrentados por profissionais da área e pelo Ministério Público, e no caso, o do Estado de Minas Gerais, serão expostas condutas que carecem de tipificação penal adequada no Brasil e quais seriam as possíveis medidas a serem tomadas pelo Brasil em busca de uma maturidade quanto a sua segurança cibernética.

Contudo, importante frisar que o exaurimento da temática neste momento é impossível, visto que é um assunto em constante metamorfose e possui diversas ramificações que vão muito além das discutidas nessa pesquisa.

## 2. DA EVOLUÇÃO TECNOLÓGICA E O DIREITO

Desde os primórdios da humanidade, o interesse em criar e desenvolver instrumentos que fossem capazes de auxiliar o trabalho do homem sempre existiu. Como decorrência disso, em 1830, o primeiro protótipo do computador que conhecemos foi construído, e nos anos 1970, a primeira versão comercial foi lançada.

Desde então, o desenvolvimento do computador acelerou drasticamente, principalmente com o auxílio da Internet, que teve sua origem nos anos 1960, nos Estados Unidos, durante a Guerra Fria, com objetivo de dar suporte aos militares, sendo apenas introduzida para os civis alguns anos depois.

Diante da existência de relevantes dados militares, a rede até então utilizada se tornou extremamente atrativa para espiões, e assim ocorreram, antes mesmo de se tornar pública no final da década de 1980, as primeiras condutas de cunho criminoso através da Internet, atualmente chamadas de Crimes Cibernéticos.[1]

[1] Cumpre destacar que os crimes cometidos com o uso de tecnologia possuem diversas nomenclaturas, como: crimes informáticos, crimes eletrônicos, crimes telemáticos, delitos computacionais, crimes virtuais, crimes digitais, entre outros. Será adotada nessa pesquisa, por entender ser a mais adequada e didática, a nomenclatura "crimes cibernéticos".

Todo o exposto demonstra como a tecnologia tem um desenvolvimento extremamente veloz. Consequentemente, surgem novas relações jurídicas e estas precisam ser reguladas e amparadas pelo Ordenamento Jurídico. O Direito é um reflexo da sociedade, do seu comportamento, estando assim em constante metamorfose. Diante disso, torna-se necessário um dinamismo entre as normas jurídicas e as novas condutas em meio digital, visando sempre a segurança jurídica e social.

É nesse sentido que se verá adiante, quais os tipos de crimes cibernéticos que ainda carecem de tipificação adequada, como o Brasil tem lidado com essas condutas e quais as possíveis alternativas para tornar ideal, a aplicação do Direito.

# 3. DOS CRIMES CIBERNÉTICOS

## 3.1 Conceito

Os crimes cibernéticos são, assim como os crimes comuns, condutas típicas, antijurídicas e culpáveis, porém praticadas contra ou com a utilização dos sistemas da informática.

Para a OECD – *Organization for Economic Cooperation and Development* (Organização para a Cooperação Econômica e Desenvolvimento) da ONU, "crime de computador é qualquer comportamento ilegal, aético, ou não autorizado envolvendo processamento automático de dados e, ou transmissão de dados".

Para Augusto Rossini (2004):

> [...] o conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade. (ROSSINI, 2004, p. 110.).

Já em 1984, María de la Luz Lima, adotou um conceito que se aproxima bastante com os atuais. Segundo ela, delito eletrônico, em sentido amplo, deve ser entendido como qualquer conduta criminógena ou criminal cuja realização haja o emprego da tecnologia como método, meio ou fim, e, em um sentido estrito, qualquer ato ilícito penal em que os computadores, suas técnicas e funções desempenham um papel como método, meio e fim.

### 3.2 Classificação

Embora existam as divergências doutrinárias quanto à classificação dos crimes cibernéticos, o presente trabalho adotará a sistematização defendida por Ivette Senise Ferreira e Vicente Greco Filho, que divide os crimes digitais em crimes próprios e impróprios[2], por ser menos complexa que as demais existentes na doutrina, todavia, mais plausível de ser adotada dada sua particular popularidade acadêmica e social.

Vicente Greco Filho (2000) explica:

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da Internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou.

Sintetizando:

a) Crimes próprios: condutas perpetradas contra um sistema informático, sejam quais forem as motivações do agente;
b) Crimes impróprios: condutas perpetradas contra outros bens jurídicos, por meio de um sistema informático.

Vale comentar que, segundo Ivette Senise Ferreira (2011), sistema de informática ou o computador é um instrumento como tantos outros, tal qual armas de fogo, explosivos, utilizados por criminosos para facilitar o cometimento de um delito. Cabe ao Estado tutelar as novas modalidades e lesões aos diversos bens e interesses que surgiram com a crescente informatização das atividades individuais e coletivas desenvolvidas na sociedade. Essa informatização colocou

[2] Chamo a atenção para essa denominação, a fim de, não se confundir com a classificação já existente no direito penal, que utiliza os termos "próprio" e "impróprio" para classificar os crimes segundo o sujeito ativo.

novos instrumentos nas mãos dos criminosos e propiciou a formação de uma criminalidade específica da informática cujo alcance ainda não foi corretamente avaliado.

Percebe-se que, com o advento da Internet, surgiram condutas ilícitas, além daquelas já previstas no ordenamento jurídico brasileiro, que precisam de regulamentação a fim de não permitir que o ambiente virtual seja acometido pela impunibilidade.

### 3.3 Denominação dos sujeitos ativo e passivo

Muito se fala em *Hackers* como sendo os responsáveis pelos crimes, e embora exista uma série de denominações para identificar os autores das condutas ilícitas cibernéticas, abordar-se-á apenas uma conceituação básica.

Os famosos *Hackers*, são aqueles que normalmente modificam softwares, desenvolvendo novas funcionalidades, encontrando falhas em sistemas para empresas, ajudando a corrigi-las, etc. São então denominados "*White-hats"* (chapéus brancos), por serem aqueles que utilizam todo o seu conhecimento para melhorar a segurança, de forma legal.

Os *Crackers*, por outro lado, são os verdadeiros invasores de computadores e sistemas, sendo até mesmo comparados a terroristas. Conhecidos como "*Black-hats"* (chapéus negros), utilizam o conhecimento da informática com propósitos ilícitos. Eles são o que o senso comum define que o *Hacker* é.

A mesma peculiaridade na denominação não ocorre quanto ao sujeito passivo do delito cibernético, uma vez que, assim como no crime comum, figura o polo passivo dos crimes cibernéticos aquele a quem recaiu a ação ou omissão, seja ele pessoa física ou jurídica, sendo assim, a vítima.

## 4. LEGISLAÇÃO COMPARADA E INTERNACIONAL

Uma característica notável da tecnologia da informação reside no fato desta não ser restringida por quaisquer limites geográficos ou fronteiras nacionais. Com isso, tem-se a conduta dos criminosos em locais diferentes daqueles em que são produzidos os resultados.

Pelo fato de as legislações nacionais estarem normalmente confinadas a um território definido, impõe-se que as soluções para os problemas que surgem com os crimes cibernéticos envolvam a legislação internacional.

Por isso, a seguir, analisar-se-á brevemente alguns instrumentos jurídicos de âmbito internacional, especificamente dos Estados Unidos e da Europa.

### 4.1 Estados Unidos da América

A primeira legislação tratando dos crimes cibernéticos foi aprovada no final da década de 1980, pelo Congresso americano, e foi chamada de *Electronic Communication Privacy Act* (ECPA[3] - Lei de Privacidade de Comunicação Eletrônica), sendo amplamente utilizada pelo FBI e a *National Security Agency* (NSA[4] - Agência de Segurança Nacional), além de servir como ponto de partida para a legislação de outros países.

Poucos anos depois, foi aprovada a *Computer Fraud and Abuse Act* (CFAA [5] - Lei de Fraude e Abuso de Computadores), que ainda está em vigor.

Vale ressaltar que desde sua criação, a CFAA foi emendada oito vezes devido à rapidez com a qual os crimes evoluíam e as previsões legais se tornavam ultrapassadas. A última emenda foi em 2008 e durante esse hiato de atualizações, diversas propostas revisionais foram feitas, tanto para reduzir as reprimendas previstas quanto para torná-las mais severas, contudo, nenhuma aprovada (JARRETT, 2010, p.8).

Em maio de 2000, o *Internet Crime Complaint Center* (IC3[6] - Centro de Denúncias de Crimes na Internet) foi criado com o objetivo de receber as denúncias relacionadas a crimes cibernéticos. De acordo com seu relatório anual, foram reportados 3.463.620 (três milhões, quatrocentos e sessenta e três mil e seiscentos e vinte) incidentes no mundo desde sua

[3] Disponível em: https://it.ojp.gov/privacyliberty/authorities/statutes/1285

[4] Disponível em: https://www.nsa.gov/

[5] Legislação disponível em: http://uscode.house.gov/view.xhtml?req=(title:18%20section:1030%20edition:prelim)#sourcecredit

[6] Disponível em: https://www.ic3.gov/default.aspx

implementação até o final de 2015. Inclusive, somente em 2015, nos Estados Unidos, estima-se um prejuízo de mais de 01 (um) bilhão de dólares, considerando ainda que apenas 15% das vítimas desses crimes reportam às autoridades competentes, o que torna o combate ainda mais difícil[7].

É caso de se destacar a atuação do FBI, que, ao longo dos anos tem tentado diversas estratégias para frear a crescente onda de crimes cibernéticos que tem se alastrado pelo mundo. Além de atuar em conjunto com outras organizações, como a IC3, o FBI possui um setor composto por agentes altamente treinados em informática forense, inclusive alguns *hackers*, chamado de *Cyber Division*[8] [9]. Ainda que os crimes cibernéticos muitas vezes não tenham um local definido, a *Cyber Division* possui escritórios espalhados por todo o solo americano, com esquadrões de aproximadamente cinquenta agentes, dentre técnicos de informática, a fim de atender rapidamente a demanda de forma extremamente especializada. (FBI, s.d.).

No início de 2016, o então presidente norte-americano Barack Obama, lançou o *Cybersecurity National Action Plan*[10] (Plano de Ação Nacional de Segurança Cibernética), que nada mais é do que um plano governamental que visou providenciar ferramentas necessárias para fortalecer a segurança nacional cibernética e proteger a economia do país. O plano da Administração do governo de Obama não só destinou mais verba para pesquisas, equipamentos, capacitação e prevenção, como também determinou uma maior interação entre o Governo, as empresas privadas, as forças policiais e os cidadãos.

[7] Conforme relatório disponível em: https://pdf.ic3.gov/2015_IC3Report.pdf

[8] Disponível em: https://www.fbi.gov/investigate/cyber

[9] "Divisão Cibernética", em inglês.

[10] Disponível em: https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

### 4.2 Europa

O continente europeu deu origem a um instrumento legislativo internacional exemplar: a Convenção de Budapeste[11] - ou Convenção sobre o Cibercrime - por meio do Conselho da Europa[12], organismo internacional composto por 47 (quarenta e sete) Estados membros, dos quais 28 (vinte e oito) são integrantes da União Europeia[13].

A Convenção, considerada um tratado internacional de justiça criminal, foi aberta para assinatura em 21 de novembro de 2001, em Budapeste, na Hungria, e, até a data da edição do presente estudo, foi ratificada por 49 (quarenta e nove) países, inclusive os Estados Unidos. Cabe destacar que o Brasil não é signatário da Convenção de Budapeste ou de qualquer outra medida legislativa no que concerne cooperação internacional relacionada aos crimes cibernéticos.

Cabe também destacar o objeto da referida Convenção:

a) A criminalização de um conjunto de delitos contra e através de computadores no direito doméstico e a harmonização dos elementos normativos relativos às infrações;
b) Definição dos poderes necessários às autoridades competentes, de acordo com o código de processo penal pátrio, para proteger as provas digitais de qualquer crime, como mandado de busca e apreensão, etc. E ainda, limitar tais poderes, a fim de evitar abuso de poder e proteger os princípios fundamentais dos Estados;
c) Instigar uma cooperação internacional rápida e eficaz, além de uma cooperação das forças policiais e do judiciário.

Isso significa, em resumo, que o objetivo da Convenção é servir como um guia consistente para outros países ao desenvolverem e executarem uma legislação interna sobre os

[11] Disponível em: http://www.internacional.mpf.mp.br/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf
[12] Disponível em: http://www.coe.int/en/web/about-us/who-we-are

[13] Lista oficial de países signatários da Convenção de Budapeste, atualizada em 13 de novembro de 2016, pelo próprio Conselho da Europa, em seu endereço eletrônico: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

crimes cibernéticos, abrangendo tanto o Direito Penal Material quanto o Processual Penal, respeitando sempre a soberania estatal.

O documento possui 48 (quarenta e oito) artigos divididos em 04 (quatro) capítulos, quais sejam: Terminologia (Artigo 1); Medidas a tomar a nível nacional (artigos 2 a 22); Cooperação Internacional (artigos 23 a 35); Disposições finais (artigos 35 a 48).

Verifica-se ser um documento de imprescindível leitura, uma vez que cada capítulo possui disposições extremamente relevantes que visam um combate colaborativo e eficiente contra os crimes cibernéticos.

No Capítulo 1, tem-se a terminologia de elementos normativos, essenciais para criação e atualização de tipos penais dos países signatários.

Sobre a importância de tais conceitos, deve-se salientar que não há, no Brasil, conceituação exata do que é "sistema informático", "sistema de informações", "dados informáticos" para fins penais, de modo que sendo estes elementos objetivos de algum tipo penal, há uma dificuldade natural do aplicador da lei ao deparar com a análise e tipificação das condutas relacionadas a estes temas.

A Seção 1 do Capítulo 2 tem por objetivo melhorar as ferramentas de prevenção e erradicação do crime cibernético, através de normas tipificadoras comuns. Assim, com a uniformidade da legislação nacional e internacional, o intercâmbio de experiências no tratamento dos casos e a cooperação internacional são facilitados.

Para alcançar esse objetivo, a Seção foi dividida em 05 (cinco) Títulos, nos quais são listadas infrações que representam um consenso mínimo, ou seja, não se exclui qualquer extensão que possa existir na legislação nacional de cada país signatário.

Nesse momento, é essencial frisar que, a linguagem utilizada na Convenção é uma linguagem neutra em termos tecnológicos, de modo que as infrações ali definidas podem ser aplicadas tanto às tecnologias atuais quanto às futuras. E ainda, todas as infrações enunciadas na Convenção devem ser cometidas "intencionalmente" para que seja imputável a responsabilidade criminal. Por fim, não se deve olvidar que a Convenção serve como um guia, cabendo às Partes, no exercício do seu poder discricionário, acrescentar condições e/ou restrições que sejam compatíveis com os seus respectivos sistemas jurídicos nacionais.

A Seção 2 do mesmo Capítulo, por sua vez, aborda: o âmbito das disposições processuais; as condições e salvaguardas; a conservação expedita de dados informáticos armazenados; a

injunção; a busca e apreensão de dados informáticos armazenados; a recolha em tempo real de dados informáticos e interceptação de dados relativos ao conteúdo.

O Capítulo 3 aborda os "princípios gerais relativos à cooperação internacional", incluindo diversas disposições relativas à extradição e assistência jurídica mútua entre os países, instituindo ainda, mecanismos específicos para tal, como a rede 24/7[14]. Ressalta-se que as disposições contidas neste capítulo não anulam nem substituem as disposições dos instrumentos internacionais relativos à assistência jurídica e a extradição, dos acordos de mesma matéria celebrados entre as Partes, ou as respectivas disposições da legislação nacional relativas à cooperação internacional.

O Capítulo 4, por sua vez, contém as disposições finais, no mesmo sentido das cláusulas finais para as convenções e acordos celebrados no quadro do Conselho da Europa, tratando de assinatura, entrada em vigor, adesão, aplicação, efeitos, declarações, reservas, aditamentos, etc. (CONVENÇÃO SOBRE O CIBERCRIME, 2001).

Após a análise supra, torna-se necessário reconhecer a importância da Convenção de Budapeste, visto que nos últimos anos ela teve um impacto global e resultou numa legislação mais forte e mais harmonizada no domínio da cibercriminalidade a nível mundial, numa cooperação internacional mais eficaz na investigação e na instauração de processos penais contra crimes cibernéticos e em parcerias público-privadas mais estreitas.

Assim, 15 anos após sua adoção, a Convenção de Budapeste continua sendo o tratado internacional mais eficaz em matéria de crimes cibernéticos e do Estado de Direito no ciberespaço. Este fato é resultado da consciência excepcional dos redatores da Convenção, pois eles sabiam que estavam escrevendo algo que não seria alterado em poucos anos, e assim, a convenção deveria ser um instrumento estável. Para tanto, eles redigiram brilhantemente em antecipação ao futuro, acomodando novas tecnologias.

# 5. LEGISLAÇÃO BRASILEIRA

[14] A rede 24/7 é um ponto de contato em cada Parte, que deve estar disponível 24 horas por dia, 7 por semana, a fim de garantir uma assistência imediata para as investigações e processos penais relativos a infrações cometidas por meio de sistemas informáticos.

Feitas as devidas considerações sobre a legislação adotada em outros países, passa-se uma indispensável análise da legislação brasileira, visto que há uma grande dificuldade no cenário pátrio em formular leis específicas e punições satisfatórias à altura dos crimes cibernéticos que são cometidos atualmente.

Até o ano 2012, não existia nenhuma lei para punir os crimes cibernéticos próprios, existindo somente legislação acerca dos crimes cibernéticos impróprios. Contudo, em decorrência de alguns episódios, como os DDoS - *Distributed Denial of Service* (ataques distribuídos de negação de serviço) a sites do governo e a divulgação de fotos íntimas da atriz Carolina Dieckmann, duas leis foram sancionadas com maior urgência, sanando algumas das várias deficiências existentes no ordenamento em relação a essa matéria, quais sejam, a Lei 12.735/2012[15], conhecida popularmente como "Lei Azeredo", e a Lei 12.737/2012[16], conhecida como "Lei Carolina Dieckmann".

Em 2014, foi sancionada pela ex-presidente Dilma Rousseff, a Lei 12.965/2014, oficialmente chamada de Marco Civil da Internet[17], que por sua vez, regula a mesma no Brasil estabelecendo princípios, garantias, direitos e deveres para o seu uso, para os usuários e também para o próprio Estado.

Além dessas legislações supracitadas, que serão tratadas de forma mais abundante, ainda tem-se a Lei nº 11.829/2008, que combate a pornografia infantil na internet; a Lei nº 9.609/1998, que trata da proteção da propriedade intelectual do programa de computador; a Lei nº 9.983/2000, que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da Administração Pública; a Lei nº 9.296/1996 disciplinou a interceptação de comunicação telemática ou informática; e a Lei nº 12.034/2009, que delimita os direitos e deveres dentro da rede mundial, durante as campanhas eleitorais.

Porém, embora representem um avanço significativo no combate à criminalidade na Internet no Brasil, as leis pátrias deixaram a desejar em vários aspectos, restando muito a ser feito quanto a criminalidade digital.

[15] Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm#art6

[16] Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm

[17] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

A seguir, será feita uma breve exposição das legislações consideradas mais relevantes, com o objetivo de tentar aferir a que distância se está de alcançar uma proteção razoável dos interesses civis e governamentais, no tocante à matéria cibernética.

Além disso, não faz parte do escopo desse trabalho detalhar todo o cenário legislativo brasileiro, uma vez que as legislações citadas a seguir serão apenas uma referência para a leitura.

### 5.1 Lei 12.735/12 – "Lei Azeredo"

Primeiramente, é importante ressaltar a distinção entre o Projeto de Lei (PL) 84/99 e a Lei 12.735/12, ambas popularmente conhecidas como "Lei Azeredo".

O PL 84/99, inicialmente apresentada pelo ex-deputado federal Luiz Piauhylino, e posteriormente alterada pelo então senador Eduardo Azeredo, dispunha sobre os crimes, penas e outras providências quanto ao meio virtual. Porém, além da linguagem utilizada ser imprecisa, muitas de suas disposições afrontavam a privacidade e a liberdade na Internet, sendo até mesmo apelidada por ativistas de "AI-5 Digital". (COMISSÃO, 2012).

Assim, a PL 84/99 foi transformada na Lei Ordinária 12.735/12 - também popularmente chamada de Lei Azeredo -, que alterou apenas o inciso II do § 3° do art. 20 da Lei n° 7.716/89[18], conhecida como Lei do Crime Racial, para permitir que uma solicitação de retirada de conteúdo discriminatório não somente de rádio, TV ou Internet, mas de qualquer meio possível, fosse feita pelo Juiz. Determinou também que os órgãos da polícia judiciária deveriam criar delegacias especializadas no combate a crimes praticados por meio da Internet ou por sistema informatizado.

### 5.2 Lei 12.737/12 – "Lei Carolina Dieckmann"

A Lei 12.737/12 se originou a partir do Projeto de Lei 2793/11[19] e foi apelidada de Lei Carolina Dieckmann – ou Lei Dieckmann – em razão do vazamento das fotos íntimas da atriz,

[18] Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L7716.htm

[19] Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=944218&filename=PL+2793/2011

que acabou por dar algum destaque ao referido projeto, proposto no ano anterior, sendo aprovado duas semanas após o referido episódio, pela Câmara dos Deputados.

De coautoria do então Deputado Federal Paulo Teixeira, a Lei Dieckmann praticamente resgatou o que o PL 84/99 perdeu, contudo, sem as polêmicas da época, dispondo sobre delitos informáticos, tipificando condutas que não eram previstas, de forma específica, como infrações penais.

Criou-se o tipo penal "invasão de dispositivo informático", previsto no art. 154-A do Código Penal Brasileiro, e sua respectiva modalidade de ação penal, prevista no art. 154-B do mesmo Código, que é, em regra, condicionada a representação.

Além da inclusão desses dois dispositivos, a redação dos delitos previstos no art. 266 298, do mesmo diploma legal, foi ampliada. O tipo penal de indisponibilização de serviço público passou a abranger serviços telemáticos ou de informação de utilidade pública. Já no tipo do crime de falsificação de documento particular, a nova lei inseriu a equiparação do cartão de crédito ou débito a documento particular.

Segundo Patrícia Peck Pinheiro (2013), vale observar ainda que:

> Ainda, receberá as mesmas penas da invasão aquele que instala uma vulnerabilidade em um sistema de informação para obter vantagem indevida, por exemplo, um *backdoor* ou uma configuração para que algumas portas de comunicação à Internet fiquem sempre abertas.
> O usuário de *gadgets* e dispositivos informáticos comuns estão protegidos contra hackers e pessoas mal-intencionadas que abusam de confiança ou buscam intencionalmente devassar dispositivo para se apropriar de dados do computador ou prejudicar o seu proprietário, com a exclusão ou alteração de dados, para que fiquem imprestáveis, ou ainda, informações íntimas e privadas, como fotos, documentos e vídeos.
> As empresas possuem maior proteção jurídica contra a espionagem digital, pois a obtenção de segredos comerciais e ou informações sigilosas definidas por lei agora também se enquadram na lei.

Apesar de parecerem suficientes, ambas as Leis 12.735 e 12.737 não lograram êxito em preencher todas as lacunas que a legislação brasileira tinha em relação ao combate aos crimes cibernéticos. Em verdade, possuem alguns vícios, que necessitam ser sanados urgentemente, a fim de se evitar a impunibilidade.

A Lei Dieckmann, por exemplo, não considerou como crime a indisponibilidade de sistemas de informação de entidades privadas, como sites de banco. Ainda, houve uma desídia do legislador ao determinar que "obter, adulterar ou destruir", presentes no *caput* do art. 154-A do

Código Penal, sejam elementares ao tipo penal de invasão a dispositivo, pois, dessa forma, o simples ato de vasculhar não se adequaria ao tipo penal. Sem contar que a Lei deixa os dispositivos que não têm mecanismos de segurança - como uma senha – completamente desamparados.

Vale trazer uma observação feita pelo Ministério Público Federal (2015) em relação à ausência de definição de termos técnicos nessa Lei, presentes, por sua vez, na Convenção de Budapeste: "O uso do termo 'dispositivo informático' também é criticado porque deveria ter sido usado 'dispositivo eletrônico' justamente para abranger a grande quantidade de celulares, televisores etc., que permitem acesso à Internet". A harmonização de termos técnicos é imprescindível para a efetiva abrangência de um tipo penal, tanto próprio quanto impróprio.

### 5.3 Lei Marco Civil da Internet

O Marco Civil da Internet, por sua vez, originou-se do combate ao polêmico PL 84/99, por isso, teve grande participação popular. Durante sua elaboração, foram realizadas consultas públicas, que se dividiram em duas fases: uma com vasta diversidade de opiniões, incluindo a sociedade civil e as mais variadas empresas, nacionais e internacionais, do ramo digital, e outra, também com participação popular, mas discutindo cada dispositivo proposto na primeira fase.

Um dos objetivos do Marco Civil da Internet era indicar um documento que servisse como base para regular os princípios gerais do Marco Civil. O referido documento-base foi o publicado pelo CGI.br - Comitê Gestor da Internet no Brasil, chamado "Princípios para a Governança e Uso da Internet no Brasil"[20].

Da mesma forma que a Lei 12.735 e a Lei Dieckmann, o Marco Civil deixa a desejar, por mais que pareça ser eficaz ao tratar dos direitos do usuário. O ato de introduzir ferramentas judiciais do mundo físico – como a obtenção de ordem judicial – no mundo virtual é contra produtivo, uma vez que as velocidades entre os dois mundos são incompatíveis, enquanto o primeiro é mais moroso, o segundo requer cada vez mais celeridade.

Isto posto, reforça-se ainda mais a urgência em inovações jurídicas na legislação pátria, no que tange os crimes cibernéticos e proteção cibernética nacional.

[20] Cartilha disponível em: http://www.cgi.br/principios/

# 6. INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

Discorrido sobre o tratamento americano, europeu e brasileiro, dado à matéria dos crimes cibernéticos, apresenta-se as forças responsáveis pela atividade investigativa da referida matéria, porém, em âmbito estadual, e no caso, através do Ministério Público de Minas Gerais.

## 6.1 Ministério Público de Minas Gerais

O MPMG - Ministério Público de Minas Gerais tem uma coordenadoria especifica para tratar de crimes cibernéticos, chamada Coordenadoria Estadual de Combate aos Crimes Cibernéticos (Coeciber). Criada em 2008, ela está vinculada ao Centro de Apoio Operacional das Promotorias Criminais, de Execução Penal, do Tribunal do Júri e da Auditoria Militar (Caocrim) e conta com promotores de justiça, policiais, analistas de inteligência e analistas jurídicos.

A Coeciber tem por finalidade auxiliar a atuação do Ministério Público (MP) em todo o estado, articulando medidas judiciais e extrajudiciais, no combate aos crimes praticados na Internet.

Segundo o *website*[21] do órgão ministerial[22],

> Aliada à sua natureza de órgão de investigação, a Coordenadoria de Combate aos Crimes Cibernéticos vem desenvolvendo, desde sua criação, importante papel preventivo junto à comunidade escolar, no sentido de orientar crianças, adolescentes e seus pais a utilizarem a Internet de forma mais segura, bem como alertá-los dos perigos que rondam a web, prevenindo, assim, que se tornem vítimas de crimes praticados na rede mundial de computadores.
> Entre as iniciativas da Coordenadoria, destacam-se palestras em escolas públicas e particulares, distribuição de fôlderes e cartilhas com dicas e orientações sobre navegação segura, bem como treinamentos institucionais e de inteligência.

Contudo, existem inúmeras dificuldades no auxilio dessa persecução penal. Hoje, por exemplo, não existe uma legislação que imponha aos provedores a obrigação de fornecer informações necessárias para a investigação às forças de segurança e ao MP. O que dificulta o

[21] Sítio eletrônico, em inglês.

[22] Disponível em: https://www.mpmg.mp.br/areas-de-atuacao/atuacao-criminal/crimes-ciberneticos/

trabalho da Coordenadoria é justamente a obtenção, não só da materialidade, mas da autoria delitiva.

Dentre os diversos estorvos, os mecanismos para obter a autoria delitiva estão em poder da iniciativa privada, dos provedores. E os provedores têm sede, principalmente, nos EUA, dependendo da cooperação jurídica internacional para obter os dados necessários para descobrir onde foi criada e utilizada a conta infratora.

Perante as dificuldades no enfrentamento aos criminosos, a Coordenadoria tem realizado também alguns trabalhos preventivos junto à população e autoridades em todo o país.

Em razão da ausência de conduta típica, o MPMG tem arquivado os inquéritos, configurando mais uma dificuldade na persecução penal, que serão abordadas no capítulo seguinte.

# 7. DIFICULDADES ENFRENTADAS NA PERSECUÇÃO PENAL

Até aqui, viu-se que a persecução penal em relação aos crimes cibernéticos no país está longe de ser satisfatória, por diversas razões. Assim, no presente capítulo, apresentar-se-á a deficiência das leis tipificadoras, a ausência de profissionais especializados, e, por fim, a importância da cooperação internacional.

## 7.1 Deficiência da lei tipificadora

A ausência de legislação bem elaborada e específica torna possível a existência de condutas atípicas que não podem ser punidas em decorrência do princípio da reserva legal. Contudo, existem também as condutas típicas, porém tipificadas de forma insatisfatória ou incompleta, o que gera graves repercussões em meio a sociedade.

Um exemplo básico, porém, relevante, deste último caso, são os Ataques Distribuídos de Negação de Serviço, ou simplesmente, DDoS, uma técnica maliciosa pela qual o agente utiliza equipamentos conectados à rede, de forma coordenada e distribuída, parar deixar um serviço, computador ou rede, inoperante.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil[23] (CERT.br), ainda explica:

> Um ataque DDoS não tem o objetivo direto de invadir e nem de coletar informações, mas sim de exaurir recursos e causar indisponibilidade ao alvo. Os usuários desses recursos são diretamente afetados e ficam impossibilitados de acessar ou realizar as operações desejadas, já que o alvo do ataque não consegue diferenciar os acessos legítimos dos maliciosos e fica sobrecarregado ao tentar tratar todas as requisições recebidas. (CERT.BR, 2016)

Tais ataques têm sido um grande problema para os usuários da Internet, sejam eles públicos ou privados, há muito tempo. E é nesse momento que se destaca uma falha presente na legislação pátria.

A Lei Dieckmann, através de seu art. 3°, altera o disposto no artigo 266 do Código Penal, como visto anteriormente, acrescentando o seguinte §1°: "Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento". Contudo, o dispositivo se mostra insuficiente, uma vez que faltam os elementos normativos do tipo: "Serviço telemático e informação de utilidade pública" não alcançam o ataque a um website porque não o é assim definido.

Percebe-se então, que, mesmo em legislação específica, a linguagem e terminologia, quando não utilizadas adequadamente, tornam a lei defeituosa. Viu-se, portanto, apenas um exemplo de falha em uma legislação existente, sendo o ataque DDoS uma conduta criminosa parcialmente amparada. Passa-se agora, ao exemplo de uma conduta criminosa, altamente recorrente, e que, mesmo sendo configurada a um tipo penal já existente, necessita urgentemente de um tipo penal específico devido às suas particularidades.

O *Ransomware*, por definição do CERT.br, "é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia[24], e que exige pagamento de um *ransom* (resgate) para restabelecer o acesso ao usuário". Muitas vezes, até mesmo outros dispositivos conectados, locais ou em rede, ao equipamento em questão, são criptografados.

[23] Esse Centro é mantido pelo Comitê Gestor da Internet no Brasil e, segundo descrito em seu próprio *website*, é de sua responsabilidade receber, analisar e responder a incidentes de segurança em computadores, envolvendo redes conectadas à Internet no território nacional.

[24] De maneira simplificada, pode-se dizer que a criptografia é um mecanismo para codificar qualquer coisa que se queira.

Importante ressaltar que o *Ransomware* é um crime cibernético próprio, vez que é perpetrado por intermédio e contra um sistema informático, sendo impraticável a realização da conduta por outros meios. Aliás, o pagamento do resgate não é feito em moeda corrente tradicional, e sim via *bitcoins*[25].

A conduta descrita muito se assemelha a um sequestro, sendo por muitas vezes chamada de "sequestro de dados". Entretanto, a prática do *Ransomware* é configurada como crime de extorsão.

Ainda que esse crime seja abarcado por outro tipo penal já existente, o *Ransomware* requer uma atenção. Apesar de ser uma conduta relativamente nova, considerando sua popularidade, e aparentar ser inofensiva ao se ouvir "sequestro de dados", ela não o é. Para elucidar a extensão de sua ameaça, bastarão alguns exemplos.

Hospitais, escolas, governos estaduais e municipais, órgãos do judiciário, empresas de pequeno porte e grandes empresas são apenas algumas das entidades que podem ser afetadas por esse código malicioso. E a impossibilidade dessas organizações de acessar seus dados pode ser catastrófica, tais como: perda de informações confidenciais ou proprietárias, interrupção das operações regulares, prejuízos financeiros para restaurar os sistemas e arquivos, e o potencial dano para a reputação de uma organização.

Sem mencionar que os computadores domésticos também são suscetíveis a *Ransomware*. A perda do acesso a dados pessoais e, muitas vezes, insubstituíveis, como fotos, vídeos e outros dados podem ser devastadores para os indivíduos, que hoje depositam grande parte de suas vidas em computadores, *hard drives* e, principalmente, na nuvem.

Por fim, confere ressaltar outra peculiaridade do *Ransomware*, que é a sua sofisticação e velocidade. Ao aumentarem gradativamente, deixam a legislação cada vez mais defasada, e, consequentemente, o *Ransomware* se torna uma conduta com alto nível de dificuldade no seu combate.

### 7.2 Necessidade de profissionais especializados

[25] É uma moeda mercadológica, uma criptomoeda e sistema de pagamento online baseado em protocolo de código aberto que é independente de qualquer autoridade central. Um *bitcoin* pode ser transferido por um computador ou smartphone sem recurso a uma instituição financeira intermediária.

O primeiro passo na investigação dos crimes cibernéticos é identificar a origem da comunicação. Por meio de uma análise do tráfego de dados, se chegará ao endereço IP de origem e ao usuário que está vinculado a esse IP.

Segundo Peck (2016), no direito digital, a identificação de um computador é feita por meio do endereço IP - *Internet Protocol* (Protocolo de Internet). O número IP é atribuído a cada usuário ou internauta, toda vez que uma conexão for estabelecida com a rede mundial de computadores. Além de permitir a identificação virtual, o IP descreve todo o tráfego de rede e acessos feito pelo usuário em determinado período.

Assim, uma vez identificado o endereço IP, serão analisadas possíveis provas da prática do delito. Essa análise, feita por peritos especializados, é uma atividade extremamente complexa, considerando a presença de programas de computador cujo objetivo é o mascaramento da verdadeira identidade do autor, principalmente quando os computadores estão localizados em locais e redes públicas. (PECK, 2016)

Por esse motivo, a comprovação dos crimes cibernéticos não é tarefa fácil. É necessária qualificação técnica específica dos profissionais responsáveis pela verificação dos vestígios deixados quando da prática de um crime virtual, nem sempre presentes nos locais em que os crimes se consumam.

Contudo, não é necessária somente a qualificação de peritos. Além da constante atualização dos peritos criminais, o Direito Digital traz a obrigação de atualização tecnológica também para advogados, juízes, delegados, procuradores, investigadores, e todos os envolvidos no processo.

Vale ressaltar que todos os juristas devem se adequar à nova realidade mundial, que busca diminuir fronteiras e dar celeridade. O conhecimento acerca do ordenamento legal deve ser associado ao conhecimento sobre os instrumentos informáticos, possibilitando o surgimento de profissionais cada vez mais capazes de solucionar conflitos atuais, que quase em sua totalidade, envolvem questões tecnológicas.

### 7.3 Necessidade de cooperação internacional

Como os crimes cibernéticos ocorrem no mundo inteiro e pelo fato de não respeitarem fronteiras, além da legislação específica, é necessário a adesão a tratados internacionais que disciplinam a matéria.

Um fator já mencionado é a harmonização das nomenclaturas dos elementos normativos dos tipos penais. Isso faz com que os tipos penais deixem, em tese, de desamparar alguns sistemas, serviços e operações, por não terem uma identidade de conceitos. Tal como explanado anteriormente em relação aos ataques DDoS.

Outro fator relevante, se não o mais importante, é a questão da celeridade. Viu-se ao longo dessa pesquisa que a questão mais constante é a de os crimes cibernéticos sempre estarem à frente da legislação. E isso se deve ao desenvolvimento incessante da tecnologia, que a cada dia abre novas possibilidades de condutas cada vez mais ágeis.

Portanto, um instrumento jurídico internacional que propõe agilizar a tipificação de algumas condutas, sugere procedimentos processuais penais, e principalmente, permite um contato entre os países, 24 horas por dia, 7 dias na semana, se torna de extremo interesse para uma nação, no caso em tela, o Brasil.

As disposições presentes na Convenção de Budapeste, demonstram a constante necessidade em dar celeridade a tudo que for possível no que se refere ao Direito clássico, pois somente assim que a distância existente entre a lei e a impunidade no mundo digital, reduzirá.

# CONCLUSÃO

As novas tecnologias da informação, especialmente a Internet, impulsionaram (e continuam impulsionando) o processo de globalização econômica e cultural. Essas mudanças trouxeram novos paradigmas para a sociedade pós-moderna e os sistemas que a organizam e regulam, como o Direito.

Novas modalidades criminosas surgiram, uma vez que o ambiente virtual alimenta no ser humano a sensação de liberdade ao separar as pessoas por uma interface e proporcionar o anonimato.

Assim, a partir das observações efetuadas ao longo deste trabalho, constatou-se que a criminalidade informática não foi responsável somente pelo aparecimento de novas condutas

ilícitas praticadas com o auxílio de um computador, mas também possibilitou a violação de bens jurídicos até então não atingidos com a prática dos delitos já previstos no ordenamento jurídico brasileiro.

Ainda que existam algumas normas que tratem da matéria, pode-se afirmar que o Brasil, quando comparado a outros países, ainda está em processo de crescimento no que tange o combate aos crimes cibernéticos.

Constata-se que a inovação jurídica e a deficiência da persecução penal abordadas nesse trabalho requerem muito mais que atualizações e regulamentações de novas leis no ordenamento jurídico brasileiro, pois o ritmo de evolução tecnológica será sempre mais veloz que o da atividade legislativa.

Grande parte da eficácia legal necessária para tentar suprir a deficiência legislativa interna de um país, exige uma colaboração internacional, ou seja, necessita de um tratamento adicional de múltiplos ordenamentos jurídicos, seja em sede de Tratados ou Convenções Internacionais, ou em outra fórmula legal ainda a ser inventada.

Enquanto os países tratarem do tema apenas dentro de suas realidades, a comunidade de usuários da Internet ainda ficará carente de soluções mais adequadas para proteger sua privacidade e garantir segurança no ambiente digital, uma vez que o isolamento do pensamento jurídico não se adequa à nova realidade digital da sociedade.

Isto posto, concluiu-se ser necessário a assinatura da Convenção de Budapeste, apresentada nesse trabalho, pelo Brasil, face à necessária uniformização e maior celeridade do combate transnacional aos crimes cibernéticos, evidentemente desterritorializados, e ao respeito aos direitos e liberdades individuais por ela impostos.

Além disso, depreende-se desse trabalho não só a exigibilidade de criatividade por parte do operador do direito, o qual deve deixar de ser um mero burocrata para se tornar um estrategista, como também a indispensabilidade de acompanhamento de todo profissional, seja ele da área jurídica, técnica ou administrativa, à evolução do Direito Digital, em razão de sua volatilidade.

Finalmente, com essa pesquisa, conclui-se que a sociedade digital está evoluindo muito rápido e o Direito deve acompanhar esta mudança, aprimorar-se, renovar seus institutos e criar novos capazes de continuar garantindo a segurança jurídica das relações sociais, sob pena de ficar obsoleto. Isso pode estimular a prática da "justiça com as próprias mãos" e todas as mazelas

associadas ao uso arbitrário das próprias razões e ao desequilíbrio gerado pelo poder desmedido das grandes corporações que são proprietárias dos recursos que permitem a realização da vida digital.

Por fim, cabe ressaltar que o presente estudo não tem a finalidade de exaurir a matéria dos crimes cibernéticos e sim discutir a relevância do tema para o ramo do Direito, através das suas repercussões. Mesmo porque a criatividade humana é ilimitada e não se conseguiria exaurir neste trabalho todos os aspectos jurídicos que a tecnologia pode possuir

# REFERÊNCIAS

BRASIL. Código Penal. **Decreto-Lei nº 2.848**, de 7 de dezembro de 1940. Disponível em:<http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm> Acesso em: 19 out. 2016.

BRASIL. **Constituição Federal de 1988**. Promulgada em 5 de outubro de 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm> Acesso em 21 out. 2016.

BRASIL. **Lei Ordinária nº 12.735**, de 30 de novembro de 2012. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 25 de out. 2016.

BRASIL. **Lei Ordinária nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 25 de out. 2016.

BRASIL. **Lei Ordinária nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 26 de out. 2016.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança No Brasil. **Cartilha de Segurança para Internet**: Ransomware. Disponível em: <http://cartilha.cert.br/ransomware/>. Acesso em: 30 out. 2016.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança No Brasil. **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)**. Disponível em: <http://www.cert.br/docs/whitepapers/ddos/>. Acesso em: 30 out. 2016.

**CONVENÇÃO SOBRE O CIBERCRIME**. Aberta para assinatura em Budapeste, Hungria, em 22 de novembro de 2001 Disponível em: <http://www.prpe.mpf.mp.br/internet/index.php/internet/content/download/2770/22203/file/CONVEN%C3%87%C3%83O%20DE%20BUDAPESTE.pdf>. Acesso em: 23 out. 2016.

**FEDERAL Bureau of Investigation**. Disponível em: <http:// https://www.fbi.gov>. Acesso em: 22 out. 2016.

FERREIRA, Ivette Senise. **A Criminalidade Informática**. Direito & Internet – Aspetos Jurídicos Relevantes. Editora Edipro, 2011.

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

JARRETT, H. Marshall; BAILIE, Michael W. **Prosecution of Computer Crimes**. Office of Legal Education Executive Office for United States Attorneys. 2010. Disponível em:<https://www.justice.gov/sites/default/files/criminalccips/legacy/2015/01/14/ccmanual.pdf>. Acesso em 19 out. 2016.

**Marco civil da internet entra em vigor**. Disponível em: <http://culturadigital.br/marcocivil/2014/06/23/marco-civil-da-internet-entra-em-vigor/>. Acesso em: 26 out. 2016.

MPF, Ministério Público Federal. **Combate aos Crimes Cibernéticos**. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/comissoes-e-grupos-de-trabalho/combate-crimes-cirberneticos>. Acesso em: 28 out. 2016.

MPMG, Ministério Público do Estado de Minas Gerais. **Combate aos Crimes Cibernéticos**. Disponível em: <https://www.mpmg.mp.br/areas-de-atuacao/atuacao-criminal/crimes-ciberneticos/-cirberneticos>. Acesso em: 28 out. 2016.

NUCCI, Guilherme de Souza. **Código Penal Comentado**. 16. ed. rev., atual e ampl. Imprenta: Rio de Janeiro, Forense, 2016.

PIAUHYLINO, Luiz. **Projeto de Lei nº 84, de 1999**. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Disponível em:<http://imagem.camara.gov.br/Imagem/d/pdf/DCD0019990511000820000.PDF#page=57>. Acesso em: 26 out. 2016.

PINHEIRO, Patricia Peck. **Direito digital**. 6. ed. rev., atual. e ampl. São Paulo: Saraiva, 2016.

PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. **A nova lei de crimes digitais**. 2013. Disponível em: <http://pppadvogados.com.br/profissionais/patricia-peck-pinheiro/a-nova-lei-de-crimes-digitais>. Acesso em: 27 out. 2016.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

TEIXEIRA, Paulo; Erundina, Luiza; D'ávila, Manuela; Arruda, João; Neto, Brizola; José, Emiliano. **Projeto de Lei nº 2793**, de 2011. Dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências. Disponível em:<http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=944218&filename=PL+2793/2011>. Acesso em: 26 out. 2016.

.