UNIVERSIDADE ESTADUAL DA PARAÍBA
CÂMPUS I, CAMPINA GRANDE - PB
CENTRO DE CIÊNCIAS JURÍDICAS
CURSO DE BACHARELADO EM DIREITO

HELDER LIMA DA SILVA

ESPAÇO DIGITAL INCONTROLÁVEL: INVASÕES CRIMINOSAS A "SITES", DADOS PRIVADOS E ESTATAIS

Campina Grande – PB,
2017.

HELDER LIMA DA SILVA

ESPAÇO DIGITAL INCONTROLÁVEL: INVASÕES CRIMINOSAS A "SITES", DADOS PRIVADOS E ESTATAIS

Trabalho de Conclusão de Curso apresentado como requisito parcial e obrigatório à obtenção do grau de Bacharel em Direito, ofertado pelo Centro de Ciências Jurídicas - Universidade Estadual da Paraíba (CCJ/UEPB).

Orientador(a): Prof. Doutor Luciano do Nascimento Silva

Campina Grande – PB,
2017.

S586e Silva, Helder Lima da Silva

Espaço digital Incontrolável [manuscrito] : invasões criminosas a "sites", dados privados e estatais. / Helder Lima da Silva. - 2017.

45 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas, 2017.

"Orientação: Prof. Dr. Luciano Nascimento Silva, Departamento de Direito Público".

1. Dados. 2. Invasões Criminosas. 3. Espaço Digital. Crime Virtual. I. Título.

21. ed. CDD 327

ESPAÇO DIGITAL INCONTROLÁVEL: INVASÕES CRIMINOLÓGICAS A "SITES", DADOS PRIVADOS E ESTATAIS

Trabalho de Conclusão de Curso apresentado como requisito parcial e obrigatório à obtenção do grau de Bacharel em Direito, ofertado pelo Centro de Ciências Jurídicas - Universidade Estadual da Paraíba (CCJ/UEPB).

Orientador(a): Prof. Doutor Luciano do Nascimento Silva

Aprovado em: 29 / 05 / 2017

BANCA EXAMINADORA

Orientador(a): prof. DOUTOR LUCIANO DO NASCIMENTO SILVA
Universidade Estadual da Paraíba (UEPB/CCJ).

Avaliador(a): prof. DOUTOR RODRIGO COSTA FERREIRA
Universidade Estadual da Paraíba (UEPB/CCJ).

Avaliador(a): prof. MESTRE MARCELO D`ANGELO LARA
Universidade Estadual da Paraíba (UEPB/CCJ).

Dedico este Trabalho de Conclusão de Curso a Deus e aos meus familiares.

AGRADECIMENTOS

Agradeço primeiramente a DEUS por ter dado a mim sabedoria, inteligência, para tamanha empreitada durante esses mais de 5 (cinco) anos de academia que, acresceu intelectualmente na minha vida acadêmico-pessoal, de forma holística.

Minha todo-poderosa mãezinha do céu sempre comigo rogando e intercedendo junto ao seu filho Jesus, protegendo-me, guiando-me no bom caminho e livrando de todo o mal, eternamente grato a Nossa Senhora.

À minha mãe, ao meu pai, aos meus avós, meus irmãos, tios, primos, amigos que fiz durante esta longa jornada, sempre incentivando e buscando dar positividade para que consiga realizar meus objetivos pessoais e profissionais por intermédio do Direito.

Agradecimento especial à minha orientadora, não mais presente entre nós, minha co-orientadora e ao meu orientador final. Por debruçar-se com afinco acadêmico e científico sempre presentes no seu ofício quanto docente.

Agradeço também, sem deixar de enaltecer, aos serventuários da justiça, técnicos, analistas, oficiais, diretor de vara, juízes – titular e substituto – da 11º Vara Federal Subsecção Paraíba da 5º Região da Justiça Federal, que me acolheram e ensinaram como se pedagogos fossem, dada a imensa dedicação e preocupação ao repassar o escólio de cada despacho, decisão, sentença por mim proferidos. Fica registrada a gratidão.

Por derradeiro, não poderia jamais deixar de me congratular com a Instituição UEPB, seus servidores e mais ainda com o corpo docente que, no ramo do direito, sem nenhum demérito a outras instituições, é excelência em capacitar intelectualmente seus discentes. São verdadeiros pais e mães orientadores do saber intelectual, dotados de responsabilidade acadêmico-profissional e interpessoal, repassando o que tem de maior relevância para o indivíduo que é o conhecimento. Doam-se com infindável vocação propedêutica possível.

“Ultrapassa-te a ti mesmo a cada dia, a cada instante. Não por vaidade, mas para corresponderes à obrigação sagrada de contribuir sempre mais e sempre melhor, para a construção do Mundo. Mais importante que escutar as palavras é adivinhar as angústias, sondar o mistério, escutar o silêncio. Feliz de quem entende que é preciso mudar muito para ser sempre o mesmo”.

Dom Hélder Câmara

SUMÁRIO

1 INTRODUÇÃO 10
2 CONCEITO DE DADOS 11
3 REVISÃO DE LITERATURA 12
3.1 O Crime Além Fronteira 13
3.2 Convenção de Budapeste 15
3.3 Breve Relato 15
3.4 Jurisdição Internacional 17
3.5 Litispendência 19
3.6 Evolução Legislativa 21
3.7 Histórico e Conceitos da Internet e das Ameaças Trazidas pela Evolução dos Recursos Tecnológicos 22
3.7.1 Internet 22
3.7.2 Ameaças Virtuais 24
3.8 Aspectos Constitucionais e Princípios do Direito Penal Relativos à Sociedade, à Informação e ao Crime Virtual 26
3.9 Crimes Virtuais e a Legislação Pertinente 31
3.9.1 Noções Preliminares 31
3.9.2 Ineficácia da Legislação 31
3.9.3 Breves Considerações sobre as Leis Ordinárias 12.735/2012 e 12.737/2012 35
4 METODOLOGIA 40
5 CONCLUSÃO 41
REFERÊNCIAS 42

RESUMO

O presente trabalho interdisciplinar visa a discutir o tema espaço digital incontrolável: invasões criminosas a "sites", dados privados e estatais, quedando sob o viés que vem sendo entoado hoje pela literatura correlata no aspecto criminal, processual criminal, jurisdicional, da internet, as ameaças trazidas pela internet, casos conflitantes, ameaças virtuais, aspectos constitucionais sobre o tema, crimes virtuais, convenção internacional correlata, marco civil da internet, conceitos, teorias, dentre outros. Trabalho desenvolvido com base no método qualitativo de busca em biografias referendadas no mundo acadêmico, tendo como fim o interesse precipuamente intelectual. Trazendo vários autores de renome como Rogério Sanches, Liliana Minardi, Patrícia Peck, Nucci. Com o intuito de abordar fatos que necessitam de uma apreciação técnico-científica de profissionais, estudantes e outros investigadores que empenham na descoberta de fatos ilegais, consubstanciados na internet. Vindo a se tornar prática criminosa que cresce a cada dia no meio cibernético, não só em lugares restritos, mas em todo o mundo, principalmente no Brasil, que por vezes, está na mídia com casos que não se têm tomada a devida providência e tornam mais e mais frequentes.

Palavras-chave: Dados. Invasões Criminosas. Espaço Digital. Crime Virtual

ABSTRAC

The present interdisciplinary work aims at discussing the topic of uncontrollable digital space: criminal invasions to "sites", private and state data, being under the bias that is being sung today by the related literature in the criminal, criminal, jurisdictional, internet, Internet threats, virtual threats, constitutional aspects of the subject, virtual crimes, international co-conventions, internet civilian framework, concepts, theories, among others. Work developed on the basis of the qualitative method of searching in referenced biographies in the academic world, aiming at the mainly intellectual interest. Bringing several renowned authors such as Rogério Sanches, Liliana Minardi, Patrícia Peck, Nucci. In order to address facts that need a technical-scientific appreciation of professionals, students and other researchers who work on the discovery of illegal facts, embodied in the Internet. It has become a criminal practice that grows every day in the cybernetic environment, not only in restricted places, but throughout the world, especially in Brazil, which is sometimes in the media with cases that have not been taken and More and more frequent.

Keywords: Data. Criminal Invasions. Digital Space. Virtual Crime.

1 INTRODUÇÃO

O presente Trabalho de Conclusão de Curso tem como título e respectivo subtítulo espaço digital incontrolável: invasões criminosas a “sites”, dados privados e estatais.

Visa abordar fatos e situações quotiadianos frequentes da nossa sociedade global que, hodiernamente, vangloria e ao mesmo tempo padece com o advento da tecnologia e mais precisamente da internet, o mundo global rendeu-se a esta ferramenta. Muitas vezes chegando a excluir uma sociedade que desconheça este salutar meio de comunicação. Muito embora, com toda qualificação dá, sim, para viver sem tanta tecnologia que o capital nos impõe, exemplo disso são tribos nômades, indígenas, alguns países socialistas que recusam a entrada desse sistema nos seus territórios, como Cuba. Sem dúvida, é uma excelente unidade comunicativa imprescindível a repartições públicas, privadas, estudantes, profissionais, leigos, enfim, toda a camada populacional usa 24 horas por dia este recurso que, sem ele, demoraria quem sabe, meses ou anos para resolvermos problemas quotidianos e longínquos. Indubitavelmente a marca do século XX.

Nesse diapasão está o trabalho dividido em três capítulos, buscando sempre a harmozização correlata nas descrições de cada um, traz já no seu primeiro capítulo a introdução, explanando o que vem a ser discutido, buscado e encontrado no trabalho.

No segundo capítulo os ojetivos, geral e específicos, com os quais serão norteados o desenrolar da busca científica.

Por fim, no terceiro capítulo, a investigação arrolada como revisão de literatura com tópicos e subtópicos, com os quais darão ao trabalho argumentos facto-jurídicos introjetados pela literatura encontrada acerca do eminente trabalho, a fim de colaborar com a propagação científico-acadêmica.

2 CONCEITO DE DADOS

Tércio Sampaio Ferraz Júnior nas suas propedêuticas lições, e, não é demasiadamente forçoso denotar que o ilustre jurista catedrático paulistano que é, citando Ives Gandra Martins, Celso Bastos e Manoel Gonçalves Ferreira Filho, esclarece:

> Em primeiro lugar, a expressão 'dados' manifesta uma certa impropriedade (Celso Bastos & Ives Gandra, p. 73). Os citados autores reconhecem que por 'dados' não se entende o objeto de comunicação, mas uma modalidade tecnológica de comunicação. Clara, nesse sentido, a observação de Manoel Gonçalves Ferreira Filho (p. 38): *"Sigilo de dados. O direito anterior não fazia referência a essa hipótese. Ela veio a ser prevista, sem dúvida, em decorrência do desenvolvimento da informática. Os dados aqui são os dados informáticos (v. ines. XIV e LXXII)". A* interpretação faz sentido. O sigilo, no inciso XII do art. 5º, está referido à *comunicação,* no interesse da defesa da privacidade. Isto é feito, no texto, em dois blocos: a Constituição fala e m sigilo *'da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas".* Note-se, para a caracterização dos blocos, que a conjunção *e* une correspondência com telegrafia, segue-se uma vírgula e depois, a conjunção de dados com comunicações telefônicas. Há uma simetria nos dois blocos. Obviamente o que se regula é *comunicação* por correspondência e telegrafia, *comunicação* de dados e telefonia. O que fere a liberdade de omitir pensamento é, pois, entrar na *comunicação* alheia, fazendo com que o que devia ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de u m terceiro. Se alguém elabora para si um cadastro sobre certas pessoas, com informações marcadas por avaliações negativas, e o torna público, poderá estar cometendo difamação, mas não quebra sigilo de dados. Se estes dados, armazenados eletronicamente, são transmitidos, privadamente, a um parceiro, em relações mercadológicas, para defesa do mercado, também não estará havendo quebra de sigilo. Mas se alguém *entra nesta transmissão,* como um terceiro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque u m a das partes lhe cede o acesso indevidamente, estará violado o sigilo de dados (FILHO e BASTOS, 1990).

Nesse escólio, ainda discorrendo sobre a temática, fazendo as devidas caracterizações acerca do que vem a ser dados, os renomados autores, com maestria, e não é demasiado dizer, brilhantismo, arrematam com o seguinte trecho, flexibilizando a celeuma:

> A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) *privativa* é que não pode ser violada por sujeito estranho à comunicação (FILHO e BASTOS, 1990).

Doutra banda, se alguém, (FILHO e BASTOS, 1990) "não por razões profissionais, ficasse sabendo legitimamente de dados incriminadores relativos a uma pessoa, ficaria impedido de cumprir o seu *dever* de denunciá-los"!

3 REVISÃO DE LITERATURA

Patricia Peck, *expert* no assunto e demasiadamente salutar nas afirmações, como excelente doutrinadora no assunto que é, vem com a seguinte lição escorreita acerca do tema com a denotação:

> O crime virtual é, em princípio, um crime de meio, utiliza-se de um meio virtual. Não é um crime de fim, por natureza, aquele cuja modalidade só ocorra em ambiente virtual, à exceção dos crimes cometidos por '*cracker'*, mas de algum modo podem ser enquadrados na categoria de estelionato, extorsão, falsidade ideológica, fraude, entre outros.
> Com o intuito de abordar fatos ainda não explorados ou já explorados, mas que ainda necessitam de uma abordagem técnica e metodológica de profissionais, estudantes, técnicos e outros investigadores que empenhem na descoberta de fatos omissos, escusos para um melhor entendimento do que vem a ser essa prática criminológica que cresce a cada dia não só em lugares restritos, mas em todo o mundo e agora também no Brasil que vez ou outra está na mídia com casos que não se têm a devida providência e tornam mais e mais frequentes (*PECK, 2004, p.216).*

A internet surge apenas como facilitador, principalmente pelo anonimato que proporciona. Portanto, as questões quanto ao conceito de crime, delito, ato e efeito são as mesmas, quer sejam aplicadas para o Direito Penal, quer para o Direito Digital. As principais inovações jurídicas trazidas no âmbito digital se referem à territorialidade e à investigação probatória e há necessidade de tipificação penal de algumas modalidades que devido a suas peculiaridades merecem ter um tipo penal próprio.

Com a finalidade de pesquisar a fundo e ver os lados de que tratam os crimes em rede, os pesquisadores, que já se manifestaram acerca do assunto. No decorrer deste projeto, analisaremos algumas soluções apresentadas pela doutrina, no sentido de suprir as lacunas legais em matéria de criminalidade informática.

Empenhados nesta dicotomia, crime e internet, o Ministério Público Federal tem realizado campanhas com o fito de desmembrar quem está por trás de sistemas computacionais, inescrupulosamente, cometendo verdadeiros assombros contra a ordem jurídica nacional e transnacional, baseando o *parquet,* no direito comparado, detectaram verdadeiros devaneios criminais, sobretudo em bancos, é o que se lê:

> Serão tomados como parâmetros, as reformas realizadas no código penal espanhol, assim como as tentativas da legislação brasileira. Contudo, centrar-nos-emos na análise dos crimes contra o patrimônio, tanto naqueles meramente de apropriação, como naqueles movidos por um ânimo de fraude. É nesse âmbito que os problemas causados pelas condutas abusivas perpetradas a invasões a sites de bancos mais se acentuam (BRASIL, 2005.)

De relevante ensinamento crítico, Liliana Minardi pondera com eloquência e magnitude a celeuma levantada e seus reflexos, consequências que cercam o sistema jurídico brasileiro ao afirmar:

> Assim, além de apontarmos a problemática concernente a essas condutas, principalmente no que se refere à utilização abusiva de informações secretas em caixas eletrônicos, além das divulgações ilícitas feitas por pessoas não autorizadas para tanto.
> O problema jurídico dos crimes virtuais, além da falta de legislação específica, é a raridade de denúncias e, pior, o despreparo da polícia investigativa e de perícia para apurá-las. Embora já seja possível fazer boletins de ocorrências pela internet, são poucas as equipes e profissionais preparados para a investigação de um crime virtual (*PAESANI, 2000, p.128).*

3.1 O crime além fronteira

Como num velho filme de faroeste, onde os pistoleiros mais rápidos daquelas terras em que inicialmente não existia a lei acabavam sendo contratados pelas comunidades que ali queriam estabelecer-se, para se tornarem seus xerifes, grandes "hackers" são contratados por corporações e governos para prestarem seus serviços. Mas é importante ressaltar que a prestação de serviço, desde que não ilegal, não é crime. O crime se configura na invasão não autorizada no furto de informações confidenciais, no acesso não permitido, independentemente do uso de senha autorizada.

Além da questão de prova, a questão da territorialidade no âmbito de crimes digitais é a que mais gera controvérsias. O Direito Criminal está sempre submetido a um determinado território nacional – o que extrapola esse território está sujeito à existência ou não de acordos entre os países envolvidos. Uma investigação bem feita pode não chegar à punição do crime e execução da pena, se for detectado que o criminoso opera de outro país e não for conseguida a extradição[1] ou seu julgamento no país de origem.

[1] "É o ato pelo qual um Estado entrega um indivíduo, acusado de um delito ou já condenado como criminoso, à justiça de outro, que o reclama, e que é competente para julgá-lo e puni-lo." A CF veda a concessão de extradição do estrangeiro por crime político ou de opinião; veda a extradição do brasileiro nato de modo absoluto; e, no caso do brasileiro naturalizado é permita a extradição desde que por crime anterior à naturalização e ou por tráfico de entorpecentes (SILVA, 2003).

Liliana Minardi enfatizando ainda mais a gravidade tecnológica expõe:

> O impacto provocado pelas tecnologias informáticas nos anos oitenta não se apresenta hoje com a mesma intensidade. Na atualidade, o uso da informática é praticamente imprescindível para o desenvolvimento das atividades na sociedade contemporânea. Todavia ainda estamos ante um fenômeno criminológico em constante evolução, pois assim é o comportamento das tecnologias informáticas. Ao mesmo tempo em que estas proporcionam desenvolvimento econômico e tecnológico, inúmeras modalidades de condutas ilícitas são praticadas através da sua indevida utilização (PAESANI, 2000, p 132).

O marco inicial da delinquência informática foi a introdução e a rápida difusão dos microcomputadores na sociedade.

Os primeiros casos que vieram à tona, e que mantém relação com alguns dos abusos cometidos em caixas eletrônicos, foram os ataques realizados em aparelhos automáticos.

Em consequência, observamos um crescimento simultâneo da difusão e vulnerabilidade dos sistemas informáticos. Essa característica da informática como meio de comunicação e de comercialização de massas gera novos desafios ao Direito Penal, com consequências um tanto problemáticas.

Advogados especialistas na área de informática alegam que, além da aprovação de projetos de lei que dispõem sobre a matéria, será necessário adaptar o ante projeto de lei que altera dispositivos da parte especial do Código Penal Brasileiro (BRASIL, 1940) aos crimes comuns praticados por meio de computadores, e, finalmente, constituir uma comissão compostas de juristas e técnicos em computação, a fim de ser elaborado um código de informática.

Vários obstáculos são enfrentados na averiguação dos dados estatísticos relacionados com o cometimento de crimes. No que diz respeito à criminalidade informática, podemos destacar fatores como a zona escura, o caráter transfronteiriço, a imaterialidade dos procedimentos informáticos, entre outros. Esses elementos estão interligados, formando um núcleo central de problemas próprios desse tipo de delinquência. Impedindo uma efetiva orientação legislativa, no sentido de punir determinadas condutas, como também pela escassez de denúncias por parte das vítimas.

Visto do âmbito social, as autoras se complementam, porém deixam apenas as condutas criminológicas à luz do Direito, sem, no entanto, preocuparem-se com a correta utilização do indivíduo com os meios digitais. Pois facilitam a invasão de dados

secretos sem um cuidado devido com a exposição. Muitas vezes, básicos cuidados que não se devem fazer na rede mundial como a não proteção de e-mails e senhas.

Ao contrário de Patricia Peck (2004), Liliana Minardi (2000) escorreita que os crimes não são meios, mas sim, consequências da rápida propagação e incremento econômico-social, dos quais a sociedade se apropriou para facilitar suas atividades cotidianas, que reduzem tempo e espaço. Com a tecnologia, facilitou bastante e acelerou suas objetivações.

As questões espaço-temporais devem ser solucionadas com base nos princípios adotados em cada país. Para tanto é necessária uma harmonização internacional do Direito Penal no sentido de evitar conflitos de competência. O Código Penal Brasileiro adota o princípio da territorialidade[2], aplicando-se, assim, aos crimes cometidos dentro do território nacional. A problemática que se apresenta é saber se o conceito de território nacional aplica-se à criminalidade informática, de transcendência ultra--nacional. A internet constitui um meio de comunicação e de transmissão de informações informatizadas e de acesso público, tornando complexa a determinação da competência em caso de ilícitos que afetam outros ordenamentos jurídicos.

3.2 Convenção de Budapeste

3.3 Breve relato

A Convenção de Budapeste é fruto da Convenção de Havana de vinte fevereiro de mil novecentos e vinte e oito.

Foi promulgado aqui no Brasil pelo Decreto-Lei n° 18.871, de 13.08.1929. Países que o subscreveram: Brasil, Cuba, República Dominicana, Haiti, Panamá, Costa Rica, Nicarágua Honduras, Salvador, Guatemala, Chile, Bolívia, Equador, Peru e Venezuela. São, portanto, ao todo, 15 (quinze) países inclusive 6 (seis) da América do Sul (Blogspot, 2008).

Não houve quase divergência entre os signatários, porque cada país escolheu o seu elemento de conexão e exclui o artigo que melhor lhe aprouvesse. O Brasil optou pela não-aplicação dos arts. 52 e 54, uma vez que tratam de matéria atinente ao divórcio. Hoje, tudo isto está superado. O Brasil já traz, na sua legislação, o instituto do divórcio (Blogspot, 2008).

[2] Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional (ANGUER, 2016. p, 359).

Tem o Código Bustamante 427 artigos assim distribuídos por assunto, ou seja, tratam primeiramente de um título preliminar, contendo regras gerais. A seguir, referem-se à matéria de Direito Civil Internacional, Direito Comercial Internacional, Direito Penal Internacional e, por último, Direito Processual Internacional (Blogspot, 2008).

Kleber Assunção Do Espirito Santo, em Trabalho de Conclusão de Curso, intitulado "crimes cibernéticos", demonstrou a preocupação que nos é afeta, haja vista a complexidade do tema e o interesse por parte do legislador em inovar acerca da reprimenda, para poder, com ela (legislação), combater os delitos ora em estudo, destarte:

> Com a explosão da globalização através do meio cibernético, o crescimento dos crimes virtuais ou crimes cibernéticos foi o estopim para a Europa se unir e criar a Convenção de Budapeste ou Convenção sobre o Cibercrime. Sendo criada em 2001 na Hungria, pelo Conselho da Europa, a Convenção de Budapeste está em vigor desde 2004, após a ratificação de cinco países, engloba mais de 20 países e tipifica os principais crimes cometidos na Internet.
> Traz em seu preâmbulo priorizando uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional e reconhecendo a necessidade de uma cooperação entre os Estados e a indústria privada. Ainda em seu escopo inicial, ressalta o obrigatório respeito: I - à Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa em 1950; II - ao Pacto Internacional sobre os Direitos Civis e Políticos da ONU em 1966; à III - Convenção das Nações Unidas sobre os Direitos da Criança em 1989; e IV - à Convenção da Organização Internacional do Trabalho sobre as piores formas do trabalho infantil em 1999. Bem com o Tratado de 2001 que possui quatro capítulos são eles: Terminologia, Medidas a tomar a nível nacional, Cooperação internacional e Disposições finais, assim como 48 artigos encorpados num texto de fácil compreensão, sobretudo porque não traz informações técnicas. O que chama a atenção na Convenção é que ela se alto define: Capítulo-I, diz respeito aos cibercrimes, tipificando-os como infrações contra sistemas e dados informáticos; Capítulo-II, Título 1, fala de infrações relacionadas com computadores; Capítulo-II, Título 2, faz referência as infrações relacionadas com o conteúdo, pornografia infantil; Capítulo-II, Título 3, diz respeito a infrações relacionadas com a violação de direitos autorais e por fim o Capítulo-II, Título 4, todos dentro do Direito Penal Material. Quanto às matérias do Direito Processual são as que seguem no âmbito das disposições processuais, condições e salvaguardas, injunção, busca e apreensão de dados informáticos armazenados, enfim um rol de conteúdo (SANTO, 2015, ps. 32-34).

Há de se falar que o Brasil ratificou, até a presente data, apenas cinco das convenções elaboradas pela Conferência Especializada Interamericana de Direito Internacional Privado. O tratado mais importante da espécie, ratificado pelo Brasil, foi o Código Bustamante, de 20 de Fevereiro de 1928, Havana, Cuba, promulgado pelo Decreto nº 18.871, de 13 de Agosto de 1929. O Código Bustamante foi ratificado por

quinze países sul-americanos. Vários países, entretanto, declararam reservas quanto à aplicação da convenção (BRASIL, 2015).

O Brasil optou pela não-aplicação dos arts. 52 e 54, uma vez que tratam de matéria atinente ao divórcio. Hoje, tudo isto está superado. O Brasil já traz, na sua legislação, o instituto do divórcio. Tem o Código Bustamante 427 artigos assim distribuídos por assunto, ou seja, tratam primeiramente de um título preliminar, contendo regras gerais. A seguir, referem-se à matéria de Direito Civil Internacional, Direito Comercial Internacional, Direito Penal Internacional[3] e, por último, Direito Processual Internacional (BRASIL, 2015).

Fruto de longos debates, o Código de Bustamante surgiu para normatizar relações quase que exclusivamente privadas ou subjetivas, destinadas a pacificação das relações entre Estados ou para regular o comércio internacional. Hoje precisa ser repensado diante dos desafios globais surgidos no final do século passado e com conseqüências que serão profundamente sentidas ao longo de todo o século XXI (Ibidem).

3.4 Jurisdição internacional

A título eminentemente informativo, é de se notar o conceito de jurisdição, para tanto mister se faz as considerações emprestadas por analogia do Código de Processo Civil para o arcabouço Processual Penal, vez ser menos debatida essa matéria adjetiva no curso do direito substancial penal.

Muito embora não seja amplamente debatida na seara processual penal, valem os ensinamentos de nossos doutos doutrinadores a respeito, lecionam "ser o poder atribuído, constitucionalmente, ao estado para aplicar a lei ao caso concreto, compondo litígios e resolvendo conflitos" (NUCCI, 2010, p. 243). Ainda nessa escorreita, o *expert* continua "é uma função estatal inerente ao poder-dever de realização de justiça,

[3] O Código de Bustamante dita as regras concernentes à aplicação do direito penal e processual penal como exemplos os arts. 340, 341, 342 e 343 do livro IV, título II, capítulo III, do referido código.
"Art. 340. para conhecer dos e faltas e o julgar, são competentes os juízes e tribunais do Estado contratante em que tenham sido cometidos.
Art. 341. A competência estende-se a todos os demais delitos e faltas a que se devia aplicar a Lei penal do Estado, conforme as disposições deste código.
Art. 342. Compreende, além disso, os delitos ou faltas cometidos no estrangeiro por funcionários nacionais que gozem do benefício da imunidade.
Art. 343. Não estão sujeitos, em matéria penal, à competência de juízes e tribunais dos Estados contratantes, as pessoais e os delitos ou infrações que não são atingidos pela lei penal do respectivo Estado" (ANGUER, 2016, p. 1919).

mediante atividade *substitutiva* de agentes do poder judiciário – juízes e tribunais -, concretizada na aplicação do direito objetivo a uma relação jurídica, com a respectiva declaração, e o consequente reconhecimento, satisfação ou assecuração do direito subjetivo material de um dos titulares das situações – ativa e passiva – que a compõem" (Ibdem, 2010, p. 243).

"Em suma, todo Juiz, investido na sua função, possui jurisdição, que é a atribuição de compor os conflitos emergentes na sociedade, valendo-se da força estatal para fazer cumprir a decisão compulsoriamente. Detendo o Estado o monopólio da distribuição da justiça, na esfera penal, evitando-se, com isso, os nefastos resultados da autotutela, que podem tender a excessos de toda ordem, gerando maior insegurança e revolta no seio social, exerce o poder judiciário a jurisdição em caráter substitutivo às partes" (ibdem, 2010, p. 244).

Nessa toada aduz Araújo (2008, p. 221), "a jurisdição é um dos elementos da soberania do Estado, e só a este compete determiná-la". Sendo assim, constitui princípio que aos Estados cabe determinar o limite da sua jurisdição, bem como sua organização judiciária. E, devido ao não interesse dos Estados de avançar indefinidamente em sua área de jurisdição sem que possa tornar efetivo o julgamento feito pelo seus tribunais, é que, aos países, de forma soberana, cabem definir os limites da sua jurisdição, encontrando, como lembra Wambier (2005, p. 93), barreiras naturais nas jurisdições de outros Estados. E, como lembra Diniz (2002, p. 329) "nenhum Estado soberano e independente exercerá jurisdição sobre outro país igualmente soberano e independente".

Sendo assim, a cada Estado cabe definir a sua organização jurídica, se responsabilizando pela definição de recursos cabíveis, formas de processo, bem como outros meios judiciais, sempre atento, como chama atenção Gonçalves (2005, p. 46), que, o juiz brasileiro não possui jurisdição em outros territórios, exatamente por dever respeitar a soberania dos outros países.

Os países, entretanto, como esclarece Dinamarco (2005, p. 362) não a determinam por bondade, ou em nome de boas relações internacionais, mas por três motivos simples:

> (a) impossibilidade ou grande dificuldade para cumprir em território estrangeiro certas decisões dos juízes nacionais, (b) a irrelevância de muitos conflitos em face dos interesses que ao Estado compete preservar e (c) a conveniência política de manter certos padrões de recíproco respeito em relação a outros Estados.

E, por isso, o Brasil definiu o alcance de sua jurisdição nos art. 88 e 89[4] do Código de Processo Civil, mas não deixou de determinar, também, em seu artigo 90 a impossibilidade da aplicabilidade da litispendência internacional.

E, neste sentido explica Moreira (1977, p. 53) que o artigo 90[5] teve a intenção de demonstrar a irrelevância dos efeitos dos processos intentados no estrangeiro para a nossa justiça, e, ainda completa que se a lide pender ou não perante juiz de outro Estado, nada importa aqui.

3.5 Litispendência

A litispendência, conforme explicita Calmon de Passos (1998, p. 265), ocorre quando os mesmos sujeitos intentam duas ações visando o mesmo bem da vida e pela mesma causa, sendo assim exigida, para sua caracterização, uma tríplice identidade, quais sejam a identidade de sujeitos, de pedido e de causa de pedir. Trata-se de um instituto que deve ser alegado antes de discutir o mérito, refere o art. 301[6] do Código de Processo Civil Brasileiro.

E assim, percebe-se, com nitidez, como opina Figueira Junior (2001, p. 233), que a possibilidade de litispendência tem o condão de evitar julgamentos contraditórios sobre a mesma lide. Bem como opõe-se que ações idênticas tramitem simultaneamente, sendo que, em tese, deveriam levar os litigantes para o mesmo resultado.

Completa Figueira Junior (2001, p.230) que "a litispendência é um pressuposto processual objetivo de validade extrínseco à relação processual que se caracteriza pela propositura de ação idêntica em relação a outra demanda, precedentemente ajuizada, e que ainda se encontra em tramitação", considerando a litispendência como um dos mais

[4] Atuais arts. 21 e 23, respectivamente do NCPC.
[5] Atual art. 24 do CPC, redação dada pela Lei 13.105/15.
[6] Atual art. 337 do CPC redação dada pela Lei 13.105/15.

importantes institutos jurídicos do processo, apresentando-se não só como pressuposto de validade, mas também, devido aos diversos efeitos que produz.

Sendo assim, percebe-se claramente que o instituto da litispendência visa evitar que duas ações idênticas tramitem simultaneamente,sendo que deveriam levar os litigantes para o mesmo resultado.

E assim, Greco Filho (2010, p. 217) identifica a litispendência internacional quando em tribunais de países diferentes, com jurisdições e ordenamentos jurídicos distintos, corre a mesma ação judicial, e, por isso, ele, assim como Alvim (1977, p. 25), defendem a prevalência de tratado internacional perante o artigo 90 do Código de Processo Civil.

Litispendência internacional e o Código de Bustamante. Acontece que, da mesma forma que o Código de Processo Civil define a possibilidade de alegação da litispendência em âmbito nacional, este, em seu artigo 90, define sua inaplicabilidade quando se trata de sistemas jurídicos internacionais. O Brasil, entretanto, homologou a Convenção de Direito Internacional de Havana, conhecida popularmente como Código Bustamante, através do decreto 18.871 de 13 de agosto de 1929.

Esta alegação, porém, deve ser feita apenas quando a sentença de um dos Estados deverá produzir efeito de coisa julgada em outro. Restando claro que só é possível a aplicação da litispendência quando se trata de competência concorrente entre os países, e ainda, como qualquer tratado de direito internacional, a aplicação somente é válida para os países signatários deste tratado internacional.

O que se nota dos julgados internacionais, entretanto, é o não acolhimento da litispendência, sob alegação de necessária aplicação do artigo 90 do Código de Processo Civil.

E, assim é simplesmente ignorada a existência do Código Bustamente, gerando relevantes impactos que causam efeitos recíprocos nas relações jurídicas internacionais, como aduz Jo (2001, p. 207), pois atualmente o sistema de processo civil internacional está relacionado diretamente à competitividade internacional dos países. E, por isso, Alvim (1977, p. 25) defende a exceção de litispendência quando o país da jurisdição estrangeira for signatário de tratado internacional, o qual prevalecerá diante do artigo 90 do Código de Processo Civil. Já, Greco Filho (2010, p. 225) defende a possibilidade de alegação do instituto da litispendência apenas para os países signatários do Código de Bustamante, lembrando que necessariamente os dois países tem que ser competentes

para julgar a causa e, que, não será permitida caso seja caso de competência exclusiva brasileira.

3.6 Evolução legislativa

Preocupados acerca da ratificação da Convenção de Budapeste, deputados se reuniram na data de sete de agosto de 2013, na Câmara dos Deputados em Brasília na Comissão de Relações Exteriores e de Defesa Nacional – CREDN, cobrando a adesão do Brasil pela supra citada Convenção (BRASIL, 2013).

“Os deputados Eduardo Azeredo (PSDB-MG) e Claudio Cajado (DEM-BA) querem que os ministros da defesa, Celso Amorim, e das relações exteriores, Antonio Patriota, forneçam informações sobre a adesão do Brasil à Convenção Internacional sobre o *cibercrime* – Convenção de Budapeste – e que medidas o país tem adotado para melhorar a sua segurança digital” (BRASIL, 2013).

De acordo com Eduardo Azeredo, "a Convenção de Budapeste é hoje o principal tratado internacional de direito penal e processual que define de forma harmônica os crimes praticados por meio das tecnologias da informação e suas formas de persecução" (BRASIL, 2013).

Claudio Cajado lembrou que "a incidência dos crimes praticados mediante o uso de tecnologias de informação e comunicação vem crescendo exponencialmente no Brasil e no mundo. Os fatos há muito evidenciam que é urgente a tomada de providências no âmbito interno, com a adoção de leis que visam o combate e a punição dos chamados *cibercrimes* e de medidas que reforçam a segurança digital de pessoas, empresas e governos" (BRASIL, 2013).

Atualmente, 40 países integrantes do Conselho da Europa, o Canadá, a África do Sul, o Japão e os Estados Unidos são signatários da Convenção de Budapeste. Na América do Sul, apenas Chile e Colômbia aderiram.

"As recentes denúncias de monitoramento norte-americano no Brasil evidenciam, para além de qualquer interferência, que o ciberespaço brasileiro está desprotegido, vulnerável a todo tipo de invasão", explicou Azeredo (BRASIL, 2013).

“Os ministros terão de responder sobre as providências tomadas no sentido de promover a adesão do Brasil à Convenção de Budapeste, quando isso irá ocorrer e quais as demais medidas adotadas para fortalecer a segurança digital do país, não apenas no

âmbito interno, mas principalmente no tocante às questões transfronteiriças" (BRASIL, 2013).

3.7 Histórico e conceitos da internet e das ameaças trazidas pela evolução dos recursos tecnológicos

3.7.1 Internet

Positivado no nosso ordenamento, o conceito de internet está previsto no art. 5º, I da lei 12.965/14, conhecido como Marco Civil da Internet e está exposado como " o sistema constituído de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes" (BRASIL, 2014).

O antecedente histórico mais remoto do surgimento da informática ocorreu em 1946, quando foi construído o primeiro computador digital, denominado computador integrador numérico electrônico (*Electronic Numerical Integrator and Computer* – ENIAC) (WENDT; JORGE, 2012, p. 5).

No entanto, o marco inicial do desenvolvimento tecnológico propriamente dito, e considerado assim por muitos autores, teria se dado em 1957, quando, o então presidente dos Estados Unidos, John Kennedy, em contrapartida ao lançamento do primeiro satélite artificial pela antiga União Soviética, prometeu enviar um americano para a lua e criar um sistema de defesa à prova de destruição. Dessa forma, tendo em vista tal objetivo, foi criada a Agência de Investigação de Projetos Avançados (*Advanced Research Project Agency* - ARPA) (WENDT; JORGE, 2012, p. 23).

Em 1958 foi criada a Administração Nacional da Aeronáutica e do Espaço (*National Aeronautics & Space Administration* - NASA), enfraquecendo o sistema da ARPA. Assim, o foco neste momento histórico passou a ser a computação interativa e os sistemas de tempo compartilhado (que era, basicamente, o início do que conhecemos hoje como sistemas operacionais, como o *Windows* e o *Linux*, por exemplo) (WENDT; JORGE, 2012, p. 6).

Com o passar dos anos, consolidou-se a ideia de se criar uma rede capaz de integrar computadores que estivessem distantes. Por meio dessa rede seria possível a transmissão de dados. Assim, foi criada a Agência de Pesquisas em Projetos Avançados

na Rede (Advanced Research Projects Agency Network - ARPANET), que é a tecnologia base do que conhecemos hoje por internet. É o nascimento da internet, pois até então, o que existiam eram sistemas isolados (*host's*) que processavam informações e apresentavam respostas de forma ágil e certa. (CRUZ, 2004, p. 19).

A primeira conexão internacional da ARPANET foi realizada em 1973, interligando a Inglaterra e a Noruega. No final dessa década, a ARPANET substituiu seu protocolo de comutação de pacotes, denominado Protocolo de Controle de Rede (*Network Control Protocol* - NCP), para o Protocolo de Controle de Transmissão/Protocolo de Interconexão (*Transmission Control Protocol/Internet Protocol* - TCP/IP), que é a linguagem básica de comunicação ou protocolo da rede mundial de computadores, ou seja, o protocolo de transmissão de dados pela internet, utilizado hoje. Assim, tal protocolo é um conjunto de camadas responsáveis por determinadas tarefas, a exemplo da comunicação entre o servidor de internet e computador local, que só pode ser feita com base na configuração TCP/IP (WENDT; JORGE, 2012, p. 7).

Nesse contexto, somente em 1986 a ARPANET começou a ser chamada de internet, com a criação da Teia Mundial (*World Wide Web* - WWW), que é um conjunto de documentos em hipermídia, da Linguagem de Marcação de Hipertexto (*HyperText Markup Language* - HTML), que é uma linguagem para a produção de páginas de internet, visualizados através de programas de computador chamados de *browsers* (programas para navegação pela internet, como o *Internet Explorer* ou o *Firefox*). Tal evolução trouxe como grande vantagem a melhoria na interface gráfica. Agora era bem mais atraente aos usuários, permitindo a interação com figuras e sons. (DAVID, 2011, p.8; POLEGATTI; KAZMIERCZAK, 2012, p. 3).

No final da década de 1990 a internet começou a se popularizar. Surgia, desse modo, a necessidade de entender aquele novo espaço social, o ciberespaço. (SOUZA; PEREIRA, 2009, p. 2).

Um dos efeitos colaterais indesejados dessa revolução tecnológica e social é o cibercrime e, com ele, as indagações de como combatê-lo, pois era um meio totalmente desconhecido à época (DAVID, 2011, p.8; POLEGATTI; KAZMIERCZAK, 2012, p. 5).

No Brasil, em 1965, foi criado o Serviço Federal de Processamento de Dados e a Empresa Brasileira de Telecomunicações, vinculada ao Ministério das Comunicações, também recém-criado. Contudo, o primeiro computador brasileiro somente foi fabricado

em 1972, pela Universidade Federal de São Paulo (USP) (WENDT; JORGE, 2012, p. 8).

Em 1992 foi criada a Secretaria de Política de Informática. Nesse mesmo ano foi implementada a primeira rede conectada à internet. Não existia interface interativa, tal como conhecemos hoje. Os usuários conectados a essa rede conseguiam apenas trocar e-mails, o que já era um avanço muito significativo. No entanto, somente em 1995 a internet foi disponibilizada de forma comercial, com uma velocidade que não ultrapassava a marca de 9,6 quilobits por segundo (Kbps). (CHAGAS, 2003, p. 9).

3.7.2. Ameaças virtuais

Os primeiros casos de uso do computador para a prática de delitos datam da década de 50. Os crimes virtuais, ou cibercrimes, que são quaisquer atos ilegais onde o conhecimento especial de tecnologia de informática é essencial para as suas execuções, consistiam basicamente, nessa época, em programas que se auto-reaplicavam, ou seja, defeituosos. Não houve, num primeiro momento, a intenção de se criar um vírus. Na verdade, o que ocorreu foi uma falha na compilação de determinado código fonte (instrução de comandos que faz um programa funcionar de determinada forma) gerando algum tipo de transtorno, o que se assemelha ao resultado danoso que o vírus que conhecemos hoje proporciona. (SZNICH, 1995; WENDT; JORGE, 2012, p. 9).

Contudo, os antecessores do que conhecemos hoje por códigos maliciosos datam da década de 1960. Tudo começou quando um grupo de programadores desenvolveu um jogo chamado *Core Wars*[7]. Tal jogo era capaz de se reproduzir cada vez que era executado, sobrecarregando a memória da máquina do outro jogador. Os inventores

[7] CoreWar é um jogo aonde jogadores (programadores) escrevem programas e os colocam em uma arena virtual que é na verdade uma parte da memória do computador, depois de carregados, os jogadores não podem interferir em suas criações, apenas observá-las se desenvolvendo e executando as funções para qual foram programadas. O objetivo de cada programa é ao mesmo tempo sobreviver no ambiente hostil da memória e "matar" os outros programas, porém não existem armas para isso, existem maneiras muito mais inteligentes de fazê-lo. Um programa pode lançar "bombas" de código inválido para destruir seu oponente (divisão por zero, por exemplo), reprogramá-los para trabalharem para você ou até capturá-los e confiná-los em sua própria armadilha obrigando-os lhe ajudar a aniquilar o restante dos inimigos, seu programa poderá se multiplicar pela memória se auto copiando, assim, se uma cópia é destruída, ainda restam outras. Poderá infectar código inimigo como um vírus se aproveitando das rotinas escritas por outros programadores para seu benefício. Seu programa poderá manter uma rotina de auto reparo para consertar danos causados por ataques inimigos e até sofrer metamorfoses mudando de estratégia dependendo da necessidade <https://sites.google.com/site/rodrigosetti/corewars>. Acesso em: 12/01/2017.

desse jogo também criaram o que seria um tipo de programa aproximado do que conhecemos hoje por antivírus, capaz de destruir cópias geradas por esse jogo (WENDT; JORGE, 2012, p. 9).

Não existe uma posição pacífica sobre o surgimento do primeiro vírus de computador. Sabe-se que em 1986 surgiu o primeiro cavalo de Tróia de que se tem notícia, o *PC Write*, o qual se apresentava como um editor de textos, mas, quando executado, corrompia os arquivos do disco rígido do computador (que consiste em um disco magnético de metal com a função de suporte físico para os dados gravados por meio de pontos magnetizados) (MONTEIRO NETO, 2008, p. 145; WENDT; JORGE, 2012, p. 11).

Quanto ao surgimento do primeiro antivírus também não existe uma posição pacífica. Muitos entendem que foi criado em 1988, por Denny Yanuar Ramdhani, em Bandung, Indonésia, e tinha a finalidade de imunizar o sistema computacional contra o vírus *Brain*, entendido por alguns como o primeiro vírus criado (WENDT; JORGE, 2012, p. 11).

Hoje, existem diversos tipos de vírus, cada qual responsável por um resultado diferente e classificados nas seguintes modalidades: vírus de *boot* – considerado precursor de todos os tipos de vírus, tendo surgido no final da década de 1980, agindo de forma a se fixar na partição de inicialização do sistema (todo disco responsável em armazenar as informações relativas ao sistema operacional possui um setor destinado à inicialização) – vírus *time bomb* – tem como característica a determinação prévia da data de sua deflagração – *worm* – conhecido também como verme reside na memória ativa do computado e se replica automaticamente – *botnets* – que se caracterizam por computadores infectados por arquivos que possibilitam o controle remoto do computador da vítima – *deface* – desfiguram sites ou perfis de redes sociais – cavalo de Tróia – permite o acesso de forma remota ao computador da vítima com o intuito de obter dados confidenciais e envio ao computador do criminoso – *keylogger* – monitora as informações digitadas pela vítima – *hijacker* – sequestra o navegador de internet da vítima e a faz navegar por sites diferentes daqueles digitados – *rootkit* – programas que permanecem ocultos no computador e podem ser instalados de forma local ou remota – *sniffer* – monitoram todo o tráfego da rede, interceptando e possibilitando a análise de dados – *backdoor* – deixa o computador vulnerável para ataques ou invasões – *hoax* – chamados também de boatos cibernéticos, consistindo em falsas histórias divulgadas pelo meio digital, causando transtornos para a vítima – e *phishing scam* – constituindo-

se na conduta daquele que pesca informações sobre o usuário do computador (JORGE, 2011, ps. 23-39).

Um fator ainda a se considerar é o elevado número de spams – que são mensagens não solicitadas e enviadas em massa – muito elevado. Tal fato é preocupante, tendo em vista que muitos crimes virtuais utilizam-no para difundir códigos maliciosos (CERT.br, 2012).

De um modo geral, as condutas indevidas praticadas por computador podem ser divididas em crimes virtuais e ações prejudiciais atípicas. Estas causam algum transtorno para a vítima, porém não existe uma previsão legal, podendo, o causador, ser responsabilizado no âmbito civil somente, como, por exemplo, casos de acesso não autorizado a redes de computadores. Já aqueles podem ser subdivididos em abertos e exclusivamente cibernéticos. Os primeiros são aqueles que podem ser praticados da forma tradicional ou por meio de computadores, como, por exemplo, casos de crime contra a honra. Os segundos somente podem ser praticados com o uso do computador ou de qualquer recurso que permita o acesso à internet, como, por exemplo, casos de *carding* (clonagem de cartão) por meio de sistema de informática (WENDT; JORGE, 2012, ps. 18-20).

Fato é que a internet tem sido utilizada para inúmeras finalidades, inclusive servindo para causar transtornos para outras pessoas. Nesse sentido, no Brasil, importante é o papel do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que está vinculado ao Comitê Gestor da Internet no Brasil, atendendo a qualquer rede brasileira conectada à internet (WENDT; JORGE, 2012, ps. 12-14).

3.8 Aspectos Constitucionais e princípios do Direito Penal relativos à sociedade da informação e ao crime virtual

A sociedade da informação surgiu a partir da facilitação no desempenho de atividades cotidianas proporcionadas pelo uso de ferramentas informatizadas. Mais do que isso: esses mecanismos eletrônicos guarnecem inúmeros bens jurídicos de suma importância para o ser humano, a exemplo da saúde, intimidade, segurança, liberdade entre muitos outros. Desse modo, a sociedade se vê vinculada às tecnologias da informação, tendo, a criminalidade, passado por esse mesmo processo. Aparecem os

crimes virtuais e, com eles, novos bens jurídicos, aos quais a ordem constitucional precisa proteger. Há um impacto da sociedade da informação na ordem constitucional, o que gera consequências na esfera penal (MONTEIRO NETO, 2008, p. 6; OLIVEIRA, 2013, p. 11).

Como reflexo de tal impacto, a Constituição, enquanto mecanismo regulador de toda a ordem política e jurídica do Estado, acabou abarcando a responsabilidade de dar contornos jurídicos à nova realidade social, cultural e econômica que surgia. Consequentemente, a Lei Suprema estendeu laços protetivos aos novos bens e valores jurídicos, resultados da chamada revolução informacional[8] (MONTEIRO NETO, 2008, p. 9).

Essa revolução deixa evidente a importância e o papel da informação. Esta se torna, então, um bem jurídico importante frente à globalização operada, principalmente, pelos meios informáticos. No pensamento de Beneyto (1997, p. 15), "para considerar-se plenamente cidadão, o homem contemporâneo precisa dispor de fontes informacionais que lhe permitam conhecer o que se passa e, em seguida, formar juízos sobre os acontecimentos".

Ainda na mesma sintonia Constitucional, concernente ao apego à Bíblia Política de 1988, expõe NETO:

> Assim, o direito à informação é um direito fundamental do homem, de forma que está vinculada à democracia moderna. A implantação dos demais direitos se materializa a partir da garantia constitucional da liberdade de informação. Mormente, é importante salientar que a ordem jurídica constitucional brasileira reservou em seu texto pétreo um Título destinado aos direitos e garantias fundamentais, ligados à ideia de pessoa humana e seus atributos de personalidade, como a liberdade, por exemplo, não podendo, o titular de tais direitos, dispor deles. (MONTEIRO NETO, 2008, p. 57, 60).

O direito à informação, que é um tipo de direito à liberdade, encontra-se previsto no *caput* do artigo 5º e em alguns de seus incisos, todos da Constituição Federal (Brasil, 1988), conforme se verifica a seguir:

---

[8] A Revolução Técnico-científico-informacional ou Terceira Revolução Industrial entrou em vigor na segunda metade do século XX, principalmente a partir da década de 1970, quando houve uma série de descobertas e evoluções no campo tecnológico. Essa nova etapa de produção está vinculada à inserção de uma enorme quantidade de tecnologia e informação.
Essa revolução, por sua vez, está ligada diretamente à informática, robótica, telecomunicação, química, uso de novos materiais, biotecnologia, engenharia genética, entre muitos outros, que recentemente fazem parte de praticamente todos os segmentos produtivos que marcam essa etapa, assim como outros fatos marcaram as revoluções industriais do passado.Essa revolução é um dos principais combustíveis para o desenvolvimento do capitalismo moderno e especialmente do processo de globalização que visa uma flexibilidade de informações, além de um acelerado dinamismo no fluxo de capitais e mercadorias. Diante dessa afirmativa, veja a seguir alguns itens indispensáveis na economia contemporânea <http://mundoeducacao.bol.uol.com.br/geografia/revolucao-tecnicocientificoinformacional.htm>. Acesso em: 21/05/2015.

"Art. 5 – Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes[9]*:*

IV – é livre a manifestação de pensamento, sendo vedado o anonimato;

V – é assegurado o direito de resposta, proporcional ao agravo, além de indenização por dano material, moral ou à imagem;

IX – é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;

XIV – é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício ao exercício profissional;

XXXIII – todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade de do Estado;

LXXII – conceder-se-á habeas data[10]*:*

a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constante de registros ou banco de dados de entidades governamentais ou de caráter público;

b) para retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;"

Todas essas garantias estão diretamente ligadas à liberdade informática, que consiste no direito que dispõe cada cidadão de utilizar-se dos instrumentos da

---

[9] Deve-se, contudo, buscar não somente essa aparente igualdade formal (consagrada no liberalismo clássico), mas, principalmente, a igualdade material, na medida em que a Lei deverá tratar igualmente os desiguais na medida de suas desigualdades.
Isso porque, no E*stado Social* Ativo, efetivador dos direitos humanos, imagina-se uma igualdade mais real perante os bens da vida, diversa daquela apenas formalizada perante a Lei.
Essa busca por uma igualdade substancial, muitas vezes idealista, reconheça-se, eterniza-se na sempre lembrada, com emoção, *O*ração *aos M*oços, de Rui Barbosa, inspirado na lição secular de Aristóteles, devendo-se tratar igualmente os iguais e desigualmente os desiguais na medida de suas desigualdades.

[10] A garantia Constitucional do *habeas data,* regulamentada pela Lei nº 9.507, de 12/11/1997, destina-se a disciplinar o direito de acesso a informações, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público, para o conhecimento ou retificação (tanto de informações erradas como imprecisas, ou apesar de corretas e verdadeiras, desatualizadas), todas referentes a dados pessoais, concernentes à pessoa do impetrante.
Essa garantia não se confunde com o direito de obter certidões (art. 5º, XXXIV, "b"), ou informações de interesse particular, coletivo ou geral (art. 5º XXXIII). Havendo recusa no fornecimento de certidões (para a defesa de direitos ou esclarecimentos de situações de interesse pessoal, próprio ou de terceiros), ou informações de terceiros o remédio próprio é o mandado de segurança, e não o *habeas data.* Se o pedido for para assegurar o conhecimento de informações relativas à pessoa do impetrante, como visto, o remédio será o *habeas data (*LENZA, 2009, p, 743*)*.

informação para informar e informar-se. Para Paesani (2006, p. 21), tal entendimento encontra respaldo no artigo 220 da Constituição Federal (BRASIL, 1988): “A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição”.

Verdade é que o dispositivo supracitado não faz restrição aos meios de difusão de informação, sendo amplo seu alcance (MONTEIRO NETO, 2008, ps. 65-66).

Mister se faz salientar que é crescente a necessidade de intervenção do Estado na fruição dos meios tecnológicos de produção e difusão da informação, como preconizado na Constituição Federal. No entanto, tal intervenção não pode ser desordenada, sob pena de ferir o princípio da intervenção mínima. Desse modo, tal intervenção deve ser focada na fiscalização e inibição de práticas nocivas (MONTEIRO NETO, 2008, p. 68).

Por conseguinte, coube ao Direito Penal a obrigação de estruturar mecanismos que viessem a prevenir e punir de forma efetiva as condutas lesivas a esses novos bens e valores jurídicos, tudo isso com respaldo nos ditames constitucionais. Tais condutas, em sua maior parte, ainda se encontram carentes de regulamentação específica, favorecendo o entendimento de que o mundo virtual é um ambiente sem leis (MONTEIRO NETO, 2008, p. 10).

No entendimento de Bobbio (1992, p. 34), "(...) o desenvolvimento da técnica, a transformação das condições econômicas e sociais, a ampliação dos conhecimentos e a intensificação dos meios de comunicação poderiam produzir mudanças na organização da vida humana e das relações sociais, criando condições favoráveis para o nascimento de novos carecimentos".

A Carta de 1988 destaca o princípio da dignidade da pessoa humana como norteador do Estado Democrático de Direito. Nesse ínterim, partindo da premissa de que o Direito Penal amolda-se ao perfil traçado pela Constituição, destacam-se princípios constitucionais-penais, como os princípios da legalidade ou da reserva legal, da anterioridade, da taxatividade e da territorialidade (MONTEIRO NETO, 2008, p. 85; SOUZA NETO, 2009, p. 58).

O princípio da legalidade ou da reserva legal é uma vertente penal do princípio da intervenção mínima e, segundo Bittencourt (2006, p. 14), "constitui uma efetiva limitação ao poder punitivo estatal".

Outro princípio constitucional do Direito Penal é o princípio da anterioridade da Lei penal, enunciado no artigo 5°, XXXIX da Constituição Federal e no artigo 1° do

Código Penal. Para que haja crime e a ele seja cominada uma pena, primeiro se faz necessário que o fato tenha sido praticado em momento posterior à criação da norma incriminadora (MONTEIRO NETO, 2008, p. 87).

Já o princípio da taxatividade impõe que a norma penal incriminadora seja exata. Ou seja, deve detalhar e pormenorizar a conduta tipificada, sob pena de perder a eficácia (Idem).

Como bem salienta NETO ao nos ensinar nos seus precisos ensinamentos principiológicos a respeito:

> O princípio da territorialidade versa sobre um dos maiores desafios para acabar com o crime virtual, por possuir, a internet, caráter global. Nesse sentido, o artigo 5º do Código Penal Brasileiro dispõe que aos crimes cometidos em território brasileiro aplicam-se a lei brasileira. Com relação aos crimes cometidos pela internet, aplica-se a lei brasileira quando o site utilizado for brasileiro. Contudo, uma exceção a este dispositivo é o princípio da extraterritorialidade, contido no artigo 7º do mesmo diploma legal. Assim, estando o agente localizado fora do país, aplica-se a lei brasileira nos casos do supracitado artigo ou nos casos em que houver acordo ou tratado nesse sentido. (SOUZA NETO, 2009, p. 58-60).

Por fim, vale ressaltar que o Direito Penal não vem acompanhando as mudanças ditadas pela explosão tecnológica, operada desde a última metade do Século XX. Tais mudanças já estão preconizadas na Constituição da República do Brasil, de forma que se buscou proteger os interesses envolvidos contra os avanços da utilização dos meios informáticos em práticas que ferem a dignidade da pessoa humana, assimilando os nuances da nova realidade social. Assim, a tutela penal de tais interesses faz-se extremamente necessária, vez que a falta de regulamentação que reprima atos que vão de encontro à nova ordem social torna instável a sustentação desse novo modelo. (SOUZA NETO, 2009, ps. 134-135).

3.9 Crimes virtuais e a legislação pertinente

3.9.1 Noções preliminares

As condutas ilícitas praticadas através do ambiente informático prejudicam a manutenção dos níveis mínimos de segurança e credibilidade necessários a qualquer negócio jurídico. Mais do que isso: interferem no cotidiano de muitas pessoas, de modo que esse novo ambiente se torna inapto para a mantença de relações sociais (MONTEIRO NETO, 2008, p. 10).

Tais condutas encontram-se sem regulamentação em sua maior parte. Assim, o mundo virtual se transforma em um verdadeiro "mundo sem leis". Esse é o entendimento de Basso e Almeida (2007, p. 123), quando afirmam que "em vários casos, as leis existentes são também aplicáveis aos novos pressupostos do contexto virtual. Em outros, uma nova regulamentação é necessária para se ter mais segurança no emprego das ferramentas eletrônicas e maior certeza quanto a validade e eficácia das transações celebradas por meio eletrônico".

O que existe atualmente é um conjunto reduzido de normas que tipificam somente algumas condutas. São tipos extremamente específicos, não sendo esse um óbice à produção de normas mais gerais (MONTEIRO NETO, 2008, p. 93).

Nesse sentido, este tópico abordará a ineficácia da normatização sobre o tema dos crimes virtuais frente aos desafios que a sociedade informatizada impõe, além de discorrer de forma mais detida sobre as Leis Ordinárias 12.735/2012 e 12.737/2012 e as implicações penais do Marco Civil da Internet, Lei 12.965/2014.

3.9.2 Ineficácia da legislação

Sem dúvida alguma, a internet é um dos meios mais eficazes para celebração de contratos. Hoje são milhares de contratos fechados por essa via, de forma que obedecem aos princípios da publicidade, da vinculação, da veracidade, da não-abusividade entre outros. No ordenamento jurídico brasileiro não existe normatização específica sobre os contratos realizados sob essa égide. No entanto, o Código Civil e o Código de Defesa do Consumidor sanam, em parte, os conflitos atinentes a respeito desse tema, faltando uma

norma específica que assegure os asseios da comunidade virtual (VEDOVATE, 2005, p. 13).

Exemplo de normas que se aplicam aos casos de contratos celebrados pelo meio virtual[11] é a aplicação do artigo 51 do CDC no combate às cláusulas abusivas e, no que tange ao direito de arrependimento, o artigo 49 (BRASIL, 1990) que assim reza: "o consumidor pode desistir do contrato, no prazo de 07 (sete) dias a contar de sua assinatura ou do ato de recebimento do produto ou serviço, sempre que a contratação de fornecimento de produtos e serviços ocorrer fora do estabelecimento comercial, especialmente por telefone ou a domicílio".

Os casos dos contratos celebrados pela via digital são mais um exemplo de que o Brasil não possui legislação específica sobre os ilícitos cometidos através desse meio. Muitas vezes, é utilizado o princípio da analogia como único meio hábil a não deixar o infrator cibernético impune. Contudo, tal princípio não é aplicável no Direito Penal, por ferir do princípio da taxatividade, sendo necessária a criação de leis mais específicas. São exemplos de normas aplicadas, com a utilização da analogia, aos crimes virtuais:

---

[11] O comercio eletrônico, é um tipo de transação realizada especificamente através de um equipamento eletrônico, como por exemplo, um computador. É, por tanto, o ato de vender e ou comprar pela internet. Bancos se utilizam desse tipo de comercio, por ser barato e seguro, para oferecer a seus cliente facilidades e ainda oferecendo shoping virtual, tornando o processo de venda mais fácil e seguro, reduzindo, inclusive, custos das empresas com largo estímulo a livre competividade O comércio eletrônico consiste na utilização de tecnologias de informação avançadas, para o aumento de eficiência nas relações comerciais e para o desenvolvimento de contratos de maneira geral, quer entre empresas, quer entre pessoas físicas.

Há que se ter em conta o relevante valor jurídico das mensagens transmitidas no comércio eletrônico, pois elas formam declarações de vontade integrantes dos contratos ou que provam a execução dos respectivos direitos e obrigações. Deste ângulo, vários problemas surgem quanto à segurança do contrato eletrônico (sua aceitação, autenticação, confidencialidade, integridade), sua publicidade nomomento da formação do contrato, a transmissão das declarações de vontade, a legitimidade representativa, a determinação do momento e do lugar da celebração do contrato e a responsabilidade civil dos contratantes (ALVIM, 1997, p. 250).

Daí surge o Direito da Informática, um novo ramo do direito voltado para uma gama de situações complexas e atípicas em relação ao tradicional ordenamento jurídico. Portanto, a evolução do comércio eletrônico trouxe aos consumidores uma variedade e quantidade imensurável de produtos e serviços oferecidos na internet.

Atualmente, é comum para grande parte dos consumidores a negociação pela rede mundial de computadores. Entretanto, as relações realizadas através da internet encontram amparo nas disposições legais vigentes, principalmente as que se referem ao Código de Defesa do Consumidor. Vale destacar que o artigo 13 do projeto de lei nº 1589/99 (OAB/SP, 1999) dispõe que “aplica-se ao comércio eletrônico as normas de defesa e proteção do consumidor”.

O fato é que, devido às transformações pelas quais a sociedade passa, surgem novas situações até então não reguladas pelo Direito, gerando várias polêmicas, às quais o ramo jurídico não pode ficar omisso, o comércio eletrônico é uma área.

Observa-se que o Código de Defesa do Consumidor (BRASIL, 1990) mostra-se plenamente capaz de regular as relações de consumo eletrônicas e que o direito de arrependimento ou prazo de reflexão se aplicam a essa nova forma de celebração contratual.

A internet disponibilizou aos consumidores a possibilidade de negociação a qualquer dia, qualquer horário e qualquer lugar do mundo. E os fornecedores, com custo reduzido, podem disponibilizar produtos em suas lojas virtuais, também disponíveis todos os dias.

Calúnia (art. 138 do Código Penal); Difamação (art. 139 do Código Penal); Injúria (art. 140 do Código Penal); Ameaça (art. 147 do Código Penal); Furto (art. 155 do Código Penal); Dano (art. 163 do Código Penal); Apropriação indébita (art. 168 do Código Penal); Estelionato (art. 171 do Código Penal); Violação ao direito autoral (art. 184 do Código Penal); Pedofilia (art. 247 da Lei nº 8.069/90 - Estatuto da Criança e do Adolescente); Crime contra a propriedade industrial (art. 183 e ss. da Lei nº 9.279/96); Interceptação de comunicações de informática (art. 10 da Lei nº 9.296/96); Interceptação de E-mail Comercial ou Pessoal (art. 10 da Lei nº 9.296/96); Crimes contra software - "Pirataria" (art. 12 da Lei nº 9.609/98) (CARNEIRO, 2012, p. 1).

Furlaneto Neto e Guimarães (2003) destacam ainda que, além das condutas descritas como crime, existem ainda aquelas consideradas ilícitos prejudiciais, as quais não são consideradas crime e não possuem legislação específica, não sendo possível, igualmente, a aplicação da analogia. São exemplos os danos praticados contra informações, os programas contidos em computador, as propagações de vírus informáticos entre outros.

Não obstante, existem normas específicas que tratam do assunto, porém, de forma a não abranger todo o campo de atuação dos criminosos cibernéticos. Assim, ainda não é suficiente o arcabouço de tipos incriminadores no ordenamento jurídico pátrio.

No entendimento de Alexandre Atheniense:

> entendo que as soluções legais a serem buscadas deverão objetivar a circulação de dados pela internet, controlando a privacidade do indivíduo sem cercear o acesso a informação. Neste sentido é necessário aprimorar nossas leis de proteção de dados, inclusive com a regulamentação da atividade dos provedores que controlam a identificação do infrator, bem como um maior aparelhamento das delegacias especializadas (ATHENIENSE, 2004, p. 1).

Nesse sentido, houve a tramitação de projetos de lei que versam sobre crimes virtuais, hoje já transformas em leis ordinárias. O mais antigo é o PL n° 84/1999, que se transformou na lei ordinária 12.735/2012. Outro projeto de lei que mereceu destaque foi o PL n° 2.793/2011, que se transformou na Lei Ordinária 12.737/2012, conhecida informalmente como "Lei Carolina Dieckman", após escândalos motivados pelo vazamento de fotos da atriz de seu computador pessoal em maio de 2012. Tal lei tipifica condutas criminosas, como a invasão de dispositivo informático alheio com a finalidade

de obter, mudar ou destruir dados ou informações, instalar vulnerabilidades entre outros (WANDERLEI, 2012, ps. 43-44).

Tais dispositivos serão vistos com mais precisão adiante.

Todas essas ações não são suficientes para coibir as práticas do infrator cibernético. Há a necessidade de regulamentação da internet, o que está sendo discutido pela sociedade atualmente, através do chamado Marco Civil da Internet. Tal instituto consiste em uma espécie de constituição da internet contendo princípios que nortearão o correto uso da internet no Brasil, além de projetar diretrizes para o Poder Público no sentido de buscar o desenvolvimento saudável da internet no Brasil (WANDERLEI, 2012, ps. 38-39).

Embora tal projeto tenha dimensão exclusivamente civil, sua aprovação não causará apenas reflexos na respectiva área, mas também efeitos na esfera criminal. No entendimento de Maciel (2012, p. 1), "uma legislação civil para a internet não pode deixar de estabelecer os limites da responsabilidade dos provedores de conexão e conteúdo, e questões relacionadas à guarda de dados, definindo o tempo que deverão armazená-los. Tais pontos são fundamentais. O primeiro por permitir a inovação e o empreendedorismo no meio digital, visto que ao empreendedor será facilitada a contabilização dos riscos jurídicos de seu negócio e assim adotar medidas preventivas. O segundo ponto, a guarda de dados, é relevante pelo fato de tais registros serem fundamentais para identificação de usuários, seja para produção de prova civil ou mesmo para subsidiar investigação criminal".

No que tange à conduta transnacional dos infratores cibernéticos, os mesmos utilizam-se de tecnologia de ponta para encobrirem aspectos relacionados à materialidade dos delitos. Assim, eles se mantêm no anonimato de forma fácil, sendo indispensável uma colaboração internacional, proposta, inclusive, na Convenção de Budapeste, ratificada pelo Brasil, a qual prioriza uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no meio digital através da cooperação internacional (WANDERLEI, 2012, p. 45-46; HAJE, 2011; SOUZA; PEREIRA, 2009, p. 5).

3.9.3 Breves considerações sobre as Leis ordinárias 12.735/2012 e 12.737/2012

A expansão de novas tecnologias faz ganhar importância a criação de legislação voltada à coibição de atos ilícitos praticados através do meio virtual. Tal legislação não é bem vista por muitos, por representar um acúmulo inútil à tipificação penal. No entanto, percebeu-se que era necessária a atualização da norma penal para que os crimes virtuais não fugissem ao controle (OLIVEIRA, 2013, p. 17).

Em 2011 uma onda de ataques de *hackers*[12] e *crackers*[13] a sites oficiais do governo e empresas públicas fizeram-nos ficar fora do ar temporariamente. Tal acontecimento influenciou na criação da lei 12.737/2012, resultante do PL 84/1999 (OLIVEIRA, 2013, p. 25; Revista Época, 2011).

---

[12] "Hacker" e "cracker" podem ser palavras parecidas, mas possuem significados bastante opostos no mundo da tecnologia. De uma forma geral, hackers são indivíduos que elaboram e modificam softwares e hardwares de computadores, seja desenvolvendo funcionalidades novas ou adaptando as antigas. Já cracker é o termo usado para designar quem pratica a quebra (ou cracking) de um sistema de segurança.
Na prática, os dois termos servem para conotar pessoas que têm habilidades com computadores, porém, cada um dos "grupos" usa essas habilidades de formas bem diferentes. Os hackers utilizam todo o seu conhecimento para melhorar softwares de forma legal e nunca invadem um sistema com o intuito de causar danos. No entanto, os crackers têm como prática a quebra da segurança de um software e usam seu conhecimento de forma ilegal, portanto, são vistos como criminosos (https://olhardigital.uol.com.br/fique_seguro/noticia/qual-a-diferenca-entre-hacker-e-cracker/38024). Acesso em: 01/02/2017.

[13] As denominações foram criadas para que leigos e, especialmente a mídia, não confundissem os dois grupos. O termo "cracker" nasceu em 1985, e foram os próprios hackers que disseminaram o nome em sua própria defesa. A ideia era que eles não fossem mais confundidos com pessoas que praticavam o roubo ou vandalismo na internet.
Apesar dos termos serem mundialmente conhecidos, chamar alguns de “bons” e outros de “maus” não agrada a todos. Há quem acredite que tanto o hacker quanto o cracker são habilidosos e podem fazer as mesmas coisas, como o programador Vinicius Camacho “Uma pessoa pode quebrar um software, como fazem os crackers, mas não usar as informações de forma antiética. O oposto também pode acontecer: um hacker usar sua habilidade de forma mal-intencionada”, conclui.
O que isso quer dizer? Isso significa que, para ele, o termo cracker, criado para denotar um “Hacker do mal”, é bastante subjetivo. Para ele os termos mais corretos são os usados dentro da ética hacker : “White Hat” (Chapéu Branco), “Black Hat” (Chapéu Preto) e “Gray Hat” (Chapéu Cinza). Os hackers "Chapéu Branco" são pessoas interessadas em segurança e, na maioria das vezes, usam suas habilidades a favor das empresas, sendo 100% éticos em suas ações. São eles que ocupam os cargos de analista de sistema, especialista em TI ou outros empregos na área de informática.
Já os hackers "Chapéu Preto" são criminosos e, normalmente, especializados em invasões maliciosas de sites. Os hackers "Chapéu Cinza" têm as intenções de um Chapéu Branco, mas suas ações são eticamente questionáveis.
Apesar dessa contradição dentro do próprio cenário de profissionais da segurança, ainda muitos programadores aceitam os termos hacker e cracker como definições corretas. Diversos Fóruns sobre programação, blogs de tecnologia, sites como Wikipedia e até dicionários conceituam os hackers como profissionais do bem e crackers como criminosos (https://olhardigital.uol.com.br/fique_seguro/noticia/qual-a-diferenca-entre-hacker-e-cracker/38024). Acesso em 01/02/2017.

Conforme Wendt e Jorge (2012, p. 26), “esse tipo de ação pode ter uma conotação de emulação, para o autor apresentar algum destaque do grupo a que pertence, ou de ciberativista, com o intuito de defender convicções religiosas, filosóficas ou políticas”.

Nesse sentido, OLIVEIRA com propriedade e escorreita lição induz:

> Independente da conotação, fato é que essas ações delitivas reinflamaram as discussões acerca da necessidade de impor limites penais às condutas praticadas pelo ambiente virtual. Nesse sentido, o já referenciado PL 84/1999 (Lei 12.737/2012) ficou conhecido por AI-5 digital pela acusação de promover a censura e a obrigação de retenção de *logs* ou IPs (endereço do computador na internet) por três anos pelos provedores. Por oportuno, um projeto de lei opcional foi trazido pela bancada governista, a saber, o PL 2.793/2011, com a intenção de não criminalizar o acesso à internet. (OLIVEIRA, 2013, p.32; Estadão, 2011).

Contudo, o que determinou a aprovação de tais institutos foi publicação de fotos íntimas da atriz Carolina Dieckmann. Segundo Oliveira (2013, p.32), “a conta de e-mail da vítima foi *hackeada,* de modo que os invasores tiveram acesso aos dados da vítima. As imagens foram postadas em sites de pornografia [...]”.

Como se vê, a produção legislativa no Brasil sofre forte influência da mídia. Fica, assim, a impressão de que a privacidade de um indivíduo famoso é mais importante do que a segurança de informações contidas em sites oficiais do governo (OLIVEIRA, 2013, p. 33).

A Lei 12.735 de 30 de novembro de 2012, inicialmente projetada para ser extravagante, foi modificada para apenas alterar os diplomas legais já existentes. Possui a seguinte ementa: "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" (BRASIL, 2012).

A criação de tal norma teve como principal influência a impossibilidade de proteção aos bens da vida, maculados pelos crimes virtuais, através de uma legislação da década de 1940, ano da criação do Código Penal (OLIVEIRA, 2013, p. 34).

Por conseguinte, a Lei 12.737 de 30 de novembro de 2012 trouxe a mesma ideia da Lei 12.735, ou seja, a legislação penal já existente seria suficiente para combater os crimes virtuais. Traz a seguinte ementa: "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" (BRASIL, 2012).

Ambas as leis aqui analisadas tiveram o objetivo de preencher lacunas legislativas que impediam a tipificação de atos ilícitos praticados pelos meios digitais. Desta feita, desejou-se cumprir os princípios que norteiam o Direito Penal, a saber, o da legalidade e a proibição da analogia. Tiveram como foco a proteção da informação. No entanto, devem ser criados mecanismos específicos no combate aos crimes virtuais. O mundo virtual ainda percebe um vazio normativo, o que contribui para a falta de punição estatal (OLIVEIRA, 2013, p. 51; MONTEIRO NETO, 2008, p. 126),

No espírito de modernização da legislação criminal, o art. 154-A do CPB tipifica o comportamentoi daquele que invade dispositivo informático alheio, conectado ou não à rede de computadores[14], mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita (SANCHES, 2013, p. 261).

O objeto jurídico do crime, é a privacidade individual e/ou profissional, resguardada (armazenada) em dispositivo informático, desdobramento lógico do direito fundamental assegurado no art. 5º, X, CF/88: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito de indenização pelo dano material ou moral decorrente de sua violação" (SANCHES, 2013, p. 261).

Em regra, o crime é de menor potencial ofebsivo, salvo na sua forma qualificada (§ 3º), quando majorado pela divulgação, comercialização ou tranmissão a terceiro, a qualquer título, dos dados ou informações obtidos (§ 4º) (SANCHES, 2013, p. 261).

Por fim, na formalidade do § 5º, do art 154-A do CPB, a pena é aumentada de um terço à metade se o crime for praticado contra: a) Presidente da República, Governadores e Prefeitos; b) Presidente do Supremo Tribunal Federal; c) Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa do Distrito

[14] "Sabe-se por certo, constiutir a comunicação telemática, o atual meio mais difundido de transmissão de mensagens de toda a ordem entre pessoas físicas e jurídicas. O e-mail tornou-se uma forma padrão de enviar informes e mensagens profissionais e particulares, seja para fins comerciais, seja para outras finalidades das mais diversas possíveis. As redes sociais criaram, também, mecanismos de comunicação, com dispositivos próprios de transmissão de mensagens. Torna cada vez mais rara a utilização de cartas e outras bases físicas, suportando escritos, para a comunicação de dados e informes. Diante disso, criou-se novel figura típica incriminadora, buscando punir quem viole não apenas a comunicação telemática, mas também os dispositivos informáticos, que mantém dados relevantes do seu proprietário" (NUCCI, p. 774-5).

Federal ou de Câmara Municipal; d) dirigente máximo da administação direta e indireta, federal, estadual, municipal ou do distrito federal (SANCHES, 2013, p. 262).

Pune-se a invasão de dispositivo informático alheio, mediante violação indevida de mecanismos de segurança ou instalação de vulnerabilidades (SANCHES, 2013, p. 262).

Por dispositivo informático entende-se qualquer aparelho (instrumento eletrônico) com capacidade de armazenar e processar automaticamente informações/programas (notebook, netbook, tablet, ipad, iphone, smartphone, pendrive etc). Importante observar ser indiferente o fato de o dispositivo estar ou não conectado à rede interna ou externa de computadores (intranet ou internet)[15] (SANCHES, 2013, p. 262).

Rogério Sanches elenca, com base no dispositivo legal[16] quais são as formas de agir, constatados no código penal, é o escólio:

> Na primeira, o agente vence os obstáculos de proteção do dispositivo (senha, chave de segurança, mecanismos de criptografia, assinatura digital, mecanismos de controle e acesso, mecanismos de certificação, etc) para obter, adulterar ou destruir dadis ou informações sem autorização do titular do dispositivo.
> Na segunda conduta, o cibercriminoso isntala no dispositivo vulnerabilidades, brechas no sistema computacional (conhecidas como "bugs" ou "worms") a fim de espalhar software malicioso que serve para atacar, degradar, impedir a utilização correta de um equipamento ou obter informações de forma encoberta, visando o agente conquistar vantagem ilícita (SANCHES, 2013, ps. 262-263).

Nos termos do § 1º[17], na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a

---

[15] Intranet é uma rede local de computadores privada, é uma rede utilizada apenas por um grupo reduzido de usuários, normalmente, relacionados a uma instituição ou departamento de uma empresa. Esta rede utiliza os mesmos protocolos da internet (TCP/IP). Entretanto o acesso a estas é restrito aos usuários autorizados. Uma intranet, normalmente, não é acessível a partir da internet por usuários não autorizados. Isto ocorre porque esta é utilizada para disponibilizar informações a todos os usuários internos como relatórios, normas, formlários, notícias, dentre outras (http://windows.microsoft.com/pt-brwindows7/keyboard-shortcuts-internet/intranet). Acesso em: 26/03/2017.

[16] Assim, o tipo penal é aberto e exige um juízo de valor para complementar a nálise da tipicidade. Aliás, é um tipo semi-aberto, ou seja, nem aberto nem fechado, pois ao mesmo tempo que abre com a locução "mediante violação indevida", fecha com a complementação "de mecanismo de segurança", limitando, portanto, o âmbito da violação. Em outros termos, qualquer outra violação que não se refira a "mecanismo de segurança", não tipificará a conduta descrita no *caput* que ora examinamos. Ou, dito de outra forma, ainda que haja a violação ou invasão "de dispositivo informático alheio, conectado ou não à rede de computadores" se não houver "mecanismo de segurança" (ou caso haja, não estando acionado) que seja violado, a conduta não se adequará a esta descrição típica. Poderá, eventualmente, adequar-se a outro dispositivo penal, mas não a este, sob pena de violar-se a tipicidade estrita (invasão de dispositivo informático. Disponível em: www.atualidadesdodireito.co.br/cezarbitencout. Acesso em 21/12/2012.

prática da conduta definida no caput (obter, adulterar, ou destruir dados ou informações, ou instalar vulnerabilidades). Com a equiparação, o legislador buscou incriminar as formas mais comuns de participação criminosa (SANCHES, 2013, ps. 263-264).

Arremata o *expert* jurista Rogério Greco, em artigo publicado no seu sítio eletrônico, rogério greco oficial, intitulado **Comentários Sobre o Crime de Invasão de Dispositivo Informático art. 154-A Código Penal**:

> Diz o § 1º do art. 154-A, verbis:
>
> § 1o Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> Produzir significa criar, gerar, fabricar; oferecer importa em ofertar, gratuita ou onerosamente; distribuir tem o sentido de partilhar, repartir; vender tem o significado de transferir (o dispositivo ou o programa de computador) mediante um preço determinado; difundir diz respeito a propagar, divulgar, espalhar. Todas essas condutas, vale dizer, produzir, oferecer, distribuir, vender ou difundir dizem respeito à dispositivo ou programa de computador. O art. 1º, da Lei nº 9.609, de 19 de fevereiro de 1998, traduz o conceito de programa de computador, dizendo: Art. 1º Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados (http://www.rogeriogreco.com.br/?p=2183).

Conforme o disposto na parte final do § 1º do art. 154-A do Código Penal, as condutas acima narradas devem ser cometidas com o intuito de permitir a prática da conduta definida no caput do citado dispositivo legal, ou seja, o agente produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador, no sentido de permitir com que terceira pessoa invada dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Com essas hipóteses, quis a lei, portanto, punir de maneira independente, aquele que, de alguma forma, auxilia para que terceiro tenha facilitada a prática do tipo penal constante do caput do art. 154-A do diploma repressivo (http://www.rogeriogreco.com.br/?p=21830).

---

[17] NUCCI, não sem razão, alerta que esta modalidade de conduta não possui nenhum sujeito passivo determinado. Afinal, consiste na preparação do delito do *caput.* Diante disso o interesse punitivo estatal, nesta hipótese, volta-se à proteção da sociedade, em nítido crime vago. Ora, se o sujeito passivo, na realidade, é a sociedade, este delito poderá não ser autonomamente punido, pois o art. 154-B seja a ação penal pública condicionada à representação da vítima, salvo se o crime é cometido contra a administração direta e indireta (Curso de Direito Penal, p. 777).

4 METODOLOGIA

Com base no método qualitativo pelo qual foi desenvolvido este Trabalho de Conclusão de Curso, com informações bibliográficas de autores que já se manifestaram acerca do assunto e sítios de busca, com o intuito de aprofundamento metodológico-científico para debruçar incisivamente na análise criminal e desenvolver pesquisas relacionadas a crimes na internet. Com fulcro na premissa científica de auferir dados catalogados nas literaturas, clássica e moderna, sobre tais empreitadas criminológicas no mundo virtual, é que se faz necessária a busca científica, justificando tal metodologia utilizada para melhor concatenação linguística, referentes a técnicas aqui impregnadas. Nas buscas realizadas para o desenvolvimento deste trabalho, foram cruzados informações e dados já publicados. A fim de possibilitar e comparar – caso seja este trabalho requisitado – que se faz mister a dedicação desenvolvida no transcorrer deste. Sempre buscando a melhor compreensão para o leitor e para o mundo científico, embasando assim, as diferentes visões de vários autores, que dia a dia, se aprofundam mais acerca do assunto. No que concerne aos meios de investigação, trata-se, pois este trabalho bibliográfico caracterizado pela busca incessante de material em livros, revistas, sítios de busca, entre outros. Quanto ao fim, refere-se a um trabalho dedicado ao interesse precipuamente intelectual, vislumbrando casos concretos que acontecem no quotidiano da sociedade moderna. Não há, portanto nenhuma entrevista a qual debrucei com a finalidade de investigar algum caso específico, nem referências a didáticas em que envolvam perguntas e respostas feitas a entrevistados ou vítimas de constrangimentos ou abusos advindos do meio *cibernético.*

5 CONCLUSÃO

Porquanto, a própria sociedade está à mercê da flexibilidade e eficiência que a tecnologia lhes cedeu. Tornou vulgar o acesso e com isso os 'piratas da internet' se auto engrandecem, pois a legislação frágil evidencia um caráter intrínseco ao cometimento de crimes em rede.

Teríamos que, reformular ou tipificar no Código Penal, ao invés de acrescentar uns ou outros dispositivos, criar uma própria codificação. Seria algo que necessariamente traria uma resposta concreta e uma reprimenda compatível para os casos alarmantes, gravíssimos, que, sequer temos conhecimentos pela sua perplexidade.

A internet não é só um objeto facilitador, também, diria, que mesmo com regramentos próprios e definidos em legislações nacionais e alienígenas, tem tornado cada vez mais um espaço deletério, anômico, atípico, no qual a impunidade impera e afronta todo e qualquer ordenamento jurídico que se vê rente à desordem.

Como podemos constatar, tão somente a penalização de condutas dessa natureza não é coerente em um Estado social e democrático de Direito. É incompatível assegurar a garantia Constitucional ao livre desenvolvimento por meio de uma limitação realizada através de leis morais, as quais venham outorgar ao legislador o poder de combater, mediante imperiosidade penal, condutas criminosas e banais. Imprescindível, destarte, é salientar que a figura do *hacker* deve ser compelida de forma harmônica e conjuntural, balisando sempre o aspecto criminológico com a conduta de enfrentamento estatal na seara penal e processual penal, não deixando de lado a garantia dos que navegam na rede computacional sem a premissa delituosa. Esses merecem total segurança jurídica e certeza de que estão em local que lhes deem o mínimo de credibilidade informacional.

Portanto, o enfrentamento jurídico concernente aos crimes interligados por meio de rede de computadores e proteção de dados, está cada vez mais em evidência e requerendo, nesse diapasão, maior atenção e políticas de segurança computacional acerca de proteção de dados, além de uma efetiva aplicação da legislação, quedando sempre para o melhoramento do sistema legal, a fim de coibir ou minimizar os trasntornos advindos com a tcnologia buscando maior eficácia normativa, nos âmbitos privado e estatal.

REFERÊNCIAS

ALVIM, Arruda. **Competência Internacional**. Revista de Processo, São Paulo, nº 7/8, 1977.

ARAUJO, Nadia de. **Direito Internacional privado**: teoria e prática brasileira. 4 ed. Atualizada e amplicada. Rio de Janeiro: Renovar, 2008.

ANGUER, Anne Joyce. **Vade mecum acadêmico de direito**, 22. ed. São Paulo, Rideel, 2016, (série Vade mecum).

ATHENIENSE, A. R. **Crimes virtuais, soluções e projetos de Lei**. DNT. [s.l.]. 29 out. 2004. Disponível em: <http://www.dnt.adv.br/noticias/direito-penal-informatico/crimes-virtuais-solucoes-e-projetos-de-lei/>. Acesso em: 27 mai. 2013.

BASSO, M.; ALMEIDA, G. A. **É preciso difundir mentalidade digital nas empresas.** In: KAMISNSKI, Omar (Org.), op. cit., 2007.

BASTOS, Celso, MARTINS, Ives Gandra. *Comeniários à Constituição do Brasil.*São Paulo : Saraiva, 1989. v.; FERREIRA FILHO, Manoel Gonçalves. *Comentários à Constituição Brasileira de 1988.* São Paulo: Saraiva, 1990. v.

BENEYTO, J. **Informação e sociedade: os mecanismos sociais da atividade informática.** Petrópolis: Vozes, 1997.

BITTENCOURT, C. R. **Tratado de Direito Penal** – Parte geral. 10. ed. São Paulo: Saraiva, 2006. v.1.

BLOGSPOT. **DIREITO INTERNACIONAL**, 2008. Disponível em: http://direitointernacionall.blogspot.com.br/2008/09/o-cdigo-bustamante.html. Acesso em: 12/10/2014.

BOBBIO, N. **A era dos direitos.** Trad. Carlos Nelson Coutinho. 10. ed. Rio de Janeiro: Campus, 1992.

BRASIL. Ministério Público Federal. **Crimes cibernéticos**. Brasília, 2005. Disponível em: <http://www.prsp.mpf.gov.br/cgi/regulamentacao/resolucao2005-01.htm>: Acesso em: 21/03/2013.

_____ . Departamento da Polícia Federal **Crimes e investigações informáticas**. Brasília, 2010. Disponível em:<http://www.policiafederal.gov.br/departamentodecrimesdecomputador/central/informacao2010.htm>: Acesso em: 14/07/2012.

_____. Decreto-Lei 2848 de 1940. **Código penal brasileiro**. Legislação Federal. sítio eletrônico internet - planalto.gov.br. Acesso em: 05/10/2016.

_____. Congresso Nacional. Câmara dos Deputados. **Diário da câmara dos deputados**, Brasília, ano 64, n. 85, 21 maio 2009, p. 20.963-21.765. Disponível em: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/credn/noticias/deputados-cobram-adesao-do-brasil-a-convencao-sobre-cibercrime>: Acesso em: 14/09/2016.

_____. **Constituição da República Federativa do Brasil:** promulgada em 5 de outubro de 1988. Obra coletiva de autoria da Editora Saraiva com a colaboração de Luiz Roberto Curia, Livia Céspedes e Juliana Nicoletti. 9. ed. São Paulo: Saraiva, 2013.

_____. Convenção de Direito Internacional Privado. Código de Bustamante, 2015. Disponível em <**https://samuelebel.jusbrasil.com.br/artigos/215397442/convencao-de-direito-internacional-privado-codigo-de-bustamante**>. Acesso em: 03/09/2016.

_____. **Lei 8.078 de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>. Acesso em: 27 mai. 2013.

_____. **Lei 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: 28 mai. 2013.

_____. **Lei 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: 28 mai. 2013.

_____. **Lei 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: 12 ago. 2014.

_____. **Lei 5.869, de 11 de janeiro de 1973**. Disponível em < http://www.planalto.gov.br/ccivil_03/leis/L5869compilada.htm>. Acesso em 08 de outubro de 2012.

_____. **LEI 12.965, de 23 de abril de 2014. MARCO CIVIL DA INTERNET.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>: Acesso em: 15/03/2017.

CABRAL, R. Três projetos e duas leis. **Estadão.** 4 set. 2011. Disponível em: <http://blogs.estadao.com.br/link/tres-projetos-para-duas-leis/>. Acesso em: 28 mai. 2013.

CARNEIRO, Athos Gusmão. **Jurisdição e Competência**: exposição didática: área de direito processual civil. 2. ed. rev. e ampl. São Paulo: Saraiva, 1983.

CARNEIRO, A. G. Crimes Virtuais: Elementos Para uma Reflexão Sobre o Problema na Tipificação. In: **Âmbito Jurídico**, Rio Grande, 15, n. 99, abr. 2012. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=11529>. Acesso em: 27 mai. 2013.

CELLI JUNIOR, Humberto. **Litispendência internacional no Brasil e no MERCOSUL**. Revista Brasileira de Direito Processual, Belo Horizonte, nº 76, ano 19, pp. 219-234.

CERT.br. **Estatísticas de Notificações de Spam Reportadas ao CERT.br.** Disponível em: http://www.cert.br/stats/spam/. Acesso em: 20 mai. 2013.

CHAGAS, C. Túnel do tempo (cronologia da internet no Brasil). **Folha de São Paulo.** Disponível em: <http://www1.folha.uol.com.br/folha/sinapse/ult1063u275.shtml>. Acesso em: 20 mai. 2013.

CRUZ, A. **Ensinar.** Disponível em: <http://www.antoniocruz.net/ensinar/internet/manuais/internet-01-internet.pdf>. Acesso em: 30 jul. 2011.

CRUZ, Danielle da Rocha. **Criminalidade informática**. Rio de Janeiro: Forense, 2006.

CUNHA, Rogério Sanches. **MANUAL DE DIREITO PENAL.** 5. ed. Parte Especial. Bahia: *Jus*PODIVM, 2013.

DAVID, H. **DR2** - Nascimento e evolução dos computadores/internet. CINEL - Centro Formação Profissional da Indústria Eletrónica. Disponível em: <http://efaredesinformaticas01.cinel.org/site_files/formandos/jose/dr2.pdf>. Acesso em: 15 jul. 2011.

DINAMARCO, Cândido Rangel. **Instituições de Direito Processual Civil**, Volume I. 5. ed. rev. e atual. São Paulo: Malheiros Editores, 2005.

DINIZ, Maria Helena. **Lei de Introdução ao código civil brasileiro interpretada**. 9. ed. Adaptada à lei n. 10.406/2001. São Paulo: Saraiva, 2002.

FIGUEIRA JÚNIOR, Joel Dias. **Comentários ao código de processo civil**: v. 4: do processo de conhecimento, arts. 282 a 331, tomo III. São Paulo: Editora Revista dos Tribunais, 2001.

FURLANETO NETO, M.; GUIMARÃES, J. A. C. Crimes na Internet: Elementos para uma Reflexão Sobre a Ética Informacional. **Revista CEJ**. Brasília, n. 20, jan./mar,2003. Disponível em: <http://www2.cjf.jus.br/ojs2/index.php/cej/article/viewFile/523/704>. Acesso em: 13 out. 2012.

GONÇALVES, Marcus Vinicius Rios. **Novo curso de direito processual civil**, volume 1: teoria geral do processo de conhecimento (1ª parte). 2. ed. rev. e atual. São Paulo: Saraiva, 2005.

GRECO FILHO, Vicente. **Direito processual civil brasileiro**, volume I : (teoria geral do processo e auxiliares da justiça). 22. ed. São Paulo: Saraiva, 2010.

GRECO, ROGÉRIO. **Comentários Sobre o Crime de Invasão de Dispositivo Informático art. 154-A Código Penal**. Artigos, Rogerio Greco Site Oficial. Disponível em: <http://www.rogeriogreco.com.br/?p=2183> Acesso em: 14/06/2016.

HAJE, L. **Saiba como os crimes na internet são tratados em outros países**. Agência Câmara de Notícias, Brasília, 08 jul. 2011. Disponível em: <http://www2.camara.leg.br/agencia/noticias/CIENCIA-E-TECNOLOGIA/199806-SAIBA-COMO-OS-CRIMES-NA-INTERNET-SAO-TRATADOS-EM-OUTROS-PAISES.html>. Acesso em: 27 mai. 2013.

<http://www.prsp.mpf.gov.br/cgi/regulamentacao/resolucao2005-01.htm> Acesso em, 21/03/2013.

<http://www.policiafederal.gov.br/departamentodecrimesdecomputador/central/informacao2010.htm> Acesso em, 14/07/2012.

<http://tcconline.utp.br/media/tcc/2015/09/**CRIMES-CIBERNETICOS.pdf**>: Acesso em, 12/06/2016.

<http://windows.microsoft.com/pt-brwindows7/keyboard-shortcuts-internet/intranet>. Acesso em: 26/03/2017.

<http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/credn/noticias/deputados-cobram-adesao-do-brasil-a-convencao-sobre-cibercrime>: Acesso em 14/09/2016.

JORGE, H. V. N. **A ameaça invisível dos Rootkits.** Disponível em: <http://www.higorjorge.com.br/279/a-ameaca-invisivel-dos-rootkits>. Acesso em: 20 mai. 2013.

JO, Hee Moon. **Moderno direito internacional privado**. São Paulo: LTr, 2001.

LENZA, Pedro. **Direito Constitucional Esquematizado**. 13. ed. São Paulo: Saraiva, 2008.

MACIEL, R. F. Marco civil da internet: o porquê, para o quê e omissões. **Jus Navigandi**, Teresina, ano 17, n. 3333, 16 ago. 2012. Disponível em: <http://jus.com.br/revista/texto/22433>. Acesso em: 28 mai. 2013.

Maior ataque hacker no Brasil partiu da Itália. **Revista Época.** Disponível em: <http://revistaepoca.globo.com/Revista/Epoca/0,,EMI243559-15224,00.html>. Acesso em: 28 mai. 2013.

MANDEL, A.; SIMON, I.; LYRA, J. L. de. **Informação: Computação e Comunicação**. Universidade de São Paulo. Disponível em: <http://www.ime.usp.br/~is/abc/abc/abc.html>. Acesso em: 30 jul. 2011.

MONTEIRO NETO, J. A. **Aspectos Constitucionais e Legais do Crime Eletrônico.** Fortaleza, 2008.

MOREIRA, José Carlos Barbosa. **Relações Entre Processos Instaurados**, Sobre a Mesma Lide Civil, No Brasil e em País Estrangeiro. Revista de Processo, São Paulo, nº 7/8, 1977.

NUCCI, Guilherme de Souza. **MANUAL DE PROCESSO PENAL E EXECUÇÃO PENAL.** 6. ed. São Paulo: Revista dos Tribunais, 2010.

OLIVEIRA, J. C. de. **O Cibercrime e as Leis 12.735 e 12.737/2012.** São Cristóvão, 2013.

PAESANI, Liliana Minardi. **Direito e internet**. São Paulo: Atlas, 2000.

PASSOS, José Joaquim Calmon de. **Comentários ao Código de Processo Civil**, Lei 5.869 de 11 de janeiro de 1973, vol. III: arts. 270 a 331. 8. ed. Rio de Janeiro: Forense, 1998.

PECK, Patrícia. **Direito digital**. São Paulo: Saraiva, 2004.

POLEGATTI, B. C.; KAZMIERCZAK, L. F. **Crimes Cibernéticos: O Desafio do Direito Penal na Era Digital.** Ourinhos, 2012.

SANTOS, Moacyr Amaral. **Primeiras linhas de direito processual civil**, volume 1. 26. ed. São Paulo: Saraiva, 2009.

SILVA NETO, Orlando Celso da. **Direito processual civil internacional brasileiro**. São Paulo: LTr, 2003.

SOUZA, G. L. M.; PEREIRA, D. V. **A Convenção de Budapeste e as Leis Brasileiras.** Paraíba, 2009.

SOUZA NETO, P. A. de. **Crimes de Informática.** Itajaí, 2009.
SZNICH, V. apud COSTA, M. A. R. da. **Jus Navigandi.** Out. 1995. Disponível em: <http://www1.jus.com.br/doutrina/texto.asp?id=1826>. Acesso em: 20 mai. 2013.

VEDOVATE, L. L. V. Contratos Eletrônicos. **INTERTEMAS.** v. 10, n. 10. Presidente Prudente, 2005.

WANDERLEI, F. P. **Crimes Cibernéticos: Obstáculos para Punibilidade do Infrator.** Araguaína, 2012.

WENDT, E.; JORGE, H. V. N. **Crimes Cibernéticos**. São Paulo: BRASPORT, 2012.