Centro Universitário do Distrito Federal – UDF
Coordenação do Curso de Direito

BIANA REBOUÇAS COELHO LIMA

A CRIMINALIDADE INFORMÁTICA:
Entraves jurídicos acerca dos crimes cibernéticos e dos desafios da investigação.

Brasília
2011

BIANA REBOUÇAS COELHO LIMA

A CRIMINALIDADE INFORMÁTICA:

Entraves jurídicos acerca dos crimes cibernéticos e dos desafios da investigação

Trabalho de conclusão de curso apresentado à Coordenação do Curso de Direito do Centro Universitário do Distrito Federal - UDF, como requisito parcial para obtenção do grau de bacharel em Direito.

Orientador: Prof. Valdinei Cordeiro Coimbra

Brasília

2011

Rebouças, Biana

A Criminalidade Informática: entraves jurídicos acerca dos crimes cibernéticos e dos desafios da investigação / Biana Rebouças Coelho Lima – Brasília, 2011.

71 f; 30 cm

Trabalho de conclusão de curso apresentado, à Coordenação do Curso de Direito do Centro Universitário do Distrito Federal – UDF. Brasília, 2011.
Orientador: Valdinei Cordeiro Coimbra.

1. Criminalidade Informática. 2.Investigação policial. 3.Legislação comparada.

CDU 340:007

BIANA REBOUÇAS COELHO LIMA

A CRIMINALIDADE INFORMÁTICA:
Entraves jurídicos acerca dos crimes cibernéticos e dos desafios da investigação

Trabalho de conclusão de curso apresentado à Coordenação de Direito do Centro Universitário do Distrito Federal - UDF, como requisito parcial para obtenção do grau de bacharel em Direito (Direito Penal e Processo Penal).

Orientador: Prof. Valdinei Cordeiro Coimbra

Brasília, 26 de novembro de 2011.

Banca Examinadora

_____
Valdinei Cordeiro Coimbra
Esp.Direito Penal e Processo Penal
Centro Universitário do Distrito Federal - UDF

_____
Eneida Orbage de Brito Taquary
Ms.Direito das Relações Internacionais
Centro Universitário do Distrito Federal - UDF

_____
Fernanda Maria A. Gomes de Aguiar
Ms.Direito Penal
Centro Universitário do Distrito Federal - UDF

Nota: 10,0

AGRADECIMENTOS

Agradeço a Graça, minha tia, que durante toda trajetória de vida sempre esteve comigo, nos melhores e piores momentos, com sua ajuda e apoio ilimitado foi possível conquistar vários sonhos e transpor grandes barreiras.

A meu irmão Bruss, que mesmo longe, esteve presente com incentivos, bem como seu próprio exemplo de determinação, força e superação.

Ao Departamento de Polícia Federal, que quando servidora, ratificou minha vocação para o Direito e, em especial, a amiga Dirce Maria, que lançou a ideia do tema.

A todos que, direta ou indiretamente, contribuíram para o término desta etapa.

RESUMO

O presente trabalho monográfico tem por objetivo discorrer sobre os crimes virtuais, nova modalidade de transgressão da era contemporânea. O estudo apresenta conceitos, caracterizações e classificações dos ciberdelitos, por categorias, considerando o bem jurídico lesionado. Tem como foco principal demonstrar os entraves ou obstáculos, no processo investigativo policial, haja vista as particularidades destes delitos, a instantaneidade do mundo digital, bem como a efemeridade ou perecimento das provas. Ressalta as questões quanto à identificação, o sujeito ativo do crime, a partir do equipamento ou número do IP (*Internet Protocol*), do uso de roteador *wireless*, além dos fatores de tempo e espaço (local de determinação do crime). Aborda os princípios penais relacionados aos crimes cibernéticos, diante do caráter da transnacionalidade, nestes tipos de delito. Por fim, faz análise comparada da legislação brasileira e estrangeira (alemã e holandesa), em alguns aspectos pontuais como o local do crime e quanto à violação de segredo informático, mediante a prática do *hacking*. No estudo foi possível contrapor à velocidade do avanço da tecnologia e do aumento deste crime, em detrimento da lenta produção legislativa, ou mesmo a inexistência de tipos penais específicos, ainda não contemplados na legislação brasileira, considerados, portanto, atípicos ou inexistentes.

Palavras-chave: Criminalidade Informática. Investigação policial. Legislação comparada.

ABSTRACT

This monograph addresses the Cybercrime, a new modality of crime which has emerged during the Contemporary Era. The present study aims at providing a characterization and a conceptual framework for this type illegal activity. In addition, it attempts to categorize the diverse types of Cybercrimes depending on the specific kind of criminal offense carried out. The dynamism of the digital world as well as the fragility of the evidence generated by Cybercrimes make it a very particular type of infraction. Consequently, the technical challenges faced by the police while carrying out a criminal investigation of this type is here addressed. In addition to the standard elements such as time and location of the crime, tracking down potential suspects rely heavily on identifying their IP (internet protocol) number and their wireless router. This work also discusses the possible legal actions that can be taken for a crime that is not necessarily circumscribed to the borders of a single country. It also draws a comparison between the Cybercrime legislation present in Brazil and those of other countries such as Germany and Holland, specially in what concerns the violation of privacy through the action of computer hacking. Finally, this study contrasts the high pace of technological development and Cybercrimes with the lagging development of adequate regulatory legislations. In the case of Brazil, a total lack of adequate legislation is found for certain categories of Cybercrimes considered atypical or non-existent.

Key words: Cybercrime. Police investigation. Comparative law.

SUMÁRIO

INTRODUÇÃO 10
1 CRIMINALIDADE CONTEMPORÂNEA 13
1.1 CONCEITO DE CRIMES INFORMÁTICOS 16
1.2 OS CRIMES DIGITAIS E SUAS CARACTERÍSTICAS 18
1.2.1 Vulnerabilidade dos sistemas e fator distância 18
1.2.2 Fator tempo 19
1.3 BENS JURÍDICOS TUTELADOS – OBJETOS TANGÍVEIS E INTANGÍVEIS 19
2 DOS PRINCÍPIOS PENAIS RELACIONADOS AOS CRIMES DIGITAIS 21
2.1 PRINCÍPIO DA LEGALIDADE OU DA RESERVA LEGAL 21
2.2 PRINCÍPIO DA TERRITORIALIDADE 22
2.3 PRINCÍPIO DA EXTRATERRITORIALIDADE 25
2.4 PRINCÍPIO DA JUSTIÇA UNIVERSAL OU COSMOPOLITA 27
2.5 PRINCÍPIO DA DEFESA, REAL OU DA PROTEÇÃO 28
2.6 COOPERAÇÃO INTERNACIONAL 29
3 A INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS 31
3.1 CIBERNÉTICA, CIBERESPAÇO E CIBERCRIME 33
3.2 QUESTÕES ESPECÍFICAS NAS INVESTIGAÇÕES DE CIBE RCRIMES 37
3.2.1 Quanto à natureza jurídica 38
3.2.2 Quanto à identificação e determinação dos sujeitos do delito informático 41
3.2.2.1 Problema 1: realidade *on line* (anonimato) e *off line* 41
3.2.2.2 Problema 2: uso de roteador *wireless* 43
3.2.2.3 Problema 3: fator tempo e espaço 44
3.2.2.4 Para determinação do sujeito 45
3.2.3 Tempo nos Cibercrimes 47
3.2.4 Local 47
3.2.5 Provas 49
4 PRODUÇÃO LEGISLATIVA BRASILEIRA E INTERNACIONAL 52
4.1 PROJETOS DE LEI NO BRASIL E O DIREITO COMPARAD O 52
4.1.1 Dispositivos nas Leis Brasileiras referentes aos sistemas informáticos 55
4.1.2 Quanto ao local do crime – Brasil e Alemanha 57
4.1.3 Quanto ao local do crime – Holanda 57

4.2 CRIMES CONTRA OS SISTEMAS INFORMÁTICOS (VIOLAÇÃO DE SEGREDO) 60
4.2.1 Direito Alemão 60
4.2.2 Direito Holandês 61
4.2.3 Direito Brasileiro 62
CONCLUSÃO 66
REFERÊNCIAS 70

INTRODUÇÃO

A internet modificou e revolucionou a forma de comunicação, comércio, relacionamento interpessoal e econômico das sociedades. Deste modo, trouxe, indubitavelmente, o incremento na circulação de riquezas, informações e, com isto, novas formas de cometimento de crimes em diversas modalidades.

Estes últimos anos demonstraram, claramente, nova tendência e características da criminalidade mundial, dentre elas a transnacionalidade, pois tais crimes superam os limites territoriais de fronteiras, haja vista, a amplitude de alcance deste meio de comunicação.

Pelo lado econômico, estes crimes trazem prejuízos de milhares de dólares com fraudes, estelionatos, clonagens, bem como lavagem de dinheiro, entre outros danos, com vultosos prejuízos financeiros. O ciberespaço é, cada vez mais, cenário para atividades do crime organizado transnacional, campo fértil para atuação criminosa.

Há que considerar, também, maior acessibilidade às redes sociais, que se tornou nova forma de comunicação, inclusive em países com instabilidade política ou que passam por alguma perturbação social, de alguma espécie, como ocorrido recentemente na Líbia, Egito, em que rebeldes utilizaram da rede mundial de computadores para se comunicar e atingir a grande massa. Assim, conseguiram mobilização para a derrubada de governos locais, inclusive a internet está sendo utilizado pelas redes terroristas para comunicação e difusão de ideologias extremistas.

Neste estudo, não se abordará o tema de Ciberterrorismo, igualmente aspecto de extrema relevância que perpassa, necessariamente, o tema escolhido de crimes cibernéticos. Tal assunto não será explorado, porque deve ser tratado em trabalhos dedicados, exclusivamente, ao assunto, sobretudo porque o Ciberterrorismo possui características específicas, com vastas considerações próprias, inclusive com enfoque político. Até porque, neste momento, não será abordado o funcionamento técnico-operacional da internet, e sim informações, conceitos básicos e superficiais, quando necessário ao entendimento do assunto.

O presente trabalho tem como objetivo analisar as particularidades dos crimes cibernéticos ou virtuais, modalidade esta de cometimento, cada vez mais, frequente nas últimas duas décadas.

O foco principal do estudo está centrado na abordagem atinente aos entraves ou obstáculos enfrentados nos procedimentos investigativos policiais, pois a criminalidade informática possui características e nuances específicas, dentre elas a própria velocidade das operações informáticas e as variabilidades da tecnologia em si.

O objetivo da pesquisa será demonstrar as diversas possibilidades de crimes, utilizando-se a internet com foco nos seguintes aspectos problemáticos enfrentados nesta área, cotidianamente, como: a) caracterização da autoria, b) determinação do local do crime; c) a perícia e a prova informática; d) prisão em flagrante.

Quando o assunto são crimes de informática há particularidades que devem ser levadas em conta. Inicialmente deverão ser feitas considerações sobre os princípios básicos do direito penal, assim como questões pré-processuais (investigativas) e processuais, no trato da matéria, com abordagem acerca dos principais princípios penais relacionados ao tema, em especial, o Princípio da Territorialidade (Princípio da Aderência). Serão feitas reflexões sobre o ciberespaço, ou seja, a) como será a determinação do local do crime, diante de bens jurídicos intangíveis e dados virtuais; b) como se daria a delimitação do local e a identificação do sujeito pela equipe investigativa considerando que a atuação delituosa pode partir de múltiplas localidades distintas e diante da instantaneidade do mundo digital; c) os questionamentos que perpassam, necessariamente, se os delitos informáticos seriam novos tipos penais que devem ser contemplados na legislação de forma específica com as terminologias apropriadas, ou seriam apenas as velhas modalidades de crimes, já tratados pelo Código Penal e em outras legislações especiais, e teria apenas o uso do computador como instrumento ou meio de ação. Estas são apenas algumas reflexões a serem tratadas no decorrer da exposição.

Assim, diante do aumento da demanda e necessidade de repressão a tais delitos, serão demonstrados, exemplos da criminalidade informática dos mais variados na veiculados na mídia. Esta parte tem como finalidade conduzir o leitor ao entendimento da grandiosidade do problema. Este tipo de criminalidade está ocasionando perdas e prejuízos de milhões ou, talvez, de bilhões de dólares requerendo, por si só atenção especial.

Este estudo monográfico está dividido em quatro capítulos. No primeiro capítulo, o leitor será situado sobre o tema criminalidade, na era contemporânea e

será dedicado à conceituação de crime informático e suas variações, bem como demonstrará os bens jurídicos afetados, quais sejam: objetos tangíveis e intangíveis.

No segundo capítulo, será feita análise dos princípios relacionados aos crimes digitais, como o da legalidade, territorialidade e extraterritorialidade. Além disto, reflexão sobre conceitos de soberania, Estado-nação, etc.

No terceiro capítulo, de suma importância para o tema escolhido, serão relatados os diversos entraves, enfrentados pelas equipes policiais, cotidianamente, nos procedimentos investigativos, no tocante aos crimes digitais.

Serão tratadas de forma específicas questões relevantes como: tipificação penal, local, tempo do cometimento do crime e provas.

Será tratada, ainda, de forma específica, a questão da identificação do sujeito ativo do delito informático, com casos concretos, levando-se em conta dois mundos *on line* (virtual) e *off line* (real), considerações atinentes ao número de IP (*Internet Protocol*) e a realidade do uso de roteador *wireless* e sua contribuição ou não para o processo investigativo.

No quarto e último capítulo, será feita no âmbito da legislação análise dos dispositivos já existentes sobre o assunto e do projeto de lei, em tramitação no Congresso Nacional. Haverá comparação entre os ordenamentos jurídicos do Brasil, da Alemanha e Holanda, em aspectos pontuais.

O método utilizado de pesquisa será do tipo dogmática ou instrumental. Foram escolhidos autores específicos que tratam do tema, no âmbito penal e processo penal. A pesquisa também abordará alguns dispositivos da atual legislação existente.

Os métodos de procedimentos adotados serão, essencialmente, os monográficos com pequena parte focada no método comparativo, com finalidade de buscar conhecer como a Comunidade Internacional, em particular os alemães e holandeses trata a matéria, em relação à legislação brasileira nos aspectos da determinação do local do crime e quanto à violação de segredo informático.

As fontes de pesquisa utilizadas serão somente bibliográficas.

1 CRIMINALIDADE CONTEMPORÂNEA

A criminalidade contemporânea do século XXI evoluiu em grande parte com as transformações tecnológicas, o uso de novas formas de comunicação que qual trouxe consequentemente, maior interação social, favorecida pelo uso dos mais diferentes meios e ferramentas, dentre elas a internet e *e-mail*, que possibilitaram comunicação, quase instantânea, por computador o qual reduziu e modificou o conceito de distância e tempo.

Neste sentido, a internet revolucionou, indubitavelmente, a sociedade das mais variadas maneiras. A rede transformou os meios de comunicação, a interação social, política e econômica trazendo enorme trânsito de informações e riquezas, além do incremento das mudanças pessoais e profissionais, com circulação de documentos, imagens, dados, senhas, mídias etc. Portanto, tais transformações trouxeram ambiente fértil, crescente e propício para o cometimento dos mais variados tipos de crimes, dentre eles o estelionato, furto, violação de sistemas e banco de dados, dentre tantos outros. Formou-se novo ambiente ao crime, utilizando-se o meio digital e trazendo novas demandas, desafios para a ciência jurídica e campo desafiador novo para direito digital. Tais mudanças se encontram nos diversos segmentos, tanto no meio particular, quanto público, inclusive nas relações de trabalho com a digitalização de documentos, processos virtualizados, além do incremento do comércio eletrônico (*e-commerce)* e disseminação de informações.

Desta maneira, o professor Emilio Viano da Universidade de Washington-DC, no prefácio da do Livro “A Criminalidade Informática”, alerta para a velocidade de ação da tecnologia e a instantaneidade dos delitos digitais que estão muito a frente da produção legislativa, da atuação governamental e até da iniciativa da comunidade internacional. Os governos não estão tendo a reação necessária no tocante ao assunto, e, quando tem na grande maioria, apenas de forma reativa.

> O ciberespaço também é cada vez mais a nova arena para as atividades do crime organizado transnacional, lavagem de dinheiro, crimes financeiro, terrorismo e outros crimes. Há quem diria que os criminosos tem sido muito mais rápidos em adaptar e tomar vantagem desse novo mundo e dessa nova tecnologia para exercerem suas atividades através dos continentes com a velocidade da luz, sem serem detectados e em segredo. A resposta dos governos e das organizações internacionais tem sido com frequência lenta, insuficientes e, na maioria das vezes, de natureza reativa (VIANO *apud* ALBUQUERQUE, 2006, p.XV).

Com o aumento do uso da internet facilitada pela maior acessibilidade ao computador, na sociedade em geral, favoreceu ambiente propício para a prática de crimes informáticos diversos.

Para o cometimento dos crimes cibernéticos, conta-se com a existência de sujeitos ativos denominados de *hackers* e *crackers*[1]*,* que invadem sistemas informáticos de bancos, empresas, governo e mesmo de particulares, causando-lhes grandes prejuízos, na maioria das vezes financeiros e/ou de cunho particular, com invasão de privacidade com uso de dados particulares e senhas. Assim, tais agentes invadem os sistemas de segurança sem autorização das instituições, com o intuito de devassar informações, modificando-as ou apagando dados essenciais, disseminando vírus na rede e, na maioria das vezes, praticando estelionatos e prejuízos financeiros. Os *hackers* são capazes de controlar sistemas à distância, via redes de computadores.

Recentemente, o próprio governo brasileiro sofreu incessantes ataques virtuais em suas páginas oficiais. Os *hackers,* objetivando violar bancos de dados e obter informações governamentais, tentaram romper sistemas de segurança, cujos resultados negativos dos crimes informáticos são destacados:

---

[1] Os *hackers* são indivíduos que invadem os sistemas informáticos. Já os *crakers* são caracterizados como *hackers* malévolos, por adulterarem, destruirem ou subtrairem dados e programas de computadores (ALBUQUERQUE, 2006, p.191).

> Os prejuízos causados por *hackers* não param de aumentar no mundo todo. Como praticamente não existe uma ética virtual, eles, muitas vezes, são alcançados ao status de herói por uma subcultura que prolifera nas redes de computadores atacando a seu bel-prazer sistemas informáticos em todo o planeta. Conforme estatísticas elaboradas pela Interpol, os prejuízos teriam alcançado globalmente o montante de US$ 1 bilhão, já em 1998. Estima-se que apenas o ataque do vírus ILOVEYOU, desencadeado a partir de Manila, nas Filipinas, em 1999, tenham ocasionados prejuízos equivalentes a US$ 10 bilhões. Conforme pesquisa divulgada pelo *Computer Security Institute* e pelo FBI, 64% das empresas já sofreram alguma espécie de ataque virtual. Segundo a consultoria *Price Waterhouse*, 73% das empresas têm problemas de segurança informática. Especialistas estimam que na maioria dos casos os ataques não deixam vestígios (ALBUQUERQUE, 2006, p.3).

Muitas empresas principalmente as do ramo financeiro, como as instituições bancárias e grandes empresas, temem que a divulgação de algum ataque na segurança do sistema de informação possa quebrar a confiança de seus clientes em seus serviços e credibilidade das empresas, tornando a divulgação deste tipo de invasão deficiente ou inexistente. Deste modo, segue a preocupação em combater o crescente avanço dos crimes virtuais, tendo em vista o aumento das transações financeiras efetuadas, via rede de computadores.

Albuquerque segue demonstrando a amplitude de atuação em matéria de crimes digitais:

> Diretamente associada aos ataques lançados por *hackers*, está a credibilidade do próprio comércio eletrônico. Praticamente qualquer crime pode ser cometido via redes de computadores. Cada vez mais serviços são disponibilizados *on line*, cada vez mais dados circulam na internet, à mercê de condutas ilícitas. Caso os constantes ataques lançados por *hackers* transformem a rede das redes, aos olhos dos consumidores, numa terra sem lei, onde grassa a impunidade, o comércio eletrônico pode ter seu desenvolvimento estancado. Seu futuro está estreitamente vinculado à criação de um ambiente virtual seguro. O princípio fundamental a ser observado é o seguinte: tudo o que não se pode fazer *off line* (desconectado), não se pode fazer *on line* (conectado). Os crimes informáticos são, algumas vezes, novos *modus operandi* de antigas modalidades criminosas, outras vezes constituem modalidades criminosas *sui generis*, atípicas (ALBUQUERQUE, 2006, p.5).

Portanto, este estilo de criminalidade contemporânea mostra-se agressiva e variada, ocasionando bilhões em prejuízos por todo mundo, afetando a segurança das instituições, ataques aos bancos de dados, necessitando investimentos cada vez maiores em sistemas de segurança da informação.

Além disto, os crimes informáticos mostram-se diferenciados, pois a invasão não se dá fisicamente ou mediante armas, explosões e não ocasionam lesões físicas. No entanto, os ataques causam prejuízos enormes quando conseguem

romper os sistemas de segurança, devassar banco de dados, invadir contas bancárias, fraudar sistemas, modificar dados, divulgar informações falsas, disseminar vírus, na rede, enfim, tipos de crimes silenciosos, mas com resultados negativos desastrosos para a sociedade.

1.1 CONCEITO DE CRIMES INFORMÁTICOS

Inicialmente, cabe esclarecer, as variações de nomenclaturas neste assunto. São atribuídas denominações diversas como: delito informático, cibernético, delitos computacionais, crimes de informática, crimes de computador, crimes eletrônicos, crimes telemáticos, crimes informacionais, ciberdelitos. No entanto, são apenas variações conceituais para o mesmo delito.

Diante da problemática e especialidade dos crimes cibernéticos é imprescindível a tentativa de definição desses delitos. Para os doutrinadores, é necessário conceituar e delimitar estas ações delituosas. Contudo, deve-se considerar a amplitude do tema, as especificidades da linguagem informática e velocidade das mudanças tecnológicas, dos sistemas e das programações em geral.

O conceito de crimes por computador adotado pela *Organization for Economic Cooperation and Development* - OCDE e apresentado como uma tentativa de conceituação seria: “Considera-se abuso informático qualquer comportamento ilícito, aético ou não autorizado relacionado ao processamento automático e à transmissão de dados” (ALBUQUERQUE, 2006, p. 40).

No entanto, este conceito não resolveria o problema da tipificação dos crimes informáticos, apresentando vários problemas como a criação de tipos penais, extremamente amplos e abertos, dando margens a dúvidas, ao subjetivismo que seria um tanto temeroso.

> Essa definição tampouco resolve a questão, apresentando vários problemas. A primeira parte da definição – “qualquer comportamento ilícito, aético ou não autorizado” – extremamente ampla, inclui condutas que não podem ser consideradas crimes, por mais repreensíveis que sejam. A segunda parte – “relacionado ao processamento automático e à transmissão de dados” – exclui, por exemplo, o armazenamento de dados (ALBUQUERQUE, 2006, p. 40).

Portanto, a possibilidade de inclusão no rol de condutas que não poderiam ser consideradas crimes, por mais reprováveis ou repreensíveis que se mostrem e a

possibilidade de interpretações dos tipos penais de forma extensiva, por parte do Poder Judiciário, seria outro fator negativo a ser considerado.

Quanto à dificuldade de conceituação dos delitos digitais e a amplitude do tema não se deve criar conceitos estáticos que possam dificultar e causar mais obstáculos a correta tipificação penal.

> Qualquer tentativa de definir o termo “crime informático”, de conceituá-lo, apresenta desvantagens. Dificilmente, pode-se elaborar uma definição sucinta e precisa sem que se deixem dúvidas quer com relação ao seu objeto, quer com respeito à própria utilização da definição que lhe for conferida. A noção de crime informático envolve várias espécies de crimes. Não se deve adotar uma definição formal, estática, o que pode criar mais confusão do que soluções. Tem-se tentado definir crime informático de várias maneiras (ALBUQUERQUE, 2006, p. 40).

Nesta mesma linha de pensamento, Emilio Viano (2006 *apud* ALBUQUERQUE, 2006, p.XV) se posiciona quanto à vasta abrangência e possibilidades de crimes informáticos. Relata que o equipamento pode ser apenas o meio utilizado pelo agente ou pode ser próprio alvo de ataque, com outras formas de repercussão distintas.

> O desafio ao definir “crime informático” surge em parte porque os computadores podem desempenhar vários papéis diferentes nas atividades criminosas. Eles podem ser o objeto utilizado para cometer o crime, o “alvo” da atividade criminosa ou tangencial ao crime. Além do mais, a conduta criminosa associada com os crimes informáticos proporciona uma lista sem fim de atividades que podem ser abrangidas com o termo “crime informático” (VIANO, 2006 *apud* ALBUQUERQUE, 2006, p. XVII).

Portanto, a dificuldade de delimitar o que seria os crimes, via digital, está justamente em saber qual a figura ou papel preponderante do computador, no crime, e definir sua abrangência. Neste sentido, o computador pode figurar em várias posições distintas como: “alvo do crime”, “instrumentos do delito” ou “incidentes ao delito”.

1.2 OS CRIMES DIGITAIS E SUAS CARACTERÍSTICAS

A criminalidade por meio digital pode resultar em uma imensa variedade de tipos penais. Como exemplo, pode-se citar: furto de uso informático, estelionato, violabilidade de dados, senhas e correspondência, crimes contra a honra, patrimônio, violação de segredo, falsificação, atentado contra a segurança de sistemas de computador, terrorismo e assédio informático, dentre tantos outros. Por sua especialidade e variedade, há várias características próprias a serem mencionadas em relação aos crimes digitais.

1.2.1 Vulnerabilidade dos sistemas e fator distância

Quando o assunto são as características dos crimes virtuais, deve-se levar em conta que os sistemas informáticos, as transmissões de dados, redes interligadas, os sistemas automáticos, de modo geral, são alvos fáceis ou abertos para a prática de atos ilícitos.

Neste sentido, necessitam proteção especial, além de sistemas preventivos que garantam a confiabilidade, pelo menos em parte, ou dispositivos que dificultem sua violação e permita certa segurança, objetivando diminuir as vulnerabilidades neste segmento.

Levando em consideração, que os bancos de dados são fontes de informação e ainda possuem valor e projeção econômica de grande valia para empresas e instituições, certamente, a violação do suporte de dados, sistemas ou das telecomunicações causariam resultados desastrosos.

Nesse sentido, Albuquerque ressalta a questão das vulnerabilidades em geral:

> A concentração de dados em sistemas informáticos interconectados pode estimular a criminalidade informática. Uma empresa pode colocar em risco sua própria existência, ao armazenar num sistema interconectado dados sensíveis ou estratégicos com relação ao desenvolvimento de novos produtos, balanços contábeis ou listas de clientes (ALBUQUERQUE, 2006, p. 42).

Além deste fator, os delitos digitais são favorecidos nos aspectos de distância e tempo, pois, tais conceitos são relativizados em informática. Deste modo,

segundo o próprio autor, as redes de computadores e de telecomunicação eliminaram o fator distância, na prática do crime, rompem fronteiras com a maior facilidade e celeridade própria do mundo digital.

1.2.2 Fator tempo

O mesmo autor observa que: “O crime informático pode ser praticado em nanossegundos, não em horas, tampouco em minutos. Isto dificulta a chance de descobrir-se o responsável. Ele pode, dependendo do caso, levar anos para ser detectado” (ALBUQUERQUE, 2006, p. 42).

Portanto, os crimes cibernéticos têm a seu favor, a rapidez na prática do crime, o distanciamento do agente e resultado, que pode inclusive ser praticado quase que, anonimamente, em muitos casos. Estes fatores facilitam a impunidade. Criam-se novos tipos de delinquência, favorecida pelo anonimato, celeridade e distanciamento entre a ação e resultado.

1.3 BENS JURÍDICOS TUTELADOS – OBJETOS TANGÍVEIS E INTANGÍVEIS

Com o desenvolvimento da sociedade pós-industrial e as transformações tecnológicas, houve o aumento vertiginoso da informática, sistemas de transmissão e armazenamento de dados, por computador. Tais mudanças ocasionaram expressivas contribuições aos meios de comunicação, inclusive da telemática.[2]

Estas novas formas de comunicação propiciaram aumento no volume das transações financeiras, via rede, acarretando, consequentemente, maior circulação de riquezas abstratas (intangíveis), nunca vista antes.

Sendo assim, é necessário que o direito penal encare as novas demandas sociais e que trate, com maior freqüência, e de maneira mais específica, os objetos intangíveis. Sobre o escasso disciplinamento dos objetos intangíveis, Albuquerque salienta:

---

[2] A utilização e manipulação de informação que combina o uso do computador com os meios de telecomunicação é chamada de telemática (COLLI, 2010, pp.147-153).

> O direito penal enfrenta problemas ao disciplinar a criminalidade informática, já que seus fundamentos estão orientados para a proteção dos objetos tangíveis. A proteção dos objetos intangíveis já é contemplada pelo direito penal, com relação, por exemplo, aos segredos profissionais e de negócio, bem como pelo direito autoral e pelo direito das patentes, no que diz respeito, respectivamente, às obras intelectuais e invenções, mas ela não desempenhou um papel central até a segunda metade do século XX (ALBUQUERQUE, 2006, p. 44).

Sendo assim, o Direito Penal, pelos seus próprios fundamentos, têm como objeto de tutela, em regra, bens materiais ou tangíveis. No entanto, em matéria de crimes informáticos, os objetos estão no campo da intangibilidade dos bens como armazenagem, processamento e transmissão de dados, que podem ter, inclusive, valor superior a muitos objetos tangíveis tutelados.

O autor esclarece ainda que, os objetos informáticos como o armazenamento, processamento e transmissão de dados não podem ser considerados coisas móveis, conforme disposto abaixo:

> Já que dados armazenados, processados ou transmitidos por sistemas informáticos não podem ser considerados coisas móveis, eles não podem ser objeto de crimes patrimoniais clássicos, como furto, roubo, dano, apropriação indébita. Dados, objetos intangíveis, não pertencem à categoria jurídica de coisas móveis, objetos tangíveis. Quando eles são copiados, os crimes patrimoniais não ocorrem. Eles podem ser objeto de crimes patrimoniais clássicos apenas quando formarem uma unidade material com o respectivo suporte. Os dados precisam estar incorporados ao suporte. Enquanto tais eles não podem ser objeto de crimes patrimoniais. O direito penal protege o meio, objeto tangível no qual os dados estão arquivados. [...] Quem se apropria de coisa móvel, exclui outrem de sua posse. Isto não acontece com os dados (ALBUQUERQUE, 2006, p. 46).

Deste modo, é fundamental à ciência jurídica, em particular, à área penal adaptar-se às novas demandas sociais e jurídicas frutos de inúmeras transformações ocorridas nas últimas décadas, com intuito de contemplar, na legislação, novos tipos penais e formas de proteção aos bens jurídicos intangíveis, como é o caso dos crimes informáticos.

Importante destacar que a intangibilidade dos bens jurídicos, em matéria de crimes cibernéticos, alterou significativamente conceitos básicos e princípios do direito penal como: soberania, territorialidade, jurisdição, tipicidade, tempo e lugar do cometimento dos crimes, temas que serão expostos ao longo do estudo.

2 DOS PRINCÍPIOS PENAIS RELACIONADOS AOS CRIMES DIGITAIS

A ciência jurídica é regida por princípios, que são essenciais ao ramo penal, haja vista que visam assegurar garantias e, como finalidade última, a proteção. Proteção do indivíduo contra arbitrariedades, pois regem as condições da punição e lidam com valor supremo do ser humano – a liberdade.

Para Bitencourt, tais princípios orientadores servem como garantias do cidadão perante o poder punitivo do Estado. São limitadores e controladores deste monopólio estatal – o *jus puniendi.*

> Poderíamos chamar de princípios reguladores do controle penal princípios constitucionais fundamentais de garantia do cidadão, ou simplesmente de Princípios fundamentais de Direito Penal de um Estado Social e Democrático de Direito. Todos esses princípios são de garantias do cidadão perante o poder punitivo estatal e estão amparados pelo novo texto constitucional de 1988, art. 5 (BITENCOURT, 2008, p. 10).

Dentre tais princípios podem-se elencar vários que são expressivos como: Princípio da Legalidade (reserva legal), da territorialidade e extraterritorialidade, da Personalidade, dentre outros.

2.1 PRINCÍPIO DA LEGALIDADE OU DA RESERVA LEGAL

Princípio fundamental do Direito, em especial na área penal. Pela relevância do tema, ensina Bitencourt:

> O princípio da legalidade ou da reserva legal constitui uma efetiva limitação ao poder punitivo estatal. [...] Feuerbach, no início do século XIX, consagrou o princípio da reserva legal através da formula latina *nullum crime, nulla poena sine lege*. O princípio da reserva legal é um imperativo que não admite desvios nem exceções e representa uma conquista da consciência jurídica que obedece a exigências de justiça, que somente os regimes totalitários o têm negado (BITENCOURT, 2008, p. 11).

O princípio, pelo grau de importância, está inserido na Constituição Federal, no Titulo II – Dos Direitos e Garantias Fundamentais- artigo 5º, inciso XXXIX – “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”.

Ainda segundo o autor, a pena, qualquer que seja, somente tem legitimidade para aplicação, quando disposta em lei. O ordenamento jurídico deve trazer de maneira clara, precisa e definida os tipos penais que são objetos de

reprimenda estatal. São inadmissíveis tipos penais inexistentes ou demasiadamente abertos. No mínimo temerário e inaceitável em um estado democrático de direito. Ensina o autor:

> [...] pelo princípio da legalidade, a elaboração de normas incriminadoras é função exclusiva da lei, isto é, nenhum fato pode ser considerado crime e nenhuma pena criminal pode ser aplicada sem que antes da ocorrência desse fato exista uma lei definindo-o como crime e cominando-lhe a sanção correspondente. A lei deve definir com precisão e de forma cristalina a conduta proibida (BITENCOURT, 2008, p. 11).

Quando se trata de crimes cibernéticos que também podem ser chamados de crimes informáticos, *cybercrimes* ou digitais, percebe-se que a própria terminologia do assunto possui variadas formas e definições distintas para o mesmo objeto.

Assim, os tipos penais devem contemplar todos os possíveis atos envolvidos: o armazenamento, o processamento e a transmissão de dados. Devem-se buscar maneiras que abarquem as condutas dos atos ilícitos praticados pelo agente e sejam devidamente caracterizados e posto pelo legislador na lei.

A conceituação precisa, clara, objetiva faz-se necessária em respeito ao princípio constitucional da legalidade. Somente assim, é que estará em consonância com os princípios fundamentais do Direito, bem como haverá maior respaldo em termos de facilitar a investigação e o julgamento destas transgressões, não violando, portanto, a segurança jurídica e os princípios basilares do Direito. Por fim, conforme demonstrado com capítulo I deste trabalho, a dificuldade de terminologia dos conceitos nesta área, bem como a dificuldade de especificar a tipificação do crime e sua pena correspondente, no campo da informática, é um desafio a ser enfrentado pelo legislador e operadores do Direito.

2.2 PRINCÍPIO DA TERRITORIALIDADE

O Código Penal brasileiro, em seu artigo 5º estabelece: “Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional”.

> O princípio da territorialidade pode ser compreendido como aquele por meio do qual a lei penal a ser aplicada aos fatos ocorridos dentro do território de um país é a lei desse mesmo país, independentemente da nacionalidade do agente, da vítima ou do bem jurídico lesado, uma vez que os Estados exercem a sua soberania dentro e de acordo com os limites do seu espaço territorial (COLLI, 2010, p. 98).

Assim, a regra de aplicação da lei penal brasileira seria inicialmente pelo princípio da territorialidade, justificada pela noção de soberania, a qual seria o monopólio do poder do Estado, dentro de suas fronteiras. A soberania apresenta três características:

> [...] plenitude, como a totalidade de competências sobre questões da vida social; a autonomia como a rejeição de influências externas nas decisões sobre essas questões; e a exclusividade, como monopólio do poder nos limites do seu território (SANTOS *apud* BITENCOURT, 2008, p. 175).

No entanto, importante aspecto a ser abordado em matéria de crimes cibernéticos, seria a mudança de antigos conceitos de Estado-Nação e Território, considerando a transnacionalidade destes tipos de crimes e a impossibilidade de retenção de suas ações e consequências, dentro de um território definido.

Sobre este aspecto, Ferreira argumenta que a superação de conceitos de Estado-Nação não mais é possível pela delimitação de fronteiras na sua conceituação clássica. Tais mudanças são fruto do efeito da globalização e interações entre países. Consequentemente, a maior acessibilidade à internet e desenvolvimento de novas formas de comunicações que contribuíram para as transformações. Somando-se a isto, o aumento do fluxo de riqueza e transações financeiras por meio digital, acabaram por derrubar e mudar conceitos.

> As novas tendências da ordem econômica internacional, corroboradas principalmente pelo processo de globalização, tanto nas áreas econômicas, sociais, políticas e culturais, trouxeram a tona a incapacidade do Estado Nacional e do Direito em regular estas novas atividades e relações que romperam com a tradicional concepção de Estado-Nação. Isto ocasiona uma releitura em certos dogmas-conceitos, dentre eles, a soberania e a jurisdição internacional, os princípios reguladores da eficácia espacial da lei, matérias até então limitadas ao Direito Internacional Público, porém, hoje, foco de atenção das diversas áreas do Direito, dentre elas o Direito Penal (FERREIRA, 2007, p. 19).

Para a regulação das leis penais no espaço, há o princípio da territorialidade que estabelece, em regra, que cada Estado aplicará suas leis nacionais em seu território, em virtude de sua soberania.

Portanto, a territorialidade se justifica pela soberania do país em seu território e a aplicação do ordenamento jurídico, dentro dos limites de suas fronteiras sem influências externas. No entanto, a autora alerta sobre a necessidade de reanalisar o conceito de soberania, jurisdição e competência após o fenômeno da globalização. Salientando que: "[...] todas (soberania, jurisdição e competência) devem ser reanalisadas agora sob a ótica de interesse comum das nações (combate à macrocriminalidade) e um novo conceito de patrimônio comum da humanidade (segurança internacional)" (FERREIRA, 2007, p. 23).

Portanto, a autora esclarece estas mudanças conceituais clássicas advindas do uso da internet e interação entre os países. Com o aumento do fluxo de transações via *web*[3], trouxeram redefinições de conceitos e a necessidade de enfrentamento da criminalidade, não mais dentro de fronteiras, de maneira isolada, mas ampliando para o combate transnacional. Tais crimes afetam toda comunidade internacional. Agora, a criminalidade é transnacional, também denominada de macrocriminalidade, não mais submetida a uma única jurisdição ou território. Assim, a necessidade de ampliação de conceitos e maior cooperação entre as nações, haja vista a mudança de perfil do crime, não isolado ou dentro dos limites fronteiriços, mas pulverizados por diversas nações sob as mais diversas jurisdições, simultaneamente.

---

[3] *World Wide Web*: conjunto interligado de documentos em hipertexto, que se convencionou chamar de páginas da *Web* (ALBUQUERQUE, 2006, p. 193).

> Na seara do Direito Penal, observa-se uma nova figura conhecida como macrocriminalidade, que rompe os limites criando uma rede de criminalidade mundial, sem respeito à soberania ou qualquer sistema de acordo internacional realizado entre os Estados. É o caso dos crimes cometidos por meio da internet, considerando o avanço da macrocriminalidade e a dependência do sistema informático entre os Estados, em virtude da globalização das informações e comunicações (PINHEIRO, 2009, p. 35).

Nesta mesma linha de pensamento e tendo também de repensar o conceito de soberania e fronteiras para Direito Digital, a autora destaca:

> Convergência, seja por internet, seja por outro meio, elimina a barreira geográfica e cria um ambiente de relacionamento virtual paralelo no qual todos estão sujeitos aos mesmos efeitos, ações e reações. É importante ressaltar, por último, que essa discussão sobre territorialidade não se esgota na necessidade de solucionar casos práticos, mas nos faz repensar o próprio conceito de soberania e, consequentemente, a concepção originária do próprio estado de direito (PINHEIRO, 2009, p. 38).

A criminalidade informática, portanto, rompe fronteiras e redefine o conceito de soberania e territorialidade, pois trata-se de macrocriminalidade, difícil, ou melhor, impossível de limitar em fronteiras físicas. Há necessidade de ampliar os conceitos tradicionais, bem como aumentar as hipóteses de extraterritorialidade para o combate destes delitos em especial, os digitais.

2.3 PRINCÍPIO DA EXTRATERRITORIALIDADE

O princípio da extraterritorialidade da lei penal é uma exceção ao da territorialidade. A lei penal elenca os casos em que será aplicada a lei brasileira fora do território nacional. Pode ser dividida em:

a) extraterritorialidade incondicionada - art.7º, inciso I do Código Penal (CP); e

b) extraterritorialidade condicionada – que depende de condições descritas do art. 7º, inciso II e §§ 2º e 3º, do CP.

A extraterritorialidade vem estampada no CP, nos seguintes termos:

> Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:
> I – Os crimes:
> a) Contra a contra a vida ou a liberdade do Presidente da República;[4]
> b)Contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público;[5]
> c)Contra a administração pública, por quem está a seu serviço;[6]
> d)de genocídio, quando o agente for brasileiro ou domiciliado no Brasil.[7]
> II- os crimes:
> a)que, por tratado ou convenção, o Brasil se obrigou a reprimir;[8]
> b)praticados por brasileiro[9];
> c)praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados.
> § 1º Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro.
> § 2º Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições:
> a)entrar o agente no território nacional;
> b)ser o fato punível também no país em que foi praticado;
> c)estar o crime incluído entre aqueles que a pelos quais a lei brasileira autoriza a extradição;
> d)não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena;
> e)não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.
> §3º A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se reunidas as condições previstas no parágrafo anterior.[10]
> a) não foi pedida ou foi negada a extradição;
> b) houve requisição do Ministro da Justiça.

Como visto anteriormente, pela intangibilidade dos crimes cibernéticos com sua velocidade de cometimento, características próprias, com inevitável superação dos limites territoriais e redefinição de soberania, faz-se necessária a aplicação mais frequente do princípio da extraterritorialidade aos casos concretos que envolvam crimes digitais.

Bitencourt ensina que o Princípio da Nacionalidade ou da Personalidade visa alcançar os nacionais que não estão dentro do território.

---

[4] Princípio da Defesa, Real ou da Proteção.
[5] Princípio da Defesa, Real ou da Proteção.
[6] Princípio da Defesa, Real ou da Proteção.
[7] Princípio da Justiça Universal ou Cosmopolita.
[8] Princípio da Justiça Universal ou Cosmopolita.
[9] Princípio da Personalidade ou da Nacionalidade Ativa.
[10] Princípio da Personalidade Passiva.

> Aplica-se a lei penal da nacionalidade do agente, pouco importando o local em que o crime foi praticado. O Estado tem o direito de exigir que o seu nacional no estrangeiro tenha determinado comportamento. Esse princípio pode apresentar-se sob duas formas: *personalidade ativa* – caso em que se considera somente a nacionalidade do autor do delito (art. 7º, II, b, do CP); *personalidade passiva* – nesta hipótese importa somente se a vítima do delito é nacional (art.7º, §3º, do CP) (BITENCOURT, 2008, p. 176).

O sentido do princípio, segundo o autor, seria evitar ou impedir a impunidade por crimes praticados em outros países, não abrangidos pelos critérios da territorialidade.

2.4 PRINCÍPIO DA JUSTIÇA UNIVERSAL OU COSMOPOLITA

O Princípio da Justiça Universal ou Cosmopolita é fundamental à segurança jurídica e prega que as leis penais devem ser aplicadas a todos, indistintamente.

> Esse princípio é característico da cooperação penal internacional, porque permite a punição, por todos os Estados, de todos os crimes que forem objeto de tratados e de convenções internacionais. Aplica-se a lei nacional a todos os fatos puníveis, sem levar em conta o lugar do delito, a nacionalidade de seu autor, ou do bem jurídico lesado (art. 7º, II, a, do CP). A competência aqui é firmada pelo critério da prevenção (BITENCOURT, 2008, p. 176).

Para os crimes cibernéticos, este princípio tem importância, pois permite ampliar a abrangência do direito penal e alcançar a punição dos sujeitos ativos onde quer que se encontrem ou a que nacionalidade pertença.

Como ensina Mestieri (1990 *apud* BITENCOURT, 2008, p.176): “o fundamento desta teoria é ser o crime um mal universal, por isso todos os Estados têm interesse em coibir a sua prática e proteger os bens jurídicos da lesão provocada pela infração penal”.

Portanto, tal princípio está previsto no art. 7º, inciso I, “d” e II, “a”, do Código Penal como citado anteriormente. É permitido aos Estados o direito de julgar pelo próprio ordenamento jurídico ou, em seu território, todas as infrações que afetem bens e interesses da comunidade internacional, ou seja, os crimes que estão elevados a categoria de crimes transnacionais que atingem vários países com necessidade de repressão uniforme.

2.5 PRINCÍPIO DA DEFESA, REAL OU DA PROTEÇÃO

O princípio da Defesa Real ou da Proteção, em termos de extraterritorialidade da lei penal, é a condição do país de se defender dentro dos seus limites territoriais, em regra. No entanto, há a possibilidade de aplicação da legislação nacional além fronteiras, em casos excepcionais, quando o bem jurídico lesionado é considerado fundamental. É condição extraordinária a aplicabilidade da lei nacional, fora dos limites da própria soberania, contudo, somente é possível devido ao grau de importância do objeto a ser tutelado.

Sobre a necessidade de extensão da jurisdição diante da realidade da globalização quando o assunto é a proteção aos bens fundamentais que ultrapassam fronteiras, Bitencourt ensina:

> Esse princípio permite a extensão da jurisdição penal do Estado titular do bem jurídico lesado, para além dos seus limites territoriais, fundamentado na nacionalidade do bem jurídico lesado. (art. 7º, I, do CP), independentemente do local em que o crime foi praticado ou da nacionalidade do agente infrator. Protege-se, assim, determinados bens jurídicos que o Estado considera fundamentais. [...] Em tempos de “economia global” os interesses nacionais têm sido violados, desrespeitados e, às vezes, até ultrajados no estrangeiro, com grande frequência. Por isso, esse princípio adquire grande importância na seara do *Direito Penal no espaço,* ante a necessidade do Estado, cada vez mais, proteger seus interesses além fronteiras (BITENCOURT, 2008, p. 176).

Pela relevância e enfrentamento da matéria, necessariamente, abarca desafios, principalmente no âmbito jurídico. A Ciência Jurídica terá de interagir nos conceitos de direito penal e de direito internacional, objetivando conseguir tipificar crimes supranacionais e respectivo julgamento. As cortes internacionais deverão estar aptas e especializadas para dirimir as controvérsias existentes, aliados, também, à estrutura nacional eficaz, para auxiliar. Assim, o objetivo de buscar garantir a segurança da informação e de navegação no ciberespaço, bem como diminuir e punir os criminosos, em qualquer lugar ou nacionalidade a que pertençam, em velocidade compatível com as mudanças tecnológicas, são essenciais para o sucesso no combate a esta espécie de crime.

2.6 COOPERAÇÃO INTERNACIONAL

Diante da impossibilidade de delimitação da fronteira nestas espécies de crimes, bem como a possibilidade de vasta repercussão de resultado negativos, nos delitos digitais, é imprescindível definir qual deve ser o ordenamento jurídico a ser aplicado ao caso concreto.

Pinheiro fala que, quando há estrapolação dos limites fronteiriços e quando há possibilidade de aplicação de leis múltiplas, com variadas opções de ordenamentos jurídicos, requer que haja a definição do país considerando a origem do ato e seu respectivo efeito.

> Como referência o Direito Internacional, pelo qual se estabeleceu que, para identificar a norma a ser aplicada, diante da extrapolação dos limites territoriais dos ordenamentos, deve-se averiguar a origem do ato e onde este tem ou teve seus efeitos, para que se possa aplicar o Direito do país que deu origem ou em que ocorreram os efeitos do ato (PINHEIRO, 2009, p. 38).

Portanto, quando os delitos estão elevados à categoria da macrocriminalidade, é de suma importância a cooperação internacional, na investigação e/ou jurisdição internacional, apta para enfrentamento das demandas.

Ferreira aponta algumas tentativas e exemplos concretos adotados pelo Brasil, em matéria penal, quanto à soberania compartilhada. Assim, ações que visam submeter o Brasil ao ordenamento internacional (corte internacional) sejam por assinatura de tratados ou termos como nos exemplos abaixo:

> a)Emenda Constitucional 45/04 que elevou à categoria de emenda constitucional os tratados e convenções internacionais sobre direitos humanos, bem como, se submeteu à Jurisdição do Tribunal Penal Internacional, instituído pelo Estatuto de Roma (CF, art. 5º,§§ 3º e 4º);
> b) Carta dos Direitos das Pessoas perante a Justiça no âmbito do Judiciário Ibero-americano, assinada em 29.11.2002 na cidade do México, durante a VII Cúpula Ibero-americana de Presidentes de Cortes Supremas e de Tribunais Superiores de Justiça;
> c)Medida Provisória 27, de 24.1.2002, que dispõe sobre infrações penais de repercussão interestadual ou internacional que exigem repressão uniforme.
> d)Decreto 3468 de 17.5.2000 promulga o Protocolo de Assistência Jurídica Mútua em Assuntos Penais, entre o Brasil e os países da Argentina, Paraguai e Uruguai, em decorrência da assinatura do Tratado de Assunção (Mercosul);
> e)Convenção de 1971 para prevenir e punir os atos de terrorismo configurados em delitos contra as pessoas e a extorsão conexa, quando tiverem eles transcendência internacional, promulgada pelo Dec. 3018, de 6.4.1999;
> f)Acordos de Cooperação Judiciária e Assistência Mútua em Matéria Penal entre o Brasil e a Itália (Dec. 862, de 9.7.1993), Portugal (Dec. 1320, de

> 30.12.1999), Colômbia (Dec. 3895, de 23.8.2001), Estados Unidos da América (Dec. 3810, de 2.5.2001)
> g)Decreto de 7.6.1993 declara o Grupo Brasileiro da Associação Internacional de Direito Penal, sociedade civil sem fins lucrativos, entidade consultiva, em matéria criminal, do Conselho Nacional de Política Criminal e Penitenciária (CNPCP), órgão do Ministério da Justiça;
> h)Decreto 585, de 26.06.1992, promulga acordo sobre a gratuidade parcial da execução das Cartas Rogatórias em Matéria Penal, entre o Governo do Brasil e França (FERREIRA, 2007, pp. 67-68).

Como exposto, os delitos digitais e tantos outros rompem fronteiras facilitadas, pelo fenômeno da globalização, e inseridos nesta nova criminalidade contemporânea devem ser tratadas de forma diferenciada, com possibilidades de ampliação do processo investigativo, com intercâmbio de informações.

Há, portanto, mais do que nunca, a necessidade de cooperação internacional, pois os fenômenos do crime, extrapolando as fronteiras físicas, exigem união entre os países. Albuquerque destaca a importância da cooperação internacional em crimes transfronteiriços:

> A cooperação internacional é de grande importância tanto para a investigação quanto para o julgamento de crimes informáticos com repercussões internacionais. Se surgirem paraísos do crime informático, à semelhança dos paraísos fiscais, locais em que sua prática for livre, conseqüências nefastas podem disseminar-se nos cinco continentes. A diversidade jurídica existente na comunidade internacional na tipificação dos crimes informáticos também pode dificultar sua investigação e julgamento, da mesma maneira que as assimetrias de jurisdição, na determinação do lugar do crime. Ambos os fatores, conjuntamente com os próprios recursos da informática, podem ser explorados por infratores, numa tentativa de reduzir riscos de punição (ALBUQUERQUE, 2006, p. 74).

Igualmente, a questão da soberania com o advento da internet proporciona a desconstituição dos limites das nações. Os crimes digitais têm o potencial de se tornarem transnacionais. Consequentemente, impedindo, dificultando a detecção, o processamento e a respectiva punição de tais delitos. A internet contribui e cria nova categoria de delinquente favorecida pela segurança do anonimato e dificuldade de captura do agente do crime.

3 A INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

Diante da acessibilidade do uso da internet e dos meios digitais, os crimes cibernéticos estão cada vez mais recorrentes. O ritmo de aumento de incidência das vítimas é vertiginoso e, exponencialmente, crescente.

Inicialmente, com a finalidade de dimensionar a grandiosidade do problema, acerca da criminalidade informática, seguem reportagens recentes veiculadas na mídia digital, em setembro de 2011, sobre o tema. Reportagens estão em variados sentidos e dispõem sobre invasões de *hackers* com acessos não autorizados em sistemas informáticos inclusive em páginas sociais de milhares de pessoas. Mostra ainda, o aumento dos casos e vítimas em todo Brasil e no mundo, com prejuízos que chegam as cifras dos milhões e bilhões de dólares. A seguir, coletânea de reportagens das mais variadas abordagens e em diferentes modos de agir (*modus operandi*) dos criminosos, publicadas recentemente (setembro de 2011), no *site* Universo *On Line* – UOL, coluna de Notícias:

> **CRIMES CIBERNÉTICOS:** Levantamento feito no último ano trouxe número assustador de vítimas de crimes cibernéticos no Brasil, a estimativa é de 80% do total de usuários adultos da Rede no Brasil. Os delitos (invasão de perfis em redes sociais, *spyware, phishing, spam* etc) além de causarem imenso prejuízo financeiro acarretam a perda de tempo para resolver problemas relacionados aos golpes. A análise demonstra que os crimes cibernéticos são mais comuns do que outros tipos de crimes, 8 em cada 10 internautas disseram já terem sofrido golpes on line. No último ano, mais de 80% dos usuários adultos de internet no Brasil foram vítimas de crimes cibernéticos, como invasão de perfis em redes sociais, *phishing, vírus* e outros *malwares*. No total, cerca de 77 mil brasileiros sofrem golpes *on line* por dia. Os dados fazem parte de um levantamento mundial divulgado pela Norton nesta terça-feira (20) em São Paulo.No mundo, o número de vítimas diárias é de 1 milhão. O prejuízo anual, em dólares, é de US$ 388 bilhões. Só no Brasil, isso chega a US$ 60 bilhões (o equivalente a R$ 104 bilhões). Quando comparado ao prejuízo causado, por exemplo, pelo tráfico de drogas como maconha, cocaína e heroína combinados -- que alcançam US$ 288 bilhões anualmente, segundo o estudo -- os crimes cibernéticos pesam mais."Quando vemos esses números temos ideia de como os crimes cibernéticos são um perigo sério. É um crime organizado, que lucra muito com os golpes, e que deve receber toda atenção das autoridades para que seja combatido", alertou Adam Palmer, consultor líder em ciberseguranca da Norton.No Brasil, outro dado mostra como os crimes na internet são comuns: cerca de 8 em cada 10 internautas do país disseram já terem sofrido golpes *on line*. Esse tipo de crime é, inclusive, mais comum que os da "vida real": cerca de 19% dos entrevistados brasileiros disseram ter sido vítimas de crimes no mundo físico, ante a 59% no mundo virtual.Além do prejuízo financeiro, há também a perda de tempo para resolver problemas relacionados a esses golpes. Brasileiros vítimas de crimes cibernéticos passaram 11 dias tentando resolver problemas relacionados a eles nos últimos 12 meses. A maioria deles (69%) revelou que não possuía uma

solução de segurança atualizada.Para o estudo sobre crimes cibernéticos, a Norton entrevistou 19 mil pessoas em 24 países. A definição do que é um crime na internet não leva em consideração a legislação dos países estudados, mas o testemunho dos entrevistados que disseram ter sofrido os golpes. Golpes-Comuns - Segundo a Norton, vírus que contaminam computadores e *malwares* são o problema mais comum no Brasil, com 68%. Invasão a perfis em redes sociais ficaram com 19% e mensagens de phishing com 11%.

INVASÃO EM REDES SOCIAIS: Segundo o pesquisador de segurança da *Sophos*, *Chet Wisniewski*, a *Timeline* oferece informações preciosas para a captura de senhas. O novo recurso *Timeline* do *Facebook* tornará ainda mais fácil para os criminosos da Internet obterem informações na popular rede social para o uso em ataques *on line* e para o roubo de senhas, afirma o especialista em segurança *Chet Wisniewski*, pesquisador da empresa *Sophos*. Anunciado na semana passada por *Mark Zuckerberg*, CEO do *Facebook*, o recurso, que deve estar disponível para todos os usuários nas próximas semanas, oferece um resumo de importantes fatos nos últimos anos de quem tem conta no serviço. Segundo Zuckerberg, ele mostra “a história da sua vida”. “Ele traz informações que já estão no *Facebook*, mas que não estavam organizadas de forma a serem acessadas tão facilmente”, explica *Wisniewski*. "Os *crackers* (criminosos da Internet) com freqüência garimpam informações em redes sociais para golpes on line, e a *Timeline* tornará a tarefa um trabalho muito simples", destaca. Como as pessoas costumam utilizar informações pessoais para montar suas senhas ou mesmo para as chamadas questões de segurança (perguntas que liberam o envio de senhas que foram esquecidas), o risco com a oferta da Timeline aumenta, segundo ele. “Você se lembra da invasão da conta da ex-governadora do Alasca, *Sarah Palin*? O *hacker* achou a resposta, que levou à senha dela, na Internet”, afirma o especialista. Em uma pesquisa feita pela *Sophos* em seu site, cerca de 50% dos respondentes afirmaram estar preocupados com o novo recurso do *Facebook*.

DISSEMINAÇÃO DE VIRUS/*SPAM'S*: FBI caça russo suspeito de liderar rede que enviava 30 bilhões de *spam's* por dia. A Microsoft entregou ao FBI, polícia federal norte-americana, evidências que podem ajudar no rastreamento e acusação legal do líder de uma das maiores redes de *spam's* do mundo, que enviava 30 bilhões de *e-mail's* por dia. As informações são do “*Register*”. De acordo com documentos da Corte Federal de Washington, o líder da Rustock, como ficou conhecida a rede de *spammers*, é um cidadão russo que usava o apelido de *Cosma2k*. Ele comprava endereços IP para hospedar o comando da rede e controlar servidores. Investigadores da Microsoft afirmam que o suspeito distribuía *malwares* e está envolvido com o envio de spam sobre medicamentos. “Isso sugere que o indivíduo é diretamente responsável pela rede de *spam's* como um todo, tanto que parte de seu apelido faz parte do código da rede *botnet*”, diz o testemunho fornecido pela empresa. A Microsoft já havia oferecido US$ 250 mil por informações sobre os responsáveis pela Rustock, além de publicar anúncios em jornais russos para satisfazer requisições legais sobre a notificação dos suspeitos sobre a ação legal. Autoridades federais nos Estados Unidos conseguiram encerrar em março deste ano as atividades de uma das maiores redes de *spam's* do mundo após uma denúncia da Microsoft. Chamada de Rustock botnet, o grupo *spammer* utilizava uma rede vasta de computadores ao redor do mundo – cerca de 1 milhão de máquinas – infectados com um software malicioso. Ele permitia aos cibercriminosos distribuir volumes enormes de spam, oferecendo desde programas falsificados a produtos farmacêuticos. O volume de *e-mail's* enviados era de quase 30 bilhões por dia. A Microsoft havia aberto, no final de fevereiro, uma ação civil em Seattle contra essa rede. Investigações internas da empresa identificaram onde a rede *botnet* tinha hospedagem em servidores nos Estados Unidos. Com as

> informações, agentes federais conseguiram apreender os computadores que a hospedavam em sete cidades do país. De acordo com a empresa de segurança *Symantec*, a *Rustock* foi responsável pelo envio da metade de todos os *e-mail's* de *spam* no mundo em 2010.
>
> **ATAQUES DE *HACKERS*/ACESSO NÃO AUTORIZADO A SISTEMAS:** *Hackers* atacam maior fabricante de armas do Japão (DA EFE, EM TÓQUIO).O grupo japonês MHI (*Mitsubishi Heavy Industries*), fabricantes de material para usinas nucleares, fornecedores do Ministério da Defesa e maior fabricante de armas do Japão, sofreu ataques de *hackers*, que podem ter tido acesso não autorizado a seu sistema, informou nesta terça-feira (20) a agência "Kyodo". O grupo IHI (*Ishikawajima-Harima Heavy Industries*) também foi alvo dos criminosos. A corporação denunciou nesta terça-feira que, desde o primeiro semestre, seus servidores e PC's receberam uma onda de *e-mail's* infectados com vírus, que caso fossem abertos poderiam causar falhas de segurança. O grupo, que fornece à Defesa japonesa peças de motor para aviões caça, afirmou, no entanto, que nenhum de seus computadores foi infectado. Já a MHI reconheceu que cerca de 80 servidores e computadores do grupo, incluindo alguns com informações técnicas sobre submarinos, mísseis e usinas nucleares, foram infectados com pelo menos oito tipos de vírus, entre eles o "Cavalo de Tróia", que permite aos *hackers* operar o computador e enviar dados procedentes do mesmo. A companhia admitiu um vazamento de informações de seu sistema de redes, como direções IP, o que permitiria executar novos ataques, mas destacou que por enquanto não foi confirmado nenhum vazamento sobre seus produtos e tecnologia. Tanto a IHI como a MHI trabalham na fabricação industrial de material de Defesa e peças para usinas nucleares, como recipientes e contêineres, por isso não se descarta que ambos tenham se tornado alvos prioritários dos hackers. O titular de Defesa japonês, Yasuo Ichikawa, afirmou por sua vez que, por enquanto, não foi informado do vazamento "de dados importantes" e apontou que seu ministério abrirá sua própria investigação sobre o caso (IEKA, 2011).

A seguir, serão abordados os entraves jurídicos e os procedimentos investigativos dos crimes cibernéticos por sua especialidade e amplitude.

3.1 CIBERNÉTICA, CIBERESPAÇO E CIBERCRIME

Inicialmente, a definição do que é cibercrimes. Colli faz interligações entre os conceitos de cibernética, ciberespaço e crime informático, objetivando conceituar cibercrime, crimes informáticos praticados pela internet, e expõe:

> Os cibercrimes pressupõem o envolvimento de mais de um computador ou dispositivo telemático ou eletrônico. Além disso, estas máquinas devem estar conectadas entre si por uma rede, seja ela material, seja ela imaterial (por exemplo, redes *wireless*). A ligação entre cibernética, ciberespaço e crimes informáticos permite que se compreenda o instituto do cibercrime como sendo aquele no qual um ou mais computador(es), equipamentos telemáticos ou dispositivos eletrônicos, interligados por meio de uma rede de computadores, são utilizados, por um ou mais indivíduos, no cometimento de uma, ou mais, conduta(s) criminalizada(s), ou são alvo(s) desta(s). O homem interagindo com uma máquina – retroalimentando-a com informações por meio de mensagens – através de uma rede de computadores (cibernética) interligados (ciberespaço), agindo conforme uma conduta previamente criminalizada (crime informático) estereotiparia um modelo de cibercrime (COLLI, 2010, p. 44).

As questões problemáticas relevantes, acerca das investigações dos cibercrimes, considerando as peculiaridades enfrentadas nestes tipos de delitos estão, segundo Colli (2010, p. 48), nos seguintes aspectos: a) quanto à natureza jurídica; b) aos sujeitos; c) ao tempo; d) ao lugar; e) às provas obtidas.

Antes de adentrar ao tema da investigação, propriamente dita, destes delitos informáticos, é essencial fazer distinções para classificar as atitudes criminosas, por categorias. A doutrina apresenta diferenciações entre delitos informáticos e criminalidade na internet e suas possíveis classificações (grifo nosso).

> Gonzalo Rodríguez Mourullo, Jaime Alonso Gallo e Juan Antonio Lascuraín Sanchéz apresentam a seguinte distinção: os delitos informáticos teriam como objeto de ataque um elemento informático, ou seja, dados e/ou sistemas informáticos, enquanto que a criminalidade na internet seria o instrumento do delito. Esta classificação tem duas categorias de crimes informáticos, distinguindo crimes cometidos contra um sistema de informática dos cometidos por meio de um sistema (FERREIRA, 2007, p. 101).

Tal classificação seria importante para verificar e distinguir entre o foco (alvo) do sujeito ativo para o delito o qual teria por objetivo atingir ou invadir algum sistema informático. Pode-se classificar, também, por: a) delitos informáticos Próprios (Puros ou Comuns), em que o resultado seria a violação do sistema em si; b) Impróprios (Impuros ou Específicos) quando o computador seria meio (“arma”), para o cometimento de algum outro crime já tipificado pelo Código Penal. Para Silva (2003 *apud* FERREIRA, 2007, p. 103) o delito do tipo Impróprio seria: “[...] o computador é usado apenas como instrumento para o ataque do bem jurídico (crime de pedofilia, tráfico de entorpecentes e armas, crimes contra a honra, são alguns exemplos)”.

Albuquerque também faz a distinção de crimes informáticos comuns (*traditional computer crimes),* nos quais os recursos informáticos são utilizados como

meio-fim, para o cometimento de crimes e que possuem previsão no ordenamento jurídico penal. Já os crimes informáticos específicos (*computer specific crimes*), as condutas lesam bens jurídicos ainda não tutelados pela norma penal, estando, portanto, sem proteção jurídica alguma. Caracteriza, portanto, atipicidade ou ausência de tipicidade. Deste modo, não haveria como cogitar a ocorrência do crime justamente por sua atipicidade. Assim, seria em tese crime, no entanto, sem possibilidade de repreensão.

> Nos crimes informáticos comuns, a informática é utilizada como meio para a prática de condutas que já são consideradas crime pelo direito penal vigente. A conduta ilícita já é objeto de punição. A situação não é a mesma com os crimes informáticos específicos, em que se praticam condutas contra bens jurídicos que ainda não são objeto de tutela penal. No caso dos crimes comuns, o fato de a informática ser utilizada como meio para a prática do crime não desvirtua o tipo penal, não impede, necessariamente, que ele incida. O instrumento informático pode não ser essencial para que se cometa o crime, que poderia ser praticado por meio de outra ferramenta. Com os crimes informáticos específicos, a situação é diferente. Como se praticam condutas conta bens jurídicos que ainda não são objeto de tutela, o direito penal pode não incidir, por atipicidade. O crime informático constitui uma parte de uma forma mais ampla de atividade criminosa, o crime do colarinho branco (ALBUQUERQUE, 2006, pp. 40-41).

Ferreira classifica e separa por categorias das ações delitivas em matéria cibernética, citando diversos autores, dentre eles, Rodrigues (2002 *apud* FERREIRA, 2007, p. 102) que as classifica como:

> a) Manipulação de dados ou informações contidos nos arquivos ou suportes informáticos alheios;
> b) Acesso aos dados e/ou utilização dos mesmos por quem não está autorizado, os denominados acessos não autorizados ao sistema podem ser realizados com a utilização de senhas ou através de falhas do sistema;
> c) Introdução de programas ou rotinas em outros computadores para destruir informações, dados ou programas, também conhecido como: produzir ou disseminar vírus de computador, ou seja, não só a produção do vírus como a sua disseminação, permitindo que outros dele se utilizem;
> d) Utilização de computadores e/ou programas de outra pessoa com o fim de obter benefícios próprios em prejuízo de outros;
> e) Utilização de computadores com fins fraudulentos, utilizando-se principalmente os ataques DoS (*denial of service*)[11];
> f) Agressão à privacidade mediante a utilização e processamento informático de dados pessoas com o fim distinto do autorizado;

[11] DoS (*Denial-of-service attacks*): remessa deliberada de uma grande quantidade de dados a um *website*, com o fim de levá-lo ao colapso (ALBUQUERQUE, 2006. p. 191).

Nesta mesma linha, Colli relata a dificuldade de conceituação e classificação dos delitos digitais e alerta que o conceito não deve se restringir apenas ao uso do computador:

> Os crimes informáticos envolvem (con)fusão e divergência em sua conceituação e classificação. A tentativa de estabelecer um critério de definição conceitual, formal objetivo e sucinto acerca do instituto apresenta desvantagens, uma vez que não há que se falar em uma única espécie de crime praticado a partir de recursos informáticos. Além disso, não se deve limitar o conceito do instituto à mera utilização de computadores (COLLI, 2010, p. 42).

Além da dificuldade de conceituação e classificação, Ferreira (2007, p. 103) ressalta também a situação brasileira que está regulada por leis esparsas e a legislação não trata o assunto de forma específica. As leis existentes elencam alguns crimes em que é utilizado o meio da informática para o seu cometimento. No entanto, a legislação brasileira não possui em seu ordenamento jurídico a regulamentação do delito informático, de forma autônoma. Segundo a autora, há países que possuem legislação mais específica, e cita alguns países mais avançados em termos de repressão a estes crimes. Segue a autora: “alguns ordenamentos já regularam especificadamente o delito informático de forma autônoma, entre eles França, Alemanha, Reino Unido, Canadá, Austrália, Itália, Venezuela, Holanda e praticamente todos os Estados Americanos”.

Na sequência, a autora apresenta classificação informal, com enfoque na atuação e resultados produzidos para os crimes da informação, frente à doutrina nacional.

O ordenamento brasileiro não possui regulamentação específica, sistemática e de forma autônoma, como diversos países do mundo. No entanto, há tentativa de classificação em categorias, de maneira ampla com campos abertos de atuação, pelos resultados produzidos e bem jurídico atingido.

> a) Crimes econômicos: espionagem, pirataria, sabotagem, acesso não autorizado.
> b) Ofensas com direitos individuais: uso incorreto de informação, obtenção ilegal de dados, revelação ilegal de informação;
> c) Ofensas com interesses supra-individuais: crimes contra a humanidade, políticos, fiscais, entre outros (FERREIRA, 2007, p. 103).

Diante da dificuldade de conceituação vista anteriormente e, consequentemente, sua adequada classificação, seguem exemplos (tipos) de delitos informáticos. Em pesquisa sobre o assunto em que quantifica alguns danos e/ou perigo de dano dos *cibercrimes* apresentados em relatórios anuais (2008) sobre crimes informáticos e crimes praticados pela internet, da CSI (*Computer Security Institute*) e da IC3 (*Internet Crime Complaint Center*), Colli expõe:

> Com base nos dados trazidos pelos relatórios da CSI e da IC3 foi possível constatar-se que, em relação aos três exemplos aqui apresentados – os quais envolvem a invasão de rede wireless, o compartilhamento ilícito de arquivos na internet e o uso de spam, *phishing* (páginas de um website) e engenharia social, a pesquisa da CSI demonstrou que em 50% dos casos houve a ocorrência de questões de segurança ligadas a vírus de computadores, em 44% de *insider abusers*[12], em 42% de fraudes em laptops-dispositivos que hoje em dia, em sua maioria, têm capacidade de acesso wireless -, em 29% de acessos não autorizados – invasões propriamente ditas – e em 12% de fraudes financeiras. Em relação ao levantamento feito pela IC3, foram 275.284 ocorrências registradas em 2008, um aumento de quase 70 mil novos casos relatados em relação ao ano anterior. Em 74% dos casos levados ao conhecimento da IC3 houve o emprego de *e-mail* como tentativa de levar a cabo a infração: em 28,9% o uso de *webpages* – geralmente com *phishing* estando agregado – e em 10,3% o uso de *instant messengers* – comunicadores instantâneos de mensagens, como por exemplo, o MSN Messenger, ICQ, AOL IM e o Yahoo! Messanger. Além disso, este relatório salienta o aumento do uso, nestes crimes, do chamado *blended and cross-protocol theats*, ou seja, o uso da combinação de diferentes métodos para a consecução de um objetivo ligado a um *cibercrime* (COLLI, 2010, pp. 49-50).

Constatam-se diversas tentativas de distinção entre delitos informáticos e criminalidade na internet, bem como de classificação em categorias, mesmo que amplas. Mostram-se claramente, tentativas de divisão quanto à repercussão do resultado. Esta classificação objetiva identificar os bens jurídicos atingidos pelas ações delitivas utilizando-se tanto o computador como instrumento (meio) ou como alvo de ataque.

3.2 QUESTÕES ESPECÍFICAS NAS INVESTIGAÇÕES DE CIBERCRIMES

As questões relevantes acerca das investigações dos cibercrimes, levando em consideração as peculiaridades destes tipos de delitos, segundo Colli (2010, p. 48),

---

[12] *Insider Abuser*: abuso ou uso indevido de uma rede por alguém que nela tenha ingressado ou dela faça parte (do inglês *insider*, ou quem está dentro) (COLLI, 2010. p. 49).

estão nos seguintes aspectos: a) quanto à natureza jurídica; b) aos sujeitos; c) ao tempo; d) ao lugar; e) às provas obtidas.

3.2.1 Quanto à natureza jurídica

A infração penal, para a sua caracterização, deverá reunir, simultaneamente, os elementos da: tipicidade + ilicitude + culpabilidade. O princípio da Reserva Legal (não há crime nem pena sem prévia cominação legal), os crimes informáticos, novamente irão esbarrar na questão da tipicidade do delito, além da velocidade da tecnologia em detrimento da produção legislativa, com tipos que ainda não foram positivados na lei brasileira. Desta maneira, caso haja um cibercrime, deve-se considerar se há fato lesivo a bem jurídico protegido pelo ordenamento jurídico, para caracterização de sua tipicidade, elemento este essencial e inicial, para configuração de infração penal.

Os crimes informáticos, muitas vezes, esbarrarão nesta problemática da ocorrência de determinada ação ilícita, com repercussão negativa e afetando determinado bem jurídico, mas que, no entanto, não poderá haver repreensão penal, pois será irrelevante ao direito penal haja vista a inexistência de tipicidade para o ato.

Contrário a esta ideia de ausência de tipicidade na maioria dos crimes informáticos, Inellas (2009, p.37), com foco na ausência de legislação específica sobre crimes virtuais, faz considerações a respeito da época do nosso Código Penal de 1940 e defende que a maiorias das infrações penais cometidas pela internet podem ser capitulada nas condutas já previstas no Código Penal em vigor, apenas sendo diferenciado pela utilização do meio próprio, o digital.

> Os crimes cometidos através da internet são delitos como quaisquer outros; somente seu modo de execução é diferente. [...] a dificuldade na parte investigatória seja os procedimentos executados de forma diferente e difícil e a prisão em flagrante delito é praticamente impossível de ser realizada (INELLAS, 2009, p. 37).

Para exemplificar, Colli faz paralelo entre o mundo real e virtual com a respectiva tipificação e análise aos casos concretos se haveria ou não infração penal.

> Uma invasão como meio de obtenção de dados de conta de um correntista, para posterior saque sem autorização, caracterizaria, na verdade, uma infração penal, qual seja, o furto qualificado pela fraude (CP, art. 155, §4º, II). Mas, e diante de um mesmo exemplo onde não haja toda a trama detrás daquela invasão, e se o roteador wireless daquele exemplo não possuísse segurança, nem uso de criptografia, estando aberto e acessos externos – como ocorre na maioria dos *hotspots*?[13]E se um dos sujeitos que acessasse esta rede utilizasse um *sniffer*[14] para angariar informações transmitidas. Haveria algum tipo de infração penal? A resposta seria afirmativa. Estar-se-ia diante do delito de interceptação de comunicações de informática, tipificado no art. 10 da Lei 9296, de 24.07.1996 – "constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo de Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa". E no compartilhamento de arquivos, há infração penal? A resposta dependerá do arquivo que estiver sendo compartilhado. Se houver o compartilhamento de imagens de pornografia ou sexo explícito de crianças ou adolescentes, poderá incidir um dos tipos penais do art. 240, 241-A, 241-B, 241-C ou 241- Estatuto da Criança e do Adolescente – Lei 8.069/90. Diante do compartilhamento de arquivos cuja proteção esteja elencada em um dos incisos do art. 7º da lei 9.610/98 (legislação sobre direitos autorais), poderá ocorrer a incidência dos art. 12 da Lei 9.609/98 – em se tratando de softwares piratas - dos artigos 180 (receptação) e/ou 184 (violação de direitos autorias) do Código Penal (COLLI, 2010, p. 82).

Portanto, a existência ou não de tipificação, para determinado ato delituoso, é fundamental para dar início à instrução investigatória e fundamental para nortear o trabalho policial.

Outro exemplo citado pelo autor é o caso de interceptação, cuja Lei 9.296/96[15], estabelece em seu artigo 10, *in verbis*: "constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados por lei. Pena: reclusão, de dois a quatro anos, e multa".

É pacífico na doutrina quanto na jurisprudência, o conceito de interceptação. Assim, realizar interceptação, tanto telefônica quanto de dados, seria uma terceira pessoa captar informações transmitidas, no caso de interceptação de dados, por meio de computadores entre dois ou mais interlocutores, sem que este tenha conhecimento do fato.

Colli observa que o artigo 10 da Lei de Interceptações esclarece que a atitude de *hacking,* que seria invasão de sistemas informáticos, não estaria abarcada

---

[13] *Hotspots*: são áreas abrangidas por sinal de *wireless* de acesso à internet.

[14] *Sniffer*: é um *software* que capta, intercepta e armazena os dados *(packets*) transmitidos em uma rede de computadores.

[15] Lei nº 9296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal - aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

pelo referido artigo. Portanto, o *hacking,* atualmente, não teria a devida tipificação para ser repelido pelo *jus puniendi* estatal.

> O tipo penal descrito no art. 10 da Lei 9.296 de 24.7.1996, tem como verbo nuclear tipificador a ação de realizar interceptação. Ou seja, o *hacking* – compreendido aqui como a invasão de um computador ou roteador mediante o uso de um *exploit*[16]– não estaria tipificado em lei (até agora), não havendo, igualmente, que se falar em crime (COLLI, 2010, pp. 84-85).

Estas ausências de tipificação penal dificultam, sobremaneira, as investigações policiais, no combate aos crimes cibernéticos. Além disto, pode acarretar o desrespeito ao princípio da legalidade, corolário essencial ao mundo jurídico.

> Diante deste cenário, uma investigação preliminar de supostos cibercrimes – típicos ilícitos e culpáveis – pode ser um território arenoso para as autoridades policiais. Isto porque a incerteza acerca da existência ou não da tipicidade de um fato pode levar, por outro lado, a uma investigação imbuída de ilegalidade. Uma interceptação de comunicações de informática sem autorização judicial configuraria, em tese, a infração penal do art. 10 da Lei 9296, de 24.7.1996 (COLLI, 2010, p. 86).

Em sua obra, o autor enfatiza o problema da falta de tipificação e utiliza o termo “em potencial” no cometimento dos cibercrimes, pois explica que, apesar de várias condutas praticadas utilizando-se a internet resultarem em dano e/ou perigo a bem protegido, não há previsão legal que as criminaliza.

---

[16] *Exploit* (do inglês: explorar) é o instrumento utilizado para explorar uma vulnerabilidade existente em um *software* ou *hardware* (COLLI, 2010. p. 38).

> Em breve análise da ausência de tipicidade em diversos cibercrimes em potencial serviu para apresentar a dificuldade que pode surgir para as autoridades policiais na hora de investigar um fato ocorrido no ambiente *on line*. A tentativa de se demonstrar a falta de tipicidade de condutas praticadas a partir de rede de computadores é potencializada pelas consequências advindas da velocidade com que surgem, diariamente, novos meios e práticas danosas ligadas aos computadores. A ausência de tipicidade pode ocasionar dificuldades para as autoridades policiais identificarem a ocorrência ou não de um (ciber)crime (COLLI, 2010, pp. 86-87).

Por fim, conclui-se que as investigações preliminares em matéria de crimes cibernéticos, quando se trata dos elementos componentes do conceito de crime em si, a tipicidade, ilicitude e culpabilidade têm como obstáculo inicial o elemento do tipo, que, na maioria das ocorrências de delitos informáticos específicos, não se encontram (ainda) positivados, de maneira específica e autônoma, no CP e em outras legislações. Este aspecto dificulta a cadeia investigatória, bem como o trato processual da matéria.

3.2.2 Quanto à identificação e determinação dos sujeitos do delito informático

A identificação do sujeito é uma peculiaridade no crime informático. A dificuldade de determinar o sujeito ativo, em face da rapidez do mundo digital, favorecida muitas vezes pela facilidade do anonimato. A dificuldade de caracterização do agente constitui tarefa árdua às autoridades policiais. Considerada fator negativo, a dificuldade de determinação do sujeito, relacionada ainda com a multiplicidade de locais, a rapidez da transmissão informática e suas variantes tecnológicas, bem como as poucas barreiras de controle do uso da internet, dificultam, sobremaneira, a identificação do sujeito ativo do delito.

3.2.2.1 Problema 1: realidade *on line* (anonimato) e *off line*

A caracterização do sujeito no mundo virtual é complexa. Pode-se dividir esta questão em dois mundos: *on line* e *off line*. Nos crimes virtuais, há dissipação do sujeito no tempo e espaço, além da intangibilidade dos objetos. Estes fatores dificultam a identificação ou concretização do sujeito ativo do crime.

Colli classifica e faz a divisão dos dois campos – *on line* (mundo virtual) e *off line* (mundo real):

> A conjugação da existência em dois mundos – *off line* e *on line* – faz com que as características de um não estejam necessariamente vinculadas ao outro. Ao ingressar no ambiente *on line*, inevitavelmente, estão agregados a um sujeito as características de outro sujeito, o real. Porém ao contrário do sujeito do mundo real (*off line*), o qual, ao manter relações interpessoais, terá uma representação única perante um grupo social, o sujeito *on line* representará uma espécie de camaleão pixelado, podendo assumir a identidade que bem entender ou mais lhe convier. É justamente nesta possibilidade de se modelar uma individualidade *on line* que reside o primeiro problema que se passa a analisar agora: o anonimato *on line*.
> O anonimato *on line* fornece uma liberdade inatingível no mundo real (COLLI, 2010, p. 87).

Para atribuir característica, no mundo virtual, é necessário uso da identidade numérica, a qual caracteriza o endereço, representado pelo número de IP (*Internet Protocol*). O endereço de IP é um atributo que identifica um computador em uma rede (qualitativamente e numericamente).

Colli (2010, p. 88) salienta que, “a identidade, seja ela qualitativa (individualidade de características na rede) ou numérica (endereço de IP), será sempre de um computador, jamais de um sujeito”.

Conclui-se que a individualização será da máquina (objeto) e não de sujeito que opera o equipamento. Portanto, é mais um aspecto complicador para a investigação policial encontrar o sujeito ativo do ato delituoso.

Outro fator importante a ser considerado seria a duplicação de endereço numérico, o chamado IP *spoofing*, em que o mesmo IP poderá representar uma máquina, com dois números de IP para o mesmo equipamento. Caracterizando, portanto um IP válido e outro IP não real (falso).

> Um endereço numérico – por exemplo, um endereço IP – poderá ser atribuído em um curto período de tempo (horas) a diferentes computadores, não podendo, entretanto, (em tese) possuírem o mesmo endereço, ao mesmo tempo, dois ou mais computadores – individualmente considerados (COLLI, 2010, p. 88).

Esta realidade de apenas um endereço de IP em correspondência a um único computador seria o ideal. No entanto, se houver uso de IP *Spoofing*, uma máquina poderá se passar por duas ao mesmo tempo, possuindo dois números de IP para o mesmo equipamento. Haveria a possibilidade de um IP verdadeiro e outro falso, simultaneamente. Seria mais um fator complicador aos procedimentos de instrução policial.

Colli relata esta realidade nas investigações policiais quanto à identificação do sujeito, a partir de seu endereço de IP flutuante (fixo ou dinâmico).

> Apesar de aparente dificuldade em se identificar um sujeito na internet a partir de seu IP, há duas questões importantes que serão problemáticas para qualquer órgão policial incumbido da investigação de um cibercrime: a) a correlação, em um determinado espaço de tempo, entre IP x máquina; b) a correlação, em um determinado espaço de tempo, entre máquina x sujeito que a opera (COLLI, 2010, p. 89).

Conclui-se que a dificuldade de fazer o elo eficaz tendente a auxiliar a instrução penal entre IP + COMPUTADOR + SUJEITO da ação, é em virtude da volatilidade de IP's, além dos fatores de espaço e tempo, que dificultam a respectiva identificação.

3.2.2.2 Problema 2: uso de roteador *wireless*

Outro obstáculo a ser enfrentado pela polícia no trabalho investigativo seriam as múltiplas possibilidades de acesso que os sistemas tecnológicos apresentam. Há, portanto, possibilidades de acesso, por caminhos alternativos, que modificam o número de IP da origem. Exemplo: o acesso à internet por meio de roteador *wireless*.

A utilização desta tecnologia retira a identificação do IP do computador e a identificação será do roteador que está sendo utilizado pelo usuário. Portanto, a única identificação possível será o IP do roteador *wireless* e não o IP do equipamento, de onde parte o acesso e ações do sujeito (grifo nosso).

> A questão que se faz é a seguinte: identificado o IP e o provedor detentor daquele IP, identificada a conta do usuário e, igualmente, o contratante do serviço de acesso à internet detentor daquela conta de usuário, há um prejuízo para a aparência de suspeição a respeito da máquina e do sujeito que praticou o suposto cibercrime? A resposta só pode ser negativa. [...] e se ao adentrar na WLAN [Wireless Local Área Network] o invasor passa a fazer parte dela, tendo um IP interno atribuído ao seu computador, bem como acesso à internet a partir do roteador *wireless*, qual endereço de IP estaria gravado como sendo aparentemente do autor no exemplo anterior? O endereço IP X gravado pelos servidores do banco seria aquele obtido pelo roteador *wireless* no momento de sua conexão com o provedor de internet. Ou seja, o acesso que é feito pelo invasor é intermediado e a partir deste dispositivo, e os registros que irão aparecer serão, portanto, não do invasor, mas sim do IP atribuído ao roteador *wireless* no momento em que este estabeleceu uma conexão com a internet (COLLI, 2010, p. 90).

Portanto, verifica-se a dificuldade de identificação do sujeito de onde partem as ações e origem do acesso. Assim, quesitos básicos a serem respondidos como: a) quem é o operador do equipamento; b) o usuário que está utilizando qual conta da internet; c) qual o provedor do acesso no momento da ação. Enfim, qual o sujeito a quem deve ser atribuída a autoria ou suposta autoria de um crime virtual? As respostas para estas perguntas seriam atribuídas, ao proprietário do roteador *wireless*, pois este terá o IP gravado, no momento da ação, e será o responsabilizado pelos atos.

Portanto, a investigação do sujeito ativo da ação deverá utilizar outros meios como sistemas operacionais específicos, como: *data logging* que possam informar, registrar a sequência de usuários e tentar identificar e correlacionar o endereço de IP do equipamento operante. Estes *logs* servem para identificar rastros deixados por computadores quando realizada conexão.

3.2.2.3 Problema 3: fator tempo e espaço

Outro obstáculo para a investigação seria, novamente, delimitar e correlacionar o USUÁRIO e MÁQUINA. Como seria a identificação do sujeito em um computador público ou computador que é utilizado por várias pessoas da mesma família? Colli exemplifica fatos corriqueiros:

> A correlação, em um determinado espaço e tempo, entre máquina *x* sujeito que a opera. Como pode haver aparência de autoria do cometimento de um cibercrime a partir de um computador de uso público, ou ainda, no caso do cometimento de um cibercrime por meio de um computador utilizado por uma família de 8 pessoas, alguns maiores, outras menores de idade? Este problema está ligado ao que já foi exposto anteriormente: a identidade, seja ela qualitativa ou numérica, será sempre de um computador, jamais de um sujeito. Não há como se automatizar o direcionamento de uma investigação preliminar com base apenas no nome do titular de um contrato de acesso à internet (COLLI, 2010, p. 91).

Conclui-se, portanto, que as investigações policiais devem embasar-se, com cautela, na identificação e rastreamento do uso da internet, pois partirão de números, como endereços de IP. A caracterização partirá inicialmente na identificação de máquinas, jamais de sujeitos (grifo nosso).

Por fim, a investigação deverá ser feita pela análise acurada de rastreamento de equipamentos, a partir de sistemas operacionais específicos,

objetivando interpretação de informações precisas do uso e acessos. Somente desta maneira, a instrução policial resultará em responsabilização subjetiva (do sujeito), como determina o Direito Penal, além de outras provas robustas que cada caso determinará as úteis e lícitas a serem utilizadas.

3.2.2.4 Para determinação do sujeito

Em busca do indiciamento e identificação do sujeito, é imprescindível correlacionar o endereço do número de IP→EQUIPAMENTO→SUJEITO que a opera, para que se possa responsabilizar o autor do delito. A dificuldade de identificação do usuário, a vulnerabilidade do sistema, e variedades tecnológicas e facilidade de acesso aos sistemas, são aspectos que, somados ao uso da rede *wirelless*, abertas (ambiente público) e fechadas (particular), ocasiona difusão ou confusão quanto ao usuário que acessa a internet. Sendo assim, partindo-se da identificação da máquina, possivelmente poderá resultar na identificação do usuário que a opera. No entanto, o fator tempo será relevante também nesta questão.

Na opinião de Colli (2010, pp. 91-92) diante da dificuldade de identificação do sujeito nos crimes virtuais, esta responsabilização subjetiva deverá está feita via prisão em flagrante, com a máquina ligada (grifo nosso). A identificação do sujeito seria precisa e certeira somente com a máquina ligada/operante. Desta maneira, haveria maior segurança, pois não haveria erro nem, tampouco, dúvidas do autor quanto à origem da ação delituosa.

> A partir da apresentação destes dois pressupostos correlacionais – correlação endereço IP *x* máquina e correção máquina *x* sujeito que a opera, uma maneira de contornar os problemas daí surgidos é a seguinte: o indiciamento e a responsabilização do sujeito que opera uma máquina, e a partir dela comete um cibercrime, poderão ser realizados desde que haja a prisão em flagrante com a máquina operante (ligada). Esta proposta tem em vista não apenas a investigação preliminar – que busca vestígios de materialidade e indícios de autoria -, mas também a ação dela decorrente. Afinal de contas, o inquérito policial – fase pré-processual - representa o instrumento a serviço do instrumento. Por este motivo, para se evitar que uma operação que se prolonga por vasto período de tempo acabe em nada, é imprescindível que sua execução seja feita de maneira organizada, com atendimento à legalidade e com vista ao processo penal (COLLI, 2010, p. 92).

Para o autor, seria imprescindível que o ato da prisão em flagrante seja com o equipamento ligado/operante para identificação de autoria. Somente assim,

estaria assegurada a materialidade e a prisão do sujeito do evento, com garantia da segurança ou, pelo menos, dos indícios de autoria.

No entanto, o posicionamento do autor não se mostra favorável ao processo investigativo, nem tampouco, à repressão destes delitos, pois, a exigência da prisão em flagrante, com a máquina operante dificultaria, extraordinariamente, a responsabilização do sujeito do crime. Se assim fosse, raramente alguém seria indiciado e responsabilizado, criminalmente, pela prática de delitos via internet.

Pelo contrário, o que se deve buscar é ampliar os meios de provas e variedades, utilizando-se de prova testemunhal, documental e demais provas lícitas possíveis. Considerar a prisão em flagrante somente com a máquina operante seria restringir a atuação policial, além de não condizente com a dinâmica e velocidade dos delitos informáticos.

Importante destacar que não há necessidade que o sujeito seja capturado em flagrante, para ser indiciado em algum crime. Pelas múltiplas formas de atuação e variadas provas existentes, é possível a prisão por outros meios e seu respectivo indiciamento.

Cabe ressaltar que, para comprovar crimes pela internet, não se utiliza somente provas derivadas da internet, tantas outras podem ser utilizadas e serem úteis. Exemplo: imagine uma pessoa que consiga desviar valores de uma conta bancária para outra, via internet. Os meios de provas serão a identificação do número de IP, do Servidor, dos *logs* de usuários do autor, somada a isto, o destino do dinheiro desviado, a quebra de sigilo bancário, entrevistas, confissões, rastreamento do gasto do dinheiro, testemunhas etc.

Por outro lado, a investigação pode ocorrer de forma inversa. O autor deste mesmo crime é identificado e foi abordado, em *shopping,* fazendo sucessivas compras, com uma sacola de dinheiro, é conduzido à delegacia e confessa o crime, informando que faz uso de um computador de um *cybercafé*. Em relato às autoridades policiais, afirma que conseguiu invadir o sistema bancário e transferir os centavos de todos os correntistas para a sua conta. A partir daí, caberá à polícia investigar o delito, na sua esfera informática. Neste caso concreto, não houve necessariamente prisão em flagrante, apenas responderá pelo crime e será indiciado normalmente. Portanto, há outras possibilidades que não seja, necessariamente, a prisão em flagrante, com a máquina operante.

No entanto, nada impede que o autor do delito seja responsabilizado criminalmente por cibercrime, após a colheita de provas das mais variadas possíveis, apontando-o como autor do delito, ocasião em que será indiciado no inquérito, pela autoridade policial.

3.2.3 Tempo nos cibercrimes

Em relação ao tempo do cometimento do crime, segue o que dispõe o Código Penal em seu artigo 4º, *in verbis:* “considera-se praticado o crime no momento da ação ou omissão, ainda que outro seja o momento do resultado”. Assim, a legislação brasileira adota a Teoria da Ação ou da Atividade, isto é, no momento da consumação do delito, é o marco temporal, em regra.

Ressalte-se que, nos delitos virtuais, pode ou não ser praticado o crime com características permanentes, aquele que se prolonga, no tempo. Bitencourt (2008, p. 213) define crime permanente como: “aquele crime cuja consumação se alonga no tempo, dependente da atividade do agente, que poderá cessar quando este quiser (cárcere privado, sequestro)”. Pode-se inferir que a ocorrência dos Crimes Permanentes podem favorecer a força repressiva do aparelho estatal, pois haverá mais tempo para as investigações policiais atuarem e conseguirem materializar a colheita de provas. Exemplo de crime permanente seria o compartilhamento ilícito de arquivos durante meses em um computador, a divulgação de imagens ilícitas de pornografia infantil em determinado site de forma contínua.

3.2.4 Local

Diante dos efeitos da globalização e avanço da tecnologia, surge nova espécie de alcance do crime, em níveis e escalas mundiais

A amplitude e complexidade dos crimes informáticos contribuíram para o fenômeno da macrocriminalidade. Segundo Ferreira (2007, p. 194), a macrocriminalidade seria “criminalidade sem fronteiras limitadoras”.

A autora discorre sobre a vastidão da internet e a problemática da definição do local do crime, pela amplitude de seu alcance.

> A internet não tem um proprietário, não tem nacionalidade e não está em território algum. Os crimes praticados através dela podem atingir mais de uma pessoa, em territórios diversos, com leis distintas, portanto, é conhecida como multijurisdicional (vários países) e ajurisdicional (localização física e geográfica são irrelevantes), de natureza, pois, multipolar (FERREIRA, 2007, p. 79).

Outra questão relevante também é a delimitação do local do crime. O Princípio da Territorialidade estabelece os limites em que a lei penal será aplicada no espaço, em regra. Este princípio justifica-se em virtude do conceito de soberania. Assim, as leis aplicadas aos fatos, em um país, deverão ser as leis do próprio país, em regra. Contudo, estes conceitos estão em constantes transformações, pois a criminalidade atinge simultaneamente diferentes sociedades/países sob diferentes ordenamentos jurídicos, necessitando repressão uniforme e conjunta.

Quanto ao local do crime, o princípio específico está consagrado no art. 5º do Código Penal, o qual define como território nacional, o espaço que abarca não apenas o espaço físico compreendido entre as suas fronteiras – solo, subsolo, águas territoriais e espaço aéreo – mas também as embarcações e as aeronaves brasileiras, a serviço do seu governo estrangeiro, ou as mercantes e privadas que se encontrem em alto mar.

É fundamental o estabelecimento dos critérios para a definição do local do crime, ou *locus commissi delicti,* objetivando fixar a competência investigativa, judicial e determinar a respectiva legislação, a ser aplicada ao caso.

O artigo 6º do Código Penal, dispõe *in verbis*: “considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como se produziu ou deveria produzir-se o resultado”. Esta é a chamada Teoria da Ubiquidade, em que contempla tanto a ação/omissão quanto o resultado do delito em questão, como sendo o lugar do crime.

Colli considera a Teoria da Ubiquidade, como preponderante, para a interpretação do lugar do crime.

> Atualmente, a teoria da ubiquidade pode ser considerada preponderante para a interpretação do local do crime. De acordo com esta, deve-se entender como local do crime tanto aquele onde se produziu o resultado como aquele onde se executou a ação. No caso de delitos em que haja a conjugação de ações e resultados em diferentes países, a teoria da Ubiquidade mostra-se mais adequada à aplicabilidade da lei penal no espaço, uma vez que há maior possibilidade de evitarem-se eventuais conflitos negativos de jurisdição e de resolverem-se os problemas dos crimes a distancia, nos quais ação e resultado ocorrem em locais diferentes. A aplicabilidade da teoria da ubiquidade quanto ao local do crime está estampada no art. 6º do Código Penal brasileiro (COLLI, 2010, pp. 99-100).

Para exemplificar a repercussão internacional e o livre acesso ao mundo virtual, há fatos que demonstram a dimensão do problema e as dificuldades operacionais cotidianas.

> O sujeito ativo de um delito pode estar no país A, enquanto o provedor por meio do qual ele se conecta a internet está no país B, os dados os quais ele acessa ou o computador que ele danifica estão no país C, e esses objetos materiais são de propriedade de um cidadão do país D. Enfim, uma complexa rede (trans)nacional e (trans)territorial de sujeitos, ativo e passivo, bens jurídicos protegidos e objetos materiais do delito pode se formar (COLLI, 2010, p. 95).

A criminalidade cibernética é bastante dinâmica, com possibilidade de ações simultâneas a qual possui a capacidade de pulverizar resultados negativos a várias nações e de maneiras distintas.

3.2.5 Provas

As provas são efêmeras pelo somatório dos fatores, pois os objetos de coleta são intangíveis e pela instantaneidade do mundo digital. Deste modo, os procedimentos de coleta não são favorecidos e devem seguir rotinas próprias.

A equipe policial deve ater-se ao risco de perecimento da prova, como perda ou o apagar de dados essenciais. Na coleta digital, as provas são chamadas de efêmeras. A efemeridade seria o risco da perda dos dados armazenados, em um disco rígido, ou sua deterioração, por algum motivo.

Colli traz, de forma pormenorizada, o ritual que deve ser observado em razão da possibilidade de perecimento das provas. Ensina rotinas e procedimentos necessários que devem ser executados pela equipe da perícia.

> Em razão do risco de perecimento de prova – por conta de sua efemeridade, os cuidados com a coleta de dados, não só por peritos que estejam envolvidos na análise de dados de um cibercrime, mas igualmente por policiais que fazem o flagrante deste, é minunciosamente tratado em um *checklist* dos procedimentos a serem adotados diante de um cenário como esse. Os passos a serem seguidos para a (con)validação da prova angariada na prisão em flagrante do sujeito cuja máquina operante esteja em flagrância de um cibercrime – ou esteja em situação potencialmente suspeita – são os seguintes: fazer um *print screen* da tela no momento da apreensão da máquina; b) adotar procedimentos para a preservação de dados voláteis (*volatile data*); c) fazer uma imagem do disco rígido da máquina operante, antes que ela seja desligada; chegar a integridade dos dados para se ter certeza que a cópia é exatamente fiel; e) desligar o sistema de acordo com as instruções do sistema operacional; f) fotografia todo os sistema e o ambiente no qual ele está inserido, inclusive cabos conectados na parte traseira do computador e fios que ele estejam conectados ; g) desconectar todos os cabos e periféricos; h) usar fita antiestática ou outro instrumento desmagnetizado antes de tocar nos equipamentos; i) colocar disquetes e outros materiais que possuam mecanismo magnético em bolsas antiestáticas (COLLI, 2010, pp. 114-115).

O autor ressalta a cautela quanto aos procedimentos de coleta dos objetos que contenham dados e o cuidado para não perdimento em fase posterior, com cuidados no próprio armazenamento pós-coleta:

> A recomendação do uso de material antiestático a fim de evitar, por conta de um indesejável campo magnético, a perda de dados armazenados é o exemplo maior da preocupação em se preservar quaisquer dados que possam ser de grande relevância para a investigação preliminar e para o processo penal (COLLI, 2010, p. 115).

Outra questão relevante, acerca das provas, é quando se depara com a possibilidade ou oportunidade de coleta de provas (ilícitas), no compartilhamento de arquivos em rede, por parte da própria polícia. Provas ilícitas seriam as que infringem e violam as normas constitucionais ou legais, de alguma forma. Portanto, tanto no mundo real quanto no virtual, indispensável cumprir as determinações legais do art. 157 e §1º do Código de Processo Penal que considera inadmissíveis as provas ilícitas as quais devem ser desentranhadas do processo.

É importante observar do dispositivo do art. 10 da Lei 9.296/96, que trata sobre interceptações em geral. Este dispositivo contempla, inclusive, a parte informática. O art. 10 da Lei 9.296/96 dispõe, *in verbis* “constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro ano, e multa”. Sendo assim, só poderá haver interceptação, mediante ordem expressa judicial, objetivando garantir o regular

andamento investigativo, além da legalidade dos atos e, na fase processual, posteriormente. Deve-se também considerar as garantias da preservação da privacidade e intimidade, valores assegurados na lei maior, CF, art. 5º, incisos IX, X, XII.

Ressalte-se que a exigência de ordem judicial para realizar diligências, em fase da quebra do sigilo telemático, figura-se como mais um entrave para o princípio da celeridade exigido, nas investigações de cibercrimes.

Outro aspecto seria a possibilidade de compartilhamento de computadores, por parte da própria polícia. A ação poderia ser eficaz em termos investigativos, pois haveria chances de visualização e armazenamento de dados de outro computador que esteja, em rede, simultaneamente. Colli discorre sobre o uso da rede P2P:

> As investigações em redes P2P podem ser feitas a partir de dados colhidos pela própria polícia, a qual, ao ingressar neste tipo de rede – cuja lista de *hosts* e arquivos é armazenada por um servidor - passaria a fazer parte do rol de computadores que compartilham arquivos. Tratar-se-ia de uma modalidade de atividade policial embasada na modalidade de investigação oculta, na qual se mesclariam características não apenas de interceptação de comunicação, mas igualmente de chamada atividade encoberta. [...] o órgão incumbido de interceptar dados e investigar cibercrimes buscaria dois tipos de informações primordiais: a) os endereços de IP que constam na lista do servidor; b) os arquivos armazenados pelas máquinas detentoras destes endereços IP (COLLI, 2010, p. 117).

Com a possibilidade de entrada, em rede, e respectivo compartilhamento de arquivos com outros computadores que estão no processo investigativo, sem que o policial conectado possa ser identificado, nesta ação de infiltração. A partir desta ação de conectividade, pode ser instrumento útil para colher informações e levantar fatos, para posterior embasamento do inquérito policial e identificação dos possíveis endereços de IP e respectivos suspeitos.

4 PRODUÇÃO LEGISLATIVA BRASILEIRA E INTERNACIONAL

A positivação de dispositivos referentes ao sistema informático se apresenta na legislação brasileira de maneira espaça. Há alguns poucos dispositivos no Código Penal os qual foram acrescidos pela Lei 9.983/00[17] e, no Estatuto da Criança e do Adolescente (ECA), inserido pela Lei 11.829/08[18], que serão analisados no decorrer deste capítulo.

Quanto à legislação internacional, optou-se seguindo os ensinamentos de Albuquerque (2006, p. 12), a seleção de dois ordenamentos jurídicos: alemão e o holandês. Segundo o próprio autor, a escolha é devida, porque o direito alemão, por ser um modelo e o direito holandês, pela sua vanguarda. Nas palavras do próprio autor “O direito alemão constitui um paradigma no assunto, pela sua precocidade e concisão, e o direito holandês, pelo seu caráter inovador”.

Na legislação comparada entre os países Brasil, Alemanha e Holanda serão tratados apenas dois aspectos, em especial: a) a definição do local do crime e b) o tópico de violação de segredo informático.

Deste modo, este capítulo abordará aspectos pontuais do Projeto de Lei em tramitação, no Congresso Nacional, sobre crimes informáticos. Posteriormente buscará na legislação brasileira, dispositivos que tratem dos sistemas informáticos, objetivando analisar de modo qualitativo e quantitativo.

4 1. PROJETOS DE LEI NO BRASIL E O DIREITO COMPARADO

A produção legislativa brasileira, em termos de crimes informáticos são poucos e muitos ainda estão em tramitação, no Congresso Nacional. Há o Projeto de Lei (PL) sobre Crimes Informáticos, o PL Substitutivo nº 89 de 2003 da Câmara dos Deputados, resultado do apensamento ou juntada de vários projetos e propostas de projetos de lei substitutivos.

---

[17] Lei 9983 de 14 de julho de 2000, altera o Decreto Lei nº 2848 de 7 de dezembro de 1940 – Código Penal e dá outras providências.

[18] Lei 11829, de 25 de novembro de 2008, altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.

Na Câmara dos Deputados teve início o PL nº 84/1999[19], ao qual posteriormente foram apensados, dentre eles o PL 2.557/00, PL 2.558/00, PL 2.558/00, PL 3.796/00 e, mais recentemente, proposta de projeto de lei substitutivo do Senado Federal nº 137/00. No ano de 2000, houve vários apensamentos de projetos de lei, com substitutivos referentes ao assunto de criminalidade informática como o PL 76/00 e o PL 89/03. Este último, originário da Casa do Senado Federal, ao qual se tem atribuído o título de Projeto de Lei dos Crimes Informáticos.

Segundo análises comparativas entre os projetos oferecidos pela Câmara dos Deputados e pelo Senado, este do Senado Federal possui teor mais punitivista e repressor em comparação ao da Câmara, o PL nº 84/99.

Colli traz, em sua obra, algumas comparações e distorções, no projeto de lei em tramitação.

> [...] A começar pelo número de novos tipos penais criados: vinte e um, o triplo do número que o PL originário da Câmara propunha. Catorze dos novos tipos penais restarão agregados ao Código Penal brasileiro, enquanto sete restarão agregados ao Código Penal Militar. Dentre as bizarrices tipificadoras penais podem ser citados os novos textos dos art. 266 e 297 do Código Penal. No primeiro, passa a ser criminalizada a conduta de mera perturbação de um serviço de rede de computadores ou de serviço informático – seja lá o que isso queira significar; o melhor é não perturbar máquina qualquer. No segundo, o exemplo estampado da desnecessidade de se tipificar uma conduta já prevista no Código Penal, qual seja, a de falsificação de documento público (COLLI, 2010, pp. 158-159).

Extrai-se da observação do autor, que continua havendo problemas quanto à precisão dos conceitos, bem como a tipificação do delito, haja vista a dificuldade de conceituar, de forma adequada, os termos e inserção de expressões inúteis, que em nada irão acrescentar ao ordenamento jurídico.

Exemplo de inserção de termos inúteis, ocorre no art. 297 do Código Penal, quando há o acréscimo do termo “dado eletrônico”, *in verbis*: “falsificar no todo ou em parte, documento público, ou alterar documento público verdadeiro”. A redação final do Substitutivo do Senado Federal ao PL 89/03 da Câmara dos Deputados, apresenta o seguinte teor: “Falsificar, no todo ou em parte, dado eletrônico ou documento público, ou alterar documento público verdadeiro” (grifo nosso).

---

[19] PL 84/1999, Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Caracteriza como crime informático ou virtual os ataques praticados por "hackers" e "crackers", em especial as alterações de "home pages" e a utilização indevida de senhas.

Para Colli (2010, p. 158), tal modificação é inútil e dispõe: “O novo tipo penal adiciona o texto dado eletrônico à redação original do art. 297 do CP, em um belo exemplo de desnecessária movimentação da máquina legiferante em prol dos fins inócuos e estéreis”.

Segue o autor fazendo análises quanto ao Projeto Substitutivo do Senado nº 89/03 ao Projeto de Lei da Câmara. Em seu art. 2º, cria no Título VIII (parte especial do CP), capítulo IV, cria dois novos tipos penais, art. 285-A e 285-B, com as seguintes redações: art. 285-A “Acesso não autorizados a rede de computadores, dispositivo de comunicação ou sistema informatizado. Art. 285-B “Obtenção, transferência ou fornecimento não autorizado de dado ou informação”. No dispositivo ao novo art. 285-C do CP prevê: “nos crimes definidos neste capítulo somente se procede mediante representação, salvo se o crime é cometido contra a União, Estado, Município, empresa concessionária de serviços públicos, agências, fundações, autarquias, empresas públicas ou sociedade de economia mista e subsidiárias”. (grifo nosso).

Portanto, nestes casos somente será iniciado o processo investigativo mediante representação. Consideram-se mais um empecilho, para o combate aos crimes digitais.

Colli faz crítica ao art. 22 do PL nº 89 da Câmara, no tocante à falta de precisão de conceitos e técnica, no dispositivo do artigo que dificulta entendimento e não delimita a ação delituosa, causando transtornos para as investigações policiais, pois os tipos penais não são fechados, claros e com precisão técnica necessária, deixando lacunas aos delinquentes da área digital, sendo que as brechas, na lei, inviabilizam os trabalhos investigativos.

> O art. 22 do PL estabelece uma série de obrigações a serem atendidas pelos provedores de acesso à internet em prol das eventuais investigações preliminares a serem efetuadas no caso de um cibercrime. O curioso é que aqui a falta de precisão técnica faz com que a norma explicativa se restringisse aos provedores, não alcançando os servidores de internet (COLLI, 2010, p. 159).

Outro fator contemplado no respectivo PL, em seu art. 18 é a previsão quanto à necessidade de estruturação dos órgãos policiais, frente à criminalidade cibernética, que avança rapidamente, e à adequada capacitação dos agentes e estrutura capaz de suprir esta demanda. Assim, o art. 18 do PL prevê: “Os órgãos da

polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivos de comunicação ou sistema informatizado". Portanto, acertado tal dispositivo, quando faz esta exigência, tendo em vista o aumento da demanda. A necessidade de capacitação e especialização das equipes policiais são fundamentais e determinantes para o enfrentamento do problema.

Neste sentido, é um grande passo rumo ao enfrentamento no combate ao problema. A especialização e capacitação da polícia, com a finalidade de melhor reprimir e prevenir tais delitos são fundamentais. Somente com a especialização neste assunto será possível encarar novos crimes digitais e as infinitas possibilidades de *modus operandi* que surgem, com as novas tecnologias disponíveis no mercado, a cada dia. São inevitáveis as transformações advindas do avanço tecnológico, algo sem volta. E, somente, a especialização e o aumento da capacitação poderão minimizar os estragos, prejuízos bilionários e vítimas pelo Brasil e mundo afora.

4.1.1 Dispositivos nas Leis Brasileiras referentes aos sistemas informáticos

Outro ponto importante a considerar, são os dispositivos já positivados, acrescentados pela Lei nº 9.983/00, no artigo 153, §1º-A, que adiciona, na seção IV, destinados aos Crimes contra a Inviolabilidade dos Segredos. Assim, está o artigo que tipifica a divulgação indevida de segredo. Art. 153, §1º-A, do CP, *in verbis* "divulgar sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública. Pena – detenção, de 1 a 4 anos e multa".

No entanto, apesar de estar contemplado no artigo, que trata sobre a divulgação de segredo que pode ou não ter sido violado, por meio de sistemas de informações ou banco de dados, nota-se que a sanção do preceito secundário correspondente é considerada menos gravosa, pois o legislador entende que é suficiente apenas a detenção.

Outro dispositivo necessário, em vista do aumento das ocorrências, no dia a dia e enseja, sem dúvida, tipificação expressa foi acrescido o artigo com redação determinada pela Lei n º 11.829/08, no Estatuto da Criança e Adolescente, no art. 241-A do ECA, *in verbis*:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer outro meio, inclusive por meio de sistemas de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente. Pena de reclusão, de 3 a 6 anos e multa.
> §1º Nas mesmas penas incorre quem:
> I - assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo.
> II - assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.

Portanto, diante da necessidade, está havendo a inserção de dispositivos específicos que regulamentam o uso do sistema informático, em aspectos próprios, objetivando a tipificação penal e não mera analogia com os artigos já existentes, no Código Penal ou ao mundo *off line*. Retorna-se a ideia de haver tipificação específica para o sistema informático, seguindo o princípio da legalidade.

A Lei 9.083/00, que trouxe para dentro do Código Penal alguns crimes relacionados a banco de dados e informática. Exemplo são os artigos 313-A e 313-B do CP. No entanto, observa-se que estes dispositivos estão presentes e inseridos, em tópico específico – título XI – dos Crimes contra a Administração Pública e no capítulo intitulado – Dos crimes praticados por funcionário público contra a administração em geral. Ambos os artigos, tanto o que trata de inserção de dados falsos em sistemas de informações e quanto a modificação ou alteração não autorizada de sistemas de informação, exige-se a condição de servidor/funcionário da Administração Pública.

> Art. 313-A – Inserir, ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou banco de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão, de 2 a 12 anos, e multa.
> Art. 313-B – Modificar ou alterar, o funcionário, sistemas de informações ou programa de informática sem autorização ou solicitação de autoridade competente. Pena – detenção, de 3 meses a 2 anos, e multa.
> Parágrafo único: As penas serão aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.

Nota-se mais uma vez, a deficiência quanto à tipificação, restringindo o dispositivo penal a exigência ou a condição de funcionário. Sabe-se que, diante da amplitude do tema e inúmeras possibilidades, este dispositivo deveria ser tratado de forma genérico, ou seja, qualquer pessoa seja ou não na condição de servidor, pessoa nacional ou estrangeira é sujeito potencial, para a prática de violação de sistemas ou banco de dados.

Defende-se, portanto, que a criminalidade informática deve ser tipificada com dispositivos próprios específicos, de forma a conseguir positivar ações ou omissões deste delito tão particular, apto a traduzir a realidade atual e em especial a segurança jurídica necessária a sua investigação e posterior repressão.

Segue-se para o entendimento brasileiro, alemão e holandês sobre a determinação do local do crime. Há entendimentos diversos entre os ordenamentos, como será exposto a seguir.

4.1.2 Quanto ao local do crime – Brasil e Alemanha

Como visto anteriormente, quanto ao local do crime a legislação brasileira adotou Teoria da Ubiquidade. Quanto ao local do crime, a Alemanha é semelhante ao Brasil, sendo desta forma, o local do crime é onde o ato ocorreu ou foi praticado (ação), ou onde o delito se realizou ou teve seu resultado. Portanto, conclui-se que o local do crime é onde se realizou qualquer dos momentos do *inter criminis*. No código alemão, não há nenhuma previsão específica quanto ao local do crime, para o delito informático. Deste modo, mostra-se com isto que a legislação estrangeira também possui lacunas a serem solucionadas.

4.1.3 Quanto ao local do crime - Holanda

Albuquerque faz análise do Código Penal holandês mostrando que, em seus artigos 2º a 7º, depende, de forma preponderante o lugar onde foi cometido. Assim, é diferente do entendimento da legislação brasileira e alemã. O Código Holandês diferentemente privilegia o Princípio da Territorialidade.

> Nos Países Baixos, como na Alemanha, não há grandes diferenças com relação ao Brasil, sob o ponto de vista de determinação do lugar do crime. Conforme o Código Penal holandês, do art. 2º ao 7º, para que a jurisdição holandesa incida, depende, fundamentalmente, do lugar onde o crime foi cometido (princípio da territorialidade), da pessoa que cometeu o crime e contra quem o crime foi cometido (princípio da personalidade) e da própria modalidade do crime praticado (princípio da proteção). O princípio da territorialidade é o de maior importância para o nosso estudo (ALBUQUERQUE, 2006, p. 70).

O autor traz exemplo clássico para demonstrar a dificuldade quanto à determinação do local do crime. Apresenta, portanto uma hipótese clássica quanto à definição do local do crime, quanto transpassa fronteiras, acarretando ao Poder Judiciário a tarefa para definir o local preponderante do cometimento do delito. No exemplo do autor:

> "A", a partir dos Países Baixos, acessa via modem, um sistema informático situado na Dinamarca, violando as medidas de segurança que o protegiam. A partir dele, ele acessa outro computador, situado nos Estados Unidos, através de sistemas informáticos localizados na Suécia e no Reino Unido. "A", então, transfere uma vultosa soma de dinheiro que é depositada, mais uma vez via modem, numa agência bancária situada na Suíça. Não constitui uma tarefa fácil determinar que país deve ser considerado competente para julgar o crime.[...] Na hipótese apresentada anteriormente, com base nas teorias formuladas pela Suprema Corte holandesa, a justiça dinamarquesa seria competente para julgar o crime informático? As medidas de segurança foram violadas na Dinamarca. Por outro lado, pode-se afirmar que o resultado do crime ocorreu na Suécia e no Reino Unido, embora os computadores situados nestes dois países também possam ser considerados apenas um instrumento. O resultado pode ter ocorrido nos Estados Unidos, onde os dados foram modificados, bem como na Suíça, aonde eles foram transferidos (ALBUQUERQUE, 2006, p. 71).

Neste caso, segundo o próprio autor, caberia, em boa medida, à jurisprudência precisar onde o ilícito ocorreu. Chega-se a inevitável conclusão, com base na Teoria da Ubiquidade, que vários países são competentes para julgar os crimes informáticos, quando transpassa fronteiras. Assim, qualquer lugar onde parte do crime tenha ocorrido pode, portanto, ser considerado lugar do crime. Haveria a possibilidade de mais um problema, quanto à competência positiva para julgamento da matéria, atribuída a vários países, como também a interpretação do delito à luz de vários ordenamentos jurídicos distintos.

Caso prático ocorreu, no âmbito da competência do Superior Tribunal de Justiça - STJ, sobre a competência do lugar para julgamento, em caso de divulgação de imagens infantis, por meio de redes sociais, a justiça federal é a competente para julgar. Em síntese, quanto à notícia veiculada pelo STJ em seu portal:

> A 6ª Turma reafirmou que a consumação do crime de divulgação pela internet de imagens pornográficas infantis se dá no momento em que o conteúdo pornográfico é enviado, sendo indiferente a localização a localização do provedor de acesso ou a efetiva visualização do conteúdo pelos seus usuários. Assim, quem divulga/compartilha conteúdo pornográfico na internet assume o risco de que esse conteúdo seja acessado por qualquer pessoa em qualquer lugar do mundo. Com isto está cumprindo o requisito da transnacionalidade, requisito necessário para atrair a competência da Justiça Federal (BRASIL, 2011).

Portanto, mais uma vez ressalta-se que estes tipos de crimes transnacionais ou de grandes magnitudes (macrocriminalidade) devem receber uma atenção especial quanto à confecção de legislação homogênea e uniforme objetivando facilitar a aplicabilidade da lei aos casos concretos.

Somando-se a isto, é imprescindível, nestes tipos de delitos, a integração dos países mediante convênios, tratados, acordos a fim de estabelecer parcerias para reprimir e prevenir tais ações criminosas. A única certeza é a necessidade de ação por parte do aparelho estatal. Os possíveis conflitos de jurisdição, que podem ocorrer, com freqüência, nestes tipos de delitos, podem ser resolvidos ou minimizados, pelo menos na teoria, com tratados internacionais, que facilitariam as relações internacionais e, consequentemente, os procedimentos investigativos necessários à resolução dos problemas.

Albuquerque argumenta sobre a determinação do lugar do crime, nestes tipos de delitos de forma geral e, em particular, o caso do Código Penal alemão e holandês, o seguinte:

> Somos da opinião de que carece de maior importância buscar determinar, com base nos princípios existentes, o país competente para julgar e processar crimes informáticos com natureza transfronteiriça. Não se pode criar um sistema fechado, rígido, para a determinação do lugar de uma modalidade de crime que, em sua execução, se caracteriza justamente pela flexibilidade. Nem o Código Penal alemão nem o holandês foram adaptados para fazer frente a essa característica (ALBUQUERQUE, 2006, p. 73).

Quanto à definição do local do crime, no projeto de lei em tramitação no Congresso Nacional, não se constatou a existência de nenhum dispositivo próprio que trate de forma específica sobre a determinação do crime informáticos. Deste modo, entende-se que segue a Teoria da Ubiquidade e a flexibilidade quanto a esta determinação de local tendo em vista que este tipo de delito possui projeção além fronteiras. Assim, a amplitude e flexibilidade neste tópico em específico têm por

objetivo privilegiar os trabalhos investigativos e os órgãos competentes para julgamento, pois permitirá ampliar o país/local e as instituições aptas para atuar no caso, tanto nacionais quanto internacionais.

4.2. CRIMES CONTRA OS SISTEMAS INFORMÁTICOS (VIOLAÇÃO DE SEGREDO)

O *hacking* pode ser definido como as ações, visando à prática de invasão de sistemas informáticos e a respectiva tomada de dados protegidos, contra acesso não autorizado. Quem o pratica é o *hacker*, como tratado no primeiro capítulo.

Desta maneira, a atuação do *hacker* ocorre, mediante invasão dos sistemas informáticos com sua respectiva violação de segredos/dados neles inseridos, de alguma forma armazenada, processada ou transmitida. Tal violação pode ser praticada de diversas formas, inclusive a distância utilizando-se das redes de telecomunicações.

O aspecto a ser abordado será, em especial, a violação de segredo informático, o qual faz parte e está contido no rol dos crimes contra sistemas informáticos. Igualmente serão feitas comparações entre as legislações brasileira, alemã e holandesa, objetivando verificar semelhanças e diferenças de entendimentos.

4.2.1 Direito Alemão

Quanto ao assunto de violação de segredos informático, segue abaixo trechos do Código Penal alemão:

> Art. 202a Espionagem de Dados
> §1º Quem obtém sem autorização para si mesmo ou para outrem dados que não lhe são destinados e que são especialmente protegidos contra acesso não autorizado, será punido com pena privativa de liberdade de até três anos ou com pena de multa.
> §2º Dados no sentido do parágrafo 1º são apenas aqueles que são armazenados ou transmitidos eletrônica ou magneticamente, ou de outra maneira que não seja diretamente perceptível (ALBUQUERQUE, 2006, p. 195).

Segundo a interpretação de Albuquerque, o autor ensina que, para que haja o *hacking*, o hacker precisa acessar ou modificar dados, podendo ainda fraudá-los.

> Na Alemanha, portanto, não se pune o mero acesso a sistema informático, mas a violação de segredo informático, a espionagem de dados que não são destinados ao infrator. Eles não devem ter sido armazenados com o objetivo de serem acessados por ele. O legislador alemão não desejou punir o *hacker* que tem como objetivo apenas ter acesso a um sistema informático, e nada mais. Outra limitação importante à incidência do art. 202a é, precisamente, a exigência da adoção de medidas especiais contra acesso aos dados por pessoas não autorizadas. Isso não diz respeito a medidas de segurança como códigos de acesso ou senhas com propósito geral, mas a medidas de segurança que tenham como objetivo manter em segredo dados específicos, que restrinjam o acesso a dados que estejam sendo, por exemplo, transmitidos via e-mail ou armazenados em disco rígido (ALBUQUERQUE, 2006, p. 138).

Importante conclusão que o art. 202a, busca proteger o interesse do titular, em que os dados sejam protegidos do *hacking* e que, tais dados não sejam explorados e usufruídos por terceiros. Além disto, o mero acesso não é punível e este deve ser guarnecido por proteção e medidas especiais que barrem o acesso aos dados por pessoas não autorizadas que possam violar o segredo informático. Tal obtenção de dados com a respectiva invasão ou violação das medidas de segurança de forma não autorizada é punível a luz do art. 202a. do Código Penal Alemão.

4.2.2 Direito Holandês

O direito holandês protege contra o *hacking,* já a legislação alemã para que seja caracterizado o *hacking* deve haver necessariamente a violação das medidas de segurança. Portanto, a violação dos sistemas informáticos quando o acesso não tenha sido autorizado, os dados armazenados, processados ou transmitidos, via computador, devem ser objeto de sanção penal. Segundo o art. 138a. Código Holandês, *in verbis*:

> Violação de domicílio informático. §1º Com pena de reclusão de no máximo seis meses e pena de multa de terceira categoria, é punido, como culpado de violação de domicílio informático, quem penetra intencionalmente e ilicitamente num mecanismo automatizado para o armazenamento ou processamento de dados, ou numa parte dele (ALBUQUERQUE, 2006, pp. 199-200).

Portanto, somente se falará em violação do segredo informático, se houver medidas de segurança para conter tal invasão.

4.2.3 Direito Brasileiro

Considerando a legislação de outros países, a brasileira não tipifica, até o momento, o *hacking.* O autor Albuquerque (2006, p. 146) ensina, com propriedade que: “o *hacking*, a violação de segredo informático, a obtenção de dados protegidos por medidas de segurança, constitui uma conduta atípica, à luz do direito brasileiro”. Esclarece o autor que o *hacking* não pode ser enquadrado e ser objeto de punição, no Código Penal brasileiro. Não há enquadramento legal no art. 151, caput, *in verbis*: “ devassar indevidamente o conteúdo de correspondência fechada dirigida a outrem”. Não é possível fazer analogia em matéria penal, nem adaptações ao tipo penal existente.

Ainda segundo o autor, a intangibilidade dos dados impossibilita o devido enquadramento em qualquer dispositivo legal vigente.

> A violação de segredo informático, de dados, objetos intangíveis, não é objeto de sanção. O art. 155, §4º, inciso III, sobre furto qualificado por chave falsa[20], tampouco enquadra o *hacking*. Pode no máximo, oferecer proteção contra quem, para furtar um computador, o equipamento, o objeto tangível, recorrer a meios de acesso inusitados, de natureza física, ao sistema informático. O furto tem como objeto coisas móveis, e não dados, objetos intangíveis. Tampouco o furto por destreza, previsto no Código Penal, art. 155, §4º, II, em que o infrator recorre a meios que impeçam a vítima de perceber a subtração da coisa móvel, do objeto tangível, abrange o *hacking*. Com a violação de segredo informático, não se subtrai nada. Tanto os dados como os programas de computador permanecerão no sistema informático que foi violado. Os dados podem ser copiados, mas continuarão sob o domínio do respectivo titular. Se eles forem destruídos, não será o caso de *hacking*, mas de dado informático, já que objetos intangíveis tampouco são objeto do crime de dano, previsto no art. 163 do CP (ALBUQUERQUE, 2006, p. 144).

Neste sentido, conclui-se que a violação de sistemas informáticos, chamado de *hacking*, atualmente, não está tipificada no Código Penal brasileiro, sendo portando atípico, até o presente momento. Desta forma, os atuais dispositivos do código penal não há como enquadrá-lo, principalmente diante do fato que os objetos em questão são intangíveis e os artigos do código são objetos materiais e tangíveis.

Como visto anteriormente, a tipificação referente à violação de segredo informático está contemplado, no Código Penal em seus artigos 313-A e 313-B

---

[20] Chave falsa: é o instrumento destinado a abrir fechaduras ou fazer funcionar aparelhos (NUCCI, 2009. p. 641).

apenas, quando o sujeito ativo é funcionário e contra a Administração Pública. No entanto, sabe-se que tal crime não há delimitação, nem tampouco restrições, de qualquer espécie.

Deste modo, mais uma vez esbarra-se na falta de tipificação adequada, para subsidiar as investigações e a parte processual fica prejudicada, quando as ações são amplas e advindas de outras possibilidades e sujeitos ativos. Espera-se maior e melhor tipificação sobre os crimes digitais e que o projeto de lei em tramitação contemple os tópicos essenciais, para traduzir a realidade dos acontecimentos.

Sobre a deficiência legislativa e existência de inúmeros vícios, os projetos de lei, Atheniense traz seu posicionamento e críticas:

> Os artigos polêmicos do Projeto de Lei sobre crimes cibernéticos que eram até então o ponto de discórdia e de atraso na tramitação do PL 84/99 tiveram nova redação a partir do substitutivo apresentado pelo Deputado Regis de Oliveira (PSC-SP) na primeira semana de outubro. O imbróglio se referia a definição da atribuição de responsabilidade quanto a preservação dos dados pelos provedores e às formas de cessão. Estes requisitos são de extrema significância para obtenção do êxito na identificação autoria do ilícito. Considero que o substitutivo demonstrou um avanço, pois a redação anterior, a meu ver continha vícios que comprometiam a apuração de autoria ao restringir a obrigação da preservação apenas aos provedores de acesso. Esta minha crítica já havia sido reiteradamente alardeada.
> Sempre defendi a tese que haveria uma chance reduzida quanto a identificação de autoria dos crimes, caso o legislador brasileiro persistisse na ideia de responsabilizar apenas o administrador da rede e mantivesse a desobrigação dos provedores de conteúdo quanto a preservação dos registros eletrônicos, inclusos os dados cadastrais, ips e outros dados que fossem indiciadores da autoria.
> Desde a entrega do parecer elaborado pela Comissão de Tecnologia da Informação da OAB Federal em junho de 2008 para o Senador Azeredo, restou enfatizado que o efetivo enfrentamento dos ilícitos praticados nos meio eletrônicos, sobretudo quanto se trata da publicação de conteúdos ilícitos, é indispensável que os provedores de conteúdo sejam obrigados a preservar os registros eletrônicos para que seja aumentada a possibilidade de êxito na identificação de autoria.
> Esta sugestão ora corroborada pelo substitutivo, finalmente alinha o texto do Projeto de Lei de Crimes Cibernéticos com a Convenção de Budapeste no tocante a atribuição de responsabilidade pela preservação dos registros eletrônicos para fins de identificação de autoria dos ilícitos. Como já havíamos salientado a versão original do artigo da Convenção que trata deste tema, havia sido alterada no Projeto de Lei Brasileiro visando eximir o provedor de conteúdo desta obrigação.
> Em decorrência desta alteração sugerida pelo Substitutivo, espera-se que, uma vez promulgada a lei, o Brasil possa futuramente aderir em parte ou na totalidade a Convenção de Budapeste para que os crimes cibernéticos, devido a suas características transfronteiriças possam ser enfrentados de forma harmônica, em diferentes países, valendo-se de um único instrumento legal aplicável em diversos países.
> Por outro lado, um aspecto que chama a atenção no substitutivo foi a proposta de alterar o critério quanto a cessão das informações cadastrais. A sugestão de flexibilizar a concessão de dados cadastrais sem autorização judicial, pode gerar conflitos quanto a invasão de privacidade, isto porque

> segundo a justificativa do relator, a ordem judicial só deveria ser exigida para fins de cessão dos dados sensíveis.
> Em se tratando de instrução penal, onde não há utilização de princípios analógicos é temerário adotar estes critérios sem uma devida individuação conceitual do que seriam na prática os dados sensíveis de cada cidadão. Na prática, este é um conceito eminentemente doutrinário, que possui características de ambiguidade, o que pode gerar diferentes interpretações causando eventuais abusos sem o exame da autoridade judicial competente.
> Não restam dúvidas de que se for adotado o critério quanto a desnecessidade da ordem judicial, causará maior celeridade quanto ao cumprimento da ordem para fornecimento de dados cadastrais e no resultado da investigação, mas esta medida poderá gerar riscos, pois haverá um limite muito tênue e subjetivo para determinar o que pode ser considerado como dado sensível, pois no texto do substitutivo não há menção expressa sobre este significado. Onde está a definição de dados sensíveis? Como vamos delimitar se determinado dado é ou não um dado sensível? O conceito sobre dados sensíveis já existe na doutrina, mas não existe na lei.
> Na legislação brasileira ainda não existe um conceito expresso sobre o que deve ser considerado como dado sensível. Esta é uma lacuna que demanda ser esclarecida, pois a legislação que trata de privacidade on line em nosso país é limitada e ultrapassada, pois em regra, está lastrada apenas em dois dispositivos constitucionais - artigos 5o, X e XII, cuja redação remonta ao ano de 1988, que convenhamos, já está distante da atual realidade dos problemas que convivemos quanto aos riscos do cruzamento e vazamento de dados, que colocam em risco as garantias fundamentais do cidadão brasileiro.
> Apesar do avanço trazido pelo substitutivo, ainda é temerário fazer uma previsão concreta sobre os efeitos imediatos do seu despacho. O que se espera é que a sua apresentação desencadeie um amplo processo de negociação entre as lideranças, para que o projeto seja remetido à sanção presidencial, finalizando os intermináveis trâmites entre os gabinetes do Congresso, para não delongar ainda mais uma novela que já duram treze anos e que contabiliza prejuízos consideráveis para todos (ATHENIENSE, 2010).

Por fim, a falta de legislação, em vários aspectos atinentes aos crimes virtuais, prejudica, sobremaneira, a investigação, apuração da autoria, a caracterização penal e os processos posteriores de indiciamento e julgamento do agente ativo.

Com base no artigo apresentado, a demora na aprovação de regulamentos que possa servir de parâmetro aos tipos penais, é fator prejudicial, pois, reiteradamente estão acontecendo os crimes, resultando em vítimas e prejuízos sem uma definição clara do que é punível ou não.

Salienta o autor, que o texto anterior do projeto de lei, trazia obstáculos para a identificação da autoria do fato. Deste modo, em vista da amplitude dos delitos virtuais, é necessária a ampliação de responsabilização a fim de se conseguir apurar a autoria e reprimir o crime. O autor defende, ainda, a busca da responsabilização dos provedores e preservação dos dados, para melhor caracterização dos responsáveis.

Ressalta ainda, como outros autores, a necessidade de acordos internacionais para viabilizar o combate aos delitos digitais. Os acordos, convenções e as cooperações internacionais trariam harmonia quanto à tipificação e evitariam assimetrias discrepantes, nesta criminalização, considerando, novamente, o caráter transfronteiriço destes crimes.

Neste sentido, faz-se necessária, como exposto ao longo do trabalho a tipificação penal adequada, em termos qualitativos e quantitativos.

Por fim, o projeto de lei deve, necessariamente, contemplar nomenclaturas próprias da linguagem informática, mas que estejam de acordo com os fatos cotidianos para que possam servir de norte, para a sociedade, para o aparelho governamental, em especial os órgãos policiais e para julgamento objetivo por parte do Poder Judiciário. Além disto, deve a legislação brasileira também tentar harmonizar-se com outros ordenamentos estrangeiros, objetivando o entendimento dos dispositivos sobre criminalidade informática, para possíveis intercâmbios de informações, bem como adequação, caso necessário, de repressão mais facilitada e uniforme.

CONCLUSÃO

O presente trabalho monográfico se propôs a mostrar a nova criminalidade, advinda das mudanças nos sistemas de comunicação, em especial a internet. A internet favoreceu e criou ambiente propício para novas pratica delituosos chamados cibernéticos ou informáticos.

O estudo se propôs a demonstrar questões cotidianas que ocorrem na atividade policial investigativa, em matéria de crimes digitais, em virtude da intangibilidade do bem jurídico tutelado.

O foco principal da abordagem se concentrou nas dificuldades quanto à determinação do sujeito ativo do delito. A complexidade na identificação do autor do *cyberdelito,* está justamente, porque há dependência em relação do número do IP que é o endereço que caracteriza o equipamento. Contudo, deve-se considerar que esta relação não é única. Existem mecanismos da tecnologia capazes de driblar a correta identificação da máquina, com a existência de IP's fixos e dinâmicos. Neste sentido, a investigação policial deve primar pela correta caracterização do responsável pelo tipo penal, apesar das dificuldades e vulnerabilidades tecnológicas.

Outro aspecto relevante são os fatos do tempo, lugar e efemeridade das provas cibernéticas. Os procedimentos investigativos não são favorecidos, tendo em vista que a instantaneidade do mundo digital dificulta a apuração porque o cometimento deste tipo de crime pode ser feito em nanossegundos e não mais em horas ou dias.

Chega-se a conclusão que a determinação do sujeito é imprescindível para a segurança jurídica e o correto andamento do inquérito e processo penal. Igualmente, a delimitação do local do crime é indispensável. No entanto, não se devem adotar critérios rígidos ou fixos para determinação do local do crime. Há que considerar a possibilidade multilocais, neste tipo de delito.

Sendo assim, considera-se que a Teoria da Ubiquidade, adotada pelo Brasil, é a opção mais viável e que melhor se enquadra nas particularidades da criminalidade informática, pois considera o local da ação/omissão ou do resultado, como parâmetro na determinação do local do crime nos procedimentos investigativos e processuais.

Na parte processual, tratou-se dos critérios suficientes para a prisão em flagrante. Foi apresentada a opinião em particular, do autor Colli, o qual defendeu que

a prisão em flagrante nos ciberdelitos deve ser realizada pela flagrância do sujeito com o respectivo equipamento ligado ou operante. Desta forma, a prisão estaria imbuída da segurança necessária para sua ocorrência. No entanto, há que se considerar o dispositivo do artigo 302 do CP que elenca opções em diversos incisos sobre as possibilidades do autor ser preso em flagrante.

Além do mais, demonstrou-se que nos crimes cibernéticos não se deve utilizar apenas provas derivados do equipamento de informática ou advindas apenas da internet. Deste modo, clara possibilidade de utilização de outros meios de prova como: as testemunhais, documentais, interceptações telefônicas ou telemáticas, dentre outras que poderão ser úteis, para a instrução também.

Importante ressaltar que, diante da intangibilidade dos dados, arquivos, processo de transmissão e vulnerabilidades dos sistemas devem ser observados pelas equipes policiais e que as provas no mundo virtual são de extrema efemeridade ou possuem facilidade de perecimento. Portanto, a coleta e o momento pós-apreensão sejam de informações, dados ou equipamentos em si, devem seguir rotinas e procedimentos próprios que evitem o desfazimento ou perdimento das provas.

Neste sentido, é importante ressaltar a necessidade de capacitação e especialização do aparato policial para o enfrentamento da criminalidade informática.

Cabe ressaltar, que a necessidade de capacitação e especialização do aparato policial para o enfrentamento da criminalidade informática são imprescindíveis.

Assim, acertadamente, o artigo 18 no Projeto de Lei nº 84/99 que trata de forma específica sobre os crimes cibernéticos, em tramitação no Congresso Nacional Este dispositivo prevê a necessidade de estruturação dos órgãos da polícia judiciária, para o enfrentamento do assunto. Os órgãos deverão fazer frente à criminalidade informática, mediante capacitação e estruturação de setores e equipes especializadas, no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. Esta intenção do legislador é imprescindível tendo em vista o aumento exponencial de vítimas, ocorrências e as especificidades que envolvem estas ações criminosas.

Quanto ao aspecto legislativo, chegou-se a conclusão que a produção legislativa está muito aquém da necessidade de disciplinamento em matéria de crimes cibernéticos. A tipificação penal, requisito primeiro que compõe juntamente com a

ilicitude e culpabilidade os componentes necessários, para a configuração do crime muitos não estão contemplados ou positivados, até o momento. Muitos dos fatos delituosos são possíveis, ocorrem cotidianamente, mas que, no entanto, não podem sofrer a reprimenda estatal, por falta da adequada tipificação penal.

É necessário observar que, em matéria de direito penal, não há possibilidade de analogias ou adequações de tipos penais. O presente estudo chega à conclusão que os delitos informáticos são específicos e que devem ser contemplados no Código Penal, de maneira própria e particular.

Considera-se também que o CP é datado de 1940 e não está atualizado com as mudanças e necessita adequar-se à nova realidade digital. Portanto, pela segurança jurídica e, em respeito ao princípio da legalidade, corolário básico da ciência jurídica, a legislação contemplar de forma específica o que será punido. Desta forma, a legislação brasileira, em particular, deve ser revista e atualizada para os delitos digitais.

Assim, os preceitos primários e secundários da lei penal, em matéria de crimes de crimes cibernéticos, devem fazer está inseridos na lei penal As possibilidades de repressão devem estar estampadas na legislação de forma clara, precisa. Deste modo, não se pode considerar válida a discussão sobre os tipos penais existentes no CP de 1940, sejam ou estejam aptos a contemplar, de forma atualizada dispositivos tão específicos e particulares do mundo digital. Não há adequações nem analogias em matéria penal. A legislação deve acompanhar as mudanças sociais, de forma atingir a paz social, tão almejada e por ser a finalidade última da ciência jurídica.

Sendo assim, a atual legislação brasileira não está adequada para disciplinar esta nova modalidade de crimes contemporâneos. A máquina legiferante deve atuar melhor nesta temática, haja vista a velocidade e dinâmica tecnológica, em detrimento da lenta produção legislativa. O Poder Legislativo, inclusive, não deve criar tipos fechados, rígidos ou mesmo exacerbados de tecnicismos que tragam mais dificuldades do que solução.

A questão da tipificação, ou seja, a própria existência de tipos contemplados no CP, de forma clara, coerente e que traduzam a realidade e crimes a ser combatidos pelo *jus puniendi* estatal, sendo imperativo para o processo investigativo e toda cadeia processual porque estará claro o que se deve ou não investigar e punir.

Constatou-se que esta nova macrocriminalidade, em termos digitais, que ultrapassa fronteiras físicas e que redefine conceitos clássicos de soberania e estado-nação, em que as ações e resultados em cibercrimes não estão confinados em lugares determinados. Neste aspecto, é imprescindível a cooperação internacional e integração por meio de tratados, acordos, convenções que garantam maior acessibilidade aos processos investigativos, bem como, o intercâmbio de informações. Há que considerar a dinâmica dos ciberdelitos e, somente com maior integração entre os países, será possível minimizar a questão da velocidade dos acontecimentos *on line*.

O estudo também abordou questões pontuais da legislação alemã e holandesa, nos tópicos específicos, quanto à determinação do local do crime e sobre a violação de segredo informático. Constatou-se, quando feita comparação entre as legislações, tanto a brasileira quanto alienígenas estão em descompasso e em diferentes momentos. Verificaram-se diferenças de entendimento que serviram para demonstrar que as nações estão em diferentes níveis legislativos, sendo que, alguns aspectos são tipificados e outros não, como o *hacking*.

Por fim, diante da característica da transnacionalidade, é necessário maior integração e cooperação internacional entre os países, tanto em termos investigativos e intercâmbio de informações, como no processo judicial em si. Deve-se buscar harmonizar as legislações entre os diferentes ordenamentos jurídicos e buscar ser o mais homogêneas e lineares possível, para facilitar a aplicação da lei penal, em diferentes países. Somente desta forma, será possível diminuir os índices alarmantes e crescentes dos crimes cibernéticos no Brasil, e no mundo.

REFERÊNCIAS

ALBUQUERQUE, Roberto Chacon de. *A Criminalidade Informática*. São Paulo: Editora Juarez de Oliveira, 2006.

ATHENIENSE, Alexandre Rodrigues. *Substitutivo do PL de Crimes Cibernéticos avança, mas ainda deixa dúvidas*. Brasília-DF: Conteúdo Jurídico, 2010. Disponível em: http://www.conteudojuridico.com.br/?colunas&colunista=2940_Alexandre_Atheniense&ver=763. Acesso em 13.out.2011.

BITENCOURT, Cezar Roberto. *Tratado de Direito Penal*. v.1. 13.ed. São Paulo: Saraiva, 2008.

BRANDÃO, Caio Rogério da Costa. Os Contratos De Consumo No Comércio Eletrônico. Júris Plenum. V. 7, n.37, pp. 63-71, jan. 2011.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. *Justiça Federal é competente para julgar pornografia infantil em redes sociais*. Portal de Notícias do STJ, Processo: CC 118722. Relator Ministro Adilson Vieira Macabu (Desembargador convocado do TJ/RJ – Terceira Seção). Disponível em: http://www.stj.jus.br/webstj/processo/justica/detalhe.asp?numreg=201102019580 Acesso em 06.out.2011.

COLLI, Maciel. *Cibercrimes*: limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá, 2010.

CONFERÊNCIA INTERNACIONAL DE PERÍCIAS EM CRIMES CIBERNÉTICOS – ICCyBER 2004: Anais da 1ª Conferência Internacional de Perícias em Crimes Cibernéticos. Departamento de Polícia Federal. 2004.

CORRÊIA, Gustavo Testa. Aspectos Jurídicos da Internet. 5ed. rev. e atual. São Paulo. Saraiva. 2010.

FERREIRA, Érica Lourenço de Lima. *Internet* : macrocriminalidade e jurisdição internacional. Curitiba: Juruá, 2007.

IEKA, Ana.UOL TECNOLOGIA. *Crimes cibernéticos atingem diariamente 77 mil brasileiros; prejuízo anual de R$ 104 bilhões*. Notícia publicada em 20.set.2011 às 11:13 horas. Disponível em: http://tecnologia.uol.com.br/ultimas-noticias/redacao/2011/09/20/crimes-ciberneticos-atingem-77-mil-brasileiros-diariamente-prejuizo-e-de-r-104-bilhoes.jhtm. Acesso em: 20.set. 2011.

INELLAS, Gabriel César Zaccaria de. *Crimes na Internet*. 2.ed.(atual. e ampl.). São Paulo: Editora Juarez de Oliveira, 2009.

LIMA, Paulo Marco Ferreira. *Crimes de Computador e Segurança Computacional*. São Paulo. Milennium. 2006.

NUCCI, Guilherme de Souza.*Código penal comentado*. Versão compacta. São Paulo: Revista dos Tribunais, 2009.

PINHEIRO, Patrícia Peck. *Direito Digital*. 3.ed. rev. (atual. e ampl.) São Paulo: Saraiva. 2009.

VALLE, Regina Ribeiro do. *E-dicas*: direito na sociedade da informação. São Paulo: Usina do Livro. 2005.

Legislação Consultada

Lei nº 9.296, de 24 de julho de 1996.

Lei nº 9.983 de 14 de julho de 2000.

Lei nº 11.829, de 25 de novembro de 2008.

Projeto de Lei Substitutivo nº 89 de 2003 ao PL nº 84/1999 (Câmara dos Deputados).