



UNIVERSIDADE FEDERAL DA BAHIA
FACULDADE DE DIREITO
MESTRADO PROFISSIONAL EM SEGURANÇA PÚBLICA,
JUSTIÇA E CIDADANIA

JOSEFA CRISTINA TOMAZ MARTINS KUNRATH

A EXPANSÃO DA CRIMINALIDADE NO CIBERESPAÇO:
DESAFIOS DE UMA POLÍTICA CRIMINAL DE PREVENÇÃO AO
CIBERCRIME

Salvador
2014

JOSEFA CRISTINA TOMAZ MARTINS KUNRATH

**A EXPANSÃO DA CRIMINALIDADE NO CIBERESPAÇO:
DESAFIOS DE UMA POLÍTICA CRIMINAL DE PREVENÇÃO AO
CIBERCRIME**

Dissertação apresentada ao Mestrado Profissional em Segurança Pública, Justiça e Cidadania, da Faculdade de Direito, Universidade Federal da Bahia, como requisito para obtenção do título de Mestre em Segurança Pública.

Orientadora: Prof.^a Dr.^a Ivone Freire Costa

Salvador
2014

K96

Kunrath, Josefa Cristina Tomaz Martins,
A expansão da criminalidade no ciberespaço: desafios de uma política criminal
de prevenção ao cibercrime / por Josefa Cristina Tomaz Martins Kunrath. – 2014.

158 f.

Orientador: Profa. Dra. Ivone Freire Costa.
Dissertação (Mestrado) – Universidade Federal da Bahia, Faculdade de
Direito, 2015.

1. Criminalidade. 2. Crime por computador. 3. Políticas públicas. I.
Universidade Federal da Bahia

CDD- 364

JOSEFA CRISTINA TOMAZ MARTINS KUNRATH

**A EXPANSÃO DA CRIMINALIDADE NO CIBERESPAÇO:
DESAFIOS DE UMA POLÍTICA CRIMINAL DE PREVENÇÃO AO
CIBERCRIME**

Dissertação apresentada como requisito para obtenção do grau de Mestre em Segurança Pública, Justiça e Cidadania, Faculdade de Direito da Universidade Federal da Bahia.

Aprovada em 22 de agosto de 2014.

Banca Examinadora

Ivone Freire Costa — Orientadora _____

Doutora em Sociologia Econômica e das Organizações pela Universidade Técnica de Lisboa, Lisboa, Portugal.
Universidade Federal da Bahia

Eduardo Manuel de Freitas Jorge _____

Doutor em Difusão do Conhecimento pela Universidade Federal da Bahia. Professor Adjunto do SENAI, Departamento Regional da Bahia

Pedro Heitor Barros Geraldo _____

Doutor em Ciência Política pela Faculté de Droit et de Science Politique, da Université Montpellier 1, Montpellier, França,
Universidade Federal Fluminense

A Deus, fonte de todos os seres e todas as coisas, por ter me concedido a fé e esperança num mundo melhor.

À minha família, meus amores, Paulo Henrique Kunrath, pelo companheirismo, apoio e incentivo ao meu aperfeiçoamento acadêmico. Aos meus filhos Alexandre e Vinicius pela confiança, e, muitas vezes, pelas presenças silenciosas nas intermináveis horas de leituras.

À minha mãe Alzira Tomaz Martins, que aos 85 anos, com leveza e sabedoria, continua orientando seus filhos a persistir nos caminhos de uma vida digna e com laços afetivos fortes. Aos meus irmãos Marcos, Cátia, Gláucia e Ana Paula, pelo amor fraterno que me dedicam.

AGRADECIMENTOS

A todos que contribuíram para a concretização deste Mestrado.

A minha Orientadora e Coordenadora do Mestrado Profissional em Segurança Pública, Justiça e Cidadania, Professora Doutora Ivone Freire Costa, pelo dinamismo e empolgação na produção de conhecimento na área da Segurança Pública.

Ao Tribunal de Justiça da Bahia, à Escola de Magistrados – Emab e à Universidade Estadual de Feira de Santana-BA - UEFS.

Aos colegas de Mestrado pelo convívio prazeroso e fortalecimento dos laços de amizade.

É preferível prevenir os delitos a ter de puni-los; e todo legislador sábio deve antes procurar impedir o mal que repará-lo, pois uma boa legislação não é mais do que a arte de proporcionar aos homens a maior soma de bem-estar possível e livrá-los de todos os pesares que se lhes possam causar, conforme o cálculo dos bens e dos males desta existência.

Cesare Beccaria (1764, p.96)

KUNRATH, Josefa Cristina Tomaz Martins. **A expansão da criminalidade no ciberespaço: desafios de uma política criminal de prevenção ao cibercrime**. 158 f. il. 2014. Dissertação (Mestrado) — Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2014.

RESUMO

Esta dissertação busca examinar, teoricamente, algumas das dimensões do cibercrime e a crescente prática de ilícitos no âmbito do ciberespaço, sob a interferência de paradigmas culturais impostos pela virtualização global da sociedade contemporânea. A grande incidência de ataques aos usuários do ciberespaço, para prática de ilícitos e crimes informáticos, implica no importante fenômeno da criminalidade cibernética, que se apresenta como um fenômeno global e em expansão, tendo despertado a preocupação da comunidade internacional, diante da constatação de que os ilícitos cibernéticos constituem real perigo ao livre e pleno exercício dos direitos fundamentais, verdadeira ameaça ao pleno desenvolvimento humano e econômico, no sentido universal. A metodologia empregada baseia-se em pesquisa exploratória, de coleta de documentos textuais, partindo da análise qualitativa do fenômeno pesquisado. A pesquisa revelou que o Estado brasileiro não dispõe de meios suficientes para coibir a prática de crimes no ciberespaço, por ausência de criminalização de alguns ataques cibernéticos considerados importantes, pela carência da estrutura da polícia judiciária para realizar investigações e, ainda, pela morosidade da Justiça. Enfim, nessa abordagem, pretende-se suscitar a discussão da importância da prevenção como a linha da Política Criminal, em face do fenômeno em ascensão da ciberdelinquência, bem como contribuir para o desenvolvimento de uma atitude reflexiva e crítica sobre os atuais quadros epistemológicos no campo das políticas públicas de segurança e políticas públicas criminais.

Palavras-chave: Cibercrime. Cibercriminalidade. Política criminal. Prevenção.

KUNRATH, Josefa Cristina Tomaz Martins. **The expansion of criminality in cyberspace: challenges of a criminal policy to prevent cybercrime.** 158 f. il. 2014. Dissertation (Master) — Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2014.

ABSTRACT

This thesis has as an aim to examine, in theory, some of the dimensions of cybercrime and the growing practice of illegal acts in the area of cyberspace, under the interference of cultural paradigms imposed by global virtualization of contemporary society. The high incidence of attacks on the users of cyberspace in the practice of illicit acts and computer crimes implies in the important phenomenon of cyber criminality that presents itself as a global and expanding phenomenon that has aroused the concern of the international community, based on the fact that cybercrimes constitute a real danger to the free and full exercise of fundamental rights and a true threat to the full human and economic development in the universal sense. The methodology used is based on exploratory research, collection of textual documents starting from the qualitative analysis of the research phenomenon. The results that were obtained showed, in the context of the Brazilian reality, given the observation that cybercrime grows in the same proportion as the new digital technologies, the insufficiency or lack of a criminal policy with intent to curb the expansion of criminality in cyberspace reflects upon society, increasing the feeling of fear and impunity. Thus, one can contextualize the questioning about the role of the State in the prevention and penal prosecution, the absence or excessive criminalization of illicit computer acting from the approach of criminal and public safety policies. The research revealed that the Brazilian State does not have at hand sufficient means to deter the practice of cybercrimes due to the lack of considering a crime some cyber attacks that are considered important, because of the shortage of structure of the judiciary police to carry out investigations and also because of the slow pace of Justice. Finally, in this approach there exists the intent to arise discussion about the importance of prevention as a line of Criminal Policy in the face of the rising phenomenon of cyber delinquency as well as contribute to the development of a reflective and critical attitude toward the current epistemological frameworks in the field of public policies of security.

Keywords: Cybercrime. Cyber criminality. Criminal policy. Prevention.

LISTA DE ILUSTRAÇÕES

Figura 1 – Internautas domiciliares ativos entre 2000 e 2012.....	21
Figura 2 – Estatísticas dos incidentes reportados ao CERT.br. Valores acumulados: 1999 a 2013.....	39
Figura 3 – Estatísticas dos incidentes reportados ao CERT.br , por mês, de janeiro a dezembro de 2013.....	40
Figura 4 – Resumo das atividades do Balcão de Justiça e Cidadania	134

LISTA DE ABREVIATURAS E SIGLAS

AC – Autoridade Certificadora

Acadepol – Academia de Polícia Civil

ADR – *Alternative Dispute Resolutions* [resolução alternativa de litígios]

Anatel – Agência Nacional de Telecomunicações

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Cetic.br – Centro de Estudos sobre as Tecnologias da Informação e da Comunicação

CGI.br – Comitê Gestor da Internet no Brasil

CNJ – Conselho Nacional de Justiça

DDOS – *distributed denial of service*

DJU – Diário de Justiça da União

DOS – *denial of service*

ibid. – *ibidem* [na mesma obra]

IBOPE – Instituto Brasileiro de Opinião Pública e Estatística

inc. – inciso

IP – *Internet Protocol* [protocolo de internet]

loc. cit. – loco citato [no local (trecho) citado anteriormente]

MJ – Ministério da Justiça

ODR – *Online Dispute Resolution*

OECD – *Organization for Economic Cooperation and Development*

ONU – Organizações das Nações Unidas

PC – *personal computer* [computador pessoal]

PL – Projeto de Lei

Pronasci – Programa Nacional de Segurança Pública com Cidadania

SSP – Secretaria de Segurança Pública

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

SUSP – Sistema Único de Segurança Pública

TI – Tecnologia da Informação

TIC – Tecnologia da Informação e da Comunicação

TJBA – Tribunal de Justiça do Estado da Bahia

URL – *Uniform Resource Locator* [Localizador de Recursos Uniforme]

WWW – *World Wide Web* ['teia (de âmbito) mundial']

SUMÁRIO

1	INTRODUÇÃO	14
2	A INTERNET	19
2.1	O DIREITO DE ACESSO À INTERNET COMO NOVO DIRETO HUMANO...	22
2.2	O DIREITO DE ACESSO À INTERNET NO BRASIL	25
3	AS RELAÇÕES NO ÂMBITO DO CIBERESPAÇO E DA CIBERCULTURA... ..	28
3.1	O FENÔMENO DA CRIMINALIDADE NO CIBERESPAÇO.....	32
3.2	A CRIMINALIDADE INFORMÁTICA SOB O ENFOQUE DAS TEORIAS CRIMINOLÓGICAS: A SUBCULTURA DA DELINQUÊNCIA CIBERNÉTICA.	36
4	O CIBERCRIME: ASPECTOS CONCEITUAIS	50
4.1	CLASSIFICAÇÃO DO CIBERCRIME	53
4.2	ESPECIFICIDADES DO CIBERCRIME	56
4.3	CIBERCRIME NA LEGISLAÇÃO PENAL BRASILEIRA.....	61
4.3.1	Crimes Informáticos: Leis n.º 12.735 e n.º 12.737/2012.....	65
4.3.1.1	<i>Invasão de dispositivo informático.....</i>	<i>69</i>
4.3.1.2	<i>Interrupção ou perturbação de serviço informático</i>	<i>72</i>
4.3.1.3	<i>Falsificação de cartão de crédito ou débito</i>	<i>74</i>
5	DESAFIOS DE UMA POLÍTICA CRIMINAL DE PREVENÇÃO AO CIBERCRIME.....	76
5.1	POLÍTICA DE SEGURANÇA PÚBLICA	77
5.2	POLÍTICA CRIMINAL DE PREVENÇÃO AO CIBERCRIME	86
5.2.1	A criminalização de ilícitos informáticos e prevenção	91
5.2.2	As Leis 12.735 e 12.737/2012 sob o enfoque da prevenção	97
5.3	POLÍTICAS PREVENTIVAS INOVADORAS	101
5.3.1	Política de segurança digital	102
5.3.2	Políticas de educação informacional e ética na internet	108
5.3.3	Política de solução de conflitos nas relações virtuais.....	116
5.3.3.1	<i>Desjudicialização e a reserva da jurisdição.....</i>	<i>121</i>
5.3.3.1.1	<i>O campo jurídico contra a desjudicialização</i>	<i>127</i>
5.3.3.1.2	<i>Vias sociais de solução de litígios</i>	<i>132</i>

5.3.3.1.3	Vias alternativas de solução de conflitos cibernéticos.....	140
6	CONCLUSÕES PARCIAIS	147
	REFERÊNCIAS	151

1 INTRODUÇÃO

No ápice do desenvolvimento da sociedade hodierna, globalmente considerada, experimenta-se o recente fenômeno da universalização das comunicações, através da rede mundial de computadores, a internet. Este surpreendente instrumento tecnológico permite o acesso fácil às informações e o desenvolvimento de praticamente todas as atividades da vida contemporânea, possibilitando relações interpessoais e de comunidades virtuais, em novo lócus, o ciberespaço, tornando-se indispensável ao desenvolvimento das potencialidades intelectuais, lúdicas e profissionais das pessoas e organizações, enfim da sociedade.

Com a mesma preocupação da comunidade internacional, a sociedade brasileira contemporânea, cada vez mais conectada com as facilidades da rede mundial de computadores, vivencia atônita, o aumento desmesurado do crime informático, também chamado crime virtual ou cibercrime.

Frequentemente, a imprensa traz notícias de invasão de *hackers* a sítios do governo, empresas, personalidades do mundo político, artístico empresarial, simples cidadãos, partidos políticos, times de futebol, etc., com danos para a segurança dos sistemas informáticos, ante a divulgação de conteúdo de documentos confidenciais.

É importante salientar que a criminalidade cibernética apresenta peculiaridades que a distingue da criminalidade comum. De um modo geral, esses delinquentes possuem mais conhecimentos tecnológicos do que o mero usuário da Internet, além de, muitas vezes, buscarem aperfeiçoamento e sofisticação das técnicas com o propósito de praticar ilícitos digitais.

A criminalidade cibernética constitui real perigo ao livre e pleno exercício dos direitos fundamentais, constituindo verdadeira ameaça ao pleno desenvolvimento da dignidade humana no sentido universal, eis que a nova criminalidade cibernética apresenta-se com características transnacionais.

A constatação notória de que os países usuários da internet são vulneráveis ao crime praticado no ambiente virtual desencadeou reações e tomada de posições dos países que criaram, desenvolveram e utilizam a alta tecnologia informática, partindo-se do consenso de que a conjuntura é grave e demanda a adoção de medidas de prevenção e combate a essa modalidade delitiva.

Desde a Convenção de Budapeste de 2001, os Estados membros do Conselho da Europa e os Estados signatários dessa convenção, conscientes das profundas mudanças trazidas pela digitalização, pela convergência e pela globalização permanente das redes informáticas, constataram a necessidade de se estabelecer uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço.¹

Além do caráter transacional do cibercrime, que dificulta a investigação e persecução, o Brasil, ainda, não é signatário de tratado ou convenção internacional sobre a cibercriminalidade, caracterizando, neste aspecto, omissão de política criminal, que afeta e limita o poder punitivo do Estado Brasileiro, nos crimes virtuais ocorridos dentro do território nacional, com repercussão em outras nações, ou praticados no exterior, com resultado no território nacional.

A atual conjuntura brasileira enseja uma ampla discussão em torno dos problemas ligados ao aumento da cibercriminalidade, passando não só pelo debate acerca da chamada política criminal ante a expansão do fenômeno como, também, pela ampla discussão dos fatores que levam à impunidade dessa modalidade de crime.

Sob a perspectiva da problemática de políticas públicas de prevenção, a elaboração de uma legislação que criminaliza condutas não é suficiente e, às vezes, pode produzir efeito contrário ao propósito da repressão, tendo em vista que são diversos os fatores que dificultam o controle do problema crescente da criminalidade.

Assim, a pesquisa tem como objetivo precípua a discussão crítica acerca da compreensão do fenômeno da cibercriminalidade, sob a ótica da nova criminologia, confrontando-se não apenas com os aspectos puramente penais, mas conjugando alternativas interdisciplinares, na busca de respostas que contribua no campo da Política Criminal, para a prevenção de práticas ilícitas no ciberespaço.

Sob o prisma desse debate, questiona-se se é possível e viável a prevenção primária, aquela que se destina a evitar que o fato ilícito ocorra ou que os prejuízos

¹ Convenção sobre o Cibercrime. Budapeste, 23 de novembro de 2001. Preâmbulo: Os Estados Membros do Conselho da Europa e os seguintes Estados signatários, [...]. Convictos da necessidade de prosseguir, com caráter prioritário, uma política criminal comum, com o objectivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adopção de legislação adequada e da melhoria da cooperação internacional; Conscientes das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanentes das redes informáticas; [...].

desse ilícito sejam minimizados, antes que os atos estatais de persecução se desencadeiem. De tal modo, busca-se debater a viabilidade e adequação de proposições e orientações, com escopo de indicar mecanismos e instrumentos preventivos extrajurídicos e extrajudiciais para a redução da cibercriminalidade.

Nesse contexto, a presente dissertação **“A expansão da criminalidade no ciberespaço: desafios de uma política criminal de prevenção ao cibercrime”**, tem como premissa o fenômeno do aumento dos crimes virtuais, e da criminalidade informática, que constitui um desafio para a criação e implementação de uma política criminal voltada para a prevenção ao cibercrime, diante da atual conjuntura econômica, sociocultural e normativa do Brasil, inserido no mundo globalizado, cada vez mais dependente da tecnologia informática para consolidação e intensificação do progresso do país.

Com efeito, o problema da investigação enfoca o crescimento do cibercrime e a exponencial expansão da delinquência cibernética, enquanto fenômeno social relevante para a segurança pública, confrontando-se à necessidade do Estado Brasileiro perseguir, em caráter prioritário, uma política de prevenção à cibercriminalidade, os desafios para concretizar e realizar tal desiderato, diante da complexidade da atuação de condutas desviantes no ciberespaço, com a discussão de proposições de Política Criminal mais adequadas à prevenção e à redução da cibercriminalidade.

Portanto, a presente pesquisa justifica-se pela pertinência, relevância e atualidade, considerando o fenômeno globalizado do cibercrime, orientando-se pela contemporânea tendência da internacionalização dos mecanismos de prevenção e combate à cibercriminalidade, que tem atingido os mais variados bens jurídicos tutelados, com séria repercussão na economia interna e no comércio internacional e, sobretudo, no campo do direito à segurança digital dos usuários da internet.

A metodologia empregada baseia-se em pesquisa exploratória, de coleta de documentos textuais, a exemplo da Convenção sobre o Cibercrime de Budapeste, partindo da análise qualitativa do fenômeno pesquisado, e procura descrever, compreender e definir o problema da pesquisa e suas hipóteses.

No desenvolvimento foi utilizado o processo indutivo, buscando oferecer interpretação aberta, não reducionista, das hipóteses estudadas, seus significados focados nas principais abordagens, sempre com o objetivo de oferecer contribuições com fundamento multidisciplinar, pautada na revisão de literatura de obras

bibliográficas jurídicas de Direito Constitucional, Penal, Direito Civil, Sociologia, Sociologia da Solidariedade, Sociologia Jurídica, Criminologia e Filosofia, bem como em estudos especializados, periódicos, artigos e jurisprudência, acessados através da internet.

Insta frisar que a presente pesquisa não está calcada na concepção puramente dogmática do Direito Penal, com construções teóricas sobre a natureza jurídica dos institutos ou elementos constitutivos dos tipos penais. A abordagem dos principais cibercrimes já positivados na legislação nacional será sintética e a título enunciativo, para proporcionar uma visão das condutas ilícitas mais comuns, com apenas algumas incursões nos aspectos objetivos e subjetivos mais relevantes, sob a perspectiva da prevenção.

Além da contextualização desta introdução, no segundo capítulo, faz-se uma abordagem panorâmica sobre a internet, o direito ao acesso à internet como um novo direito anexo às prerrogativas fundamentais e à dignidade da pessoa humana, passando-se em seguida, a focar o ciberespaço, sua dimensão e as relações estabelecidas no âmbito virtual, sob o enfoque sociológico da formação do que se convencionou denominar de cibercultura, buscando situar os novos paradigmas culturais impostos pela virtualização da sociedade contemporânea, com os fenômenos da globalização e seus efeitos nas relações humanas ditadas pela urgência na sociedade pós-moderna, rapidamente habituada às respostas instantâneas oferecidas pela internet.

A seguir, introduz-se o problema da nova criminalidade que surgiu com os avanços tecnológicos aplicados ao computador e à internet, como fenômeno que ultrapassa as soberanias estatais, sob o viés de algumas teorias da Criminologia Crítica, na tentativa de traçar analogicamente as condutas dos ciberdelinquentes sob a vertente das teorias criminológicas a respeito do crime, o controle social e a defesa social.

No terceiro estágio do trabalho, abordam-se os aspectos conceituais do cibercrime, sua classificação e especificidades quanto à alta tecnologia empregada, à instantaneidade, ao anonimato, às dificuldades de identificação da autoria, à repercussão da internet – à extraterritorialidade, dentre outras características. No passo seguinte, analisam-se os tipos penais de cibercrime previstos na legislação penal brasileira, especialmente as Leis n.º 12.735 e 12.737, de 30 de novembro de 2012, que introduzem no ordenamento penal os delitos informáticos.

Por último, põem-se em relevo os desafios para adoção de Política Criminal de prevenção que, para ser realizável, interfere no paradigma do monopólio estatal da jurisdição, colocando na centralidade valorativa da quebra desse paradigma os mecanismos alternativos de solução dos conflitos gerados no meio cibernético, a serem desenvolvidos e postos em prática no âmbito da própria rede mundial de computadores, deixando para a Jurisdição Estatal a competência residual dos conflitos não resolvidos pelas técnicas alternativas, ou que pela importância e natureza do direito discutido, o Estado, como titular da Jurisdição, deva atuar através do poder jurisdicional.

2 A INTERNET

A internet surgiu nos Estados Unidos em 1962, por criação de Paul Baran, como consequência de pesquisas na área de tecnologia militar, que objetivava estabelecer uma rede de telecomunicação o menos vulnerável possível a um ataque nuclear soviético, na época da guerra fria entre americanos e russos, e a primeira rede, denominada Arpanet, foi conectada em 1969 entre quatro potentes computadores da época (FERREIRA, 2010, p. 80).

Comercialmente, no Brasil, a internet passou a ser utilizada a partir de 1995, quando a Agência Nacional de Telecomunicações (Anatel), com o objetivo de regular o uso de meios da Rede Pública de Telecomunicações e os Serviços de Conexão à Internet, através da Norma 004/1995², que define a internet como

nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos necessários à comunicação entre computadores, bem como o "software" e os dados contidos nestes computadores;

Em junho de 2005, em Nota Conjunta³ divulgada pelos Ministério das Comunicações e Ministério da Ciência e Tecnologia, comunica-se a necessidade de informar à sociedade a respeito da introdução da internet no Brasil, em nota pública, afirmando-se que: “O Governo considera de importância estratégica para o País tornar a INTERNET disponível a toda a Sociedade, com vistas à inserção do Brasil na **Era da Informação**.” (grifos no original).

Nesse documento, Ministério das Comunicações e Ministério da Ciência e Tecnologia esclarecem a forma do funcionamento da internet no país, definindo a estrutura e organização de redes na forma de “**espinhas dorsais** (*backbones*), que são estruturas de rede capazes de manipular grandes volumes de informações, constituídas basicamente por roteadores de tráfego interligados por circuitos de alta velocidade.” (grifos no original). As espinhas dorsais possuem âmbito nacional, de abrangência regional, estadual ou metropolitana, que possibilitarão a interiorização da internet no País.

² Disponível em: <http://www.anatel.gov.br/hotsites/Direito_Telecomunicacoes/TextoIntegral/ANE/prt/minicom_19950531_148.pdf>.

³ Nota Conjunta de junho de 1995, divulgada pelos Ministério das Comunicações e Ministério da Ciência e Tecnologia, itens 2.2 a 2.5.

A referida Nota Conjunta de 2005 divulga, ainda, que “**os provedores de acesso ou de informações**” conectados às espinhas dorsais são os efetivos prestadores de serviços aos usuários finais da internet, com acesso tipicamente através do serviço telefônico, esclarecendo que os prestadores de serviços ficam sob a responsabilidade de diversas entidades, e sob o controle da iniciativa privada, de livre escolha do usuário final.

Sabe-se que o explosivo avanço da informática nas últimas décadas vem causando um impacto profundo sobre as instituições sociais, políticas e financeiras de praticamente todas as nações do mundo, contribuindo para a formação do fenômeno da globalização.

Segundo o sociólogo Octavio Ianni (1994), a globalização está calcada nos novos processos tecnológicos, conquanto a sociedade global apresenta-se articulada por emissões, ondas, mensagens, signos, símbolos, redes e alianças que tecem os lugares e as atividades, os campos e as cidades, as diferenças e as identidades, as nações e as nacionalidades. Esses são os meios pelos quais se desterritorializam mercados, tecnologias, capitais, mercadorias, ideias, decisões, práticas, expectativas e ilusões.

Inegavelmente a internet como fruto das novas tecnologias, dentre elas a informática, a eletrônica e as telecomunicações, tecem uma nova ordem organizacional do tempo e do espaço, envolvendo capitais, pessoas e informações, dando ensejo a um novo arranjo do capitalismo, em âmbito global (IANNI, 1994).

O Brasil desponta em quinto lugar entre os 20 países com maior número de pessoas conectadas na rede mundial de computadores, atrás apenas do Japão, da Índia, dos Estados Unidos e da China.⁴ Segundo essa mesma fonte, as vendas do comércio eletrônico cresceram de R\$ 540 milhões para R\$ 18 bilhões, em dez anos.

De acordo com pesquisa do Ibope Media, o número de pessoas com acesso à internet no Brasil ultrapassou, pela primeira vez, os 100 milhões. Os dados referentes ao primeiro trimestre de 2013 indicam que o país tem 102,3 milhões de internautas, dos quais 72,7 milhões têm acesso em casa ou trabalho e 53,7 milhões efetivamente navegam em casa ou no trabalho, segundo dados de abril de 2013.⁵

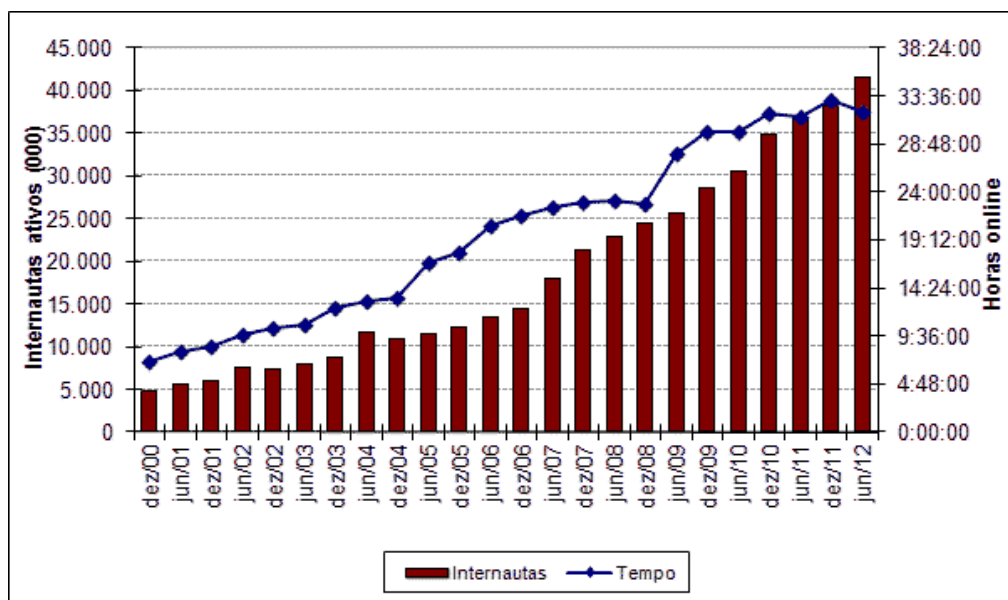
⁴ Disponível em: <<http://info.abril.com.br/noticias/internet/brasil-e-o-quinto-pais-mais-conectado-do-mundo-22042012-7.shl>>.

⁵ Disponível em: <<http://tecnologia.uol.com.br/noticias/redacao/2013/07/10/numero-de-internautas-no-brasil-ultrapassa-100-milhoes-segundo-ibope.htm>>.

Não obstante, segundo dados da pesquisa elaborada pelo Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (Cetic.br), em junho de 2013, são 80,9 milhões de usuários de internet no Brasil, mas a expansão nas classes D e E, nas zonas rurais, ainda é um desafio, evidenciando que o novo direito humano de acesso à internet ainda é inalcançável aos milhares de brasileiros pobres, moradores das zonas rurais, desafiando políticas públicas inclusivas, com a ampliação e desoneração de mecanismos de acesso à internet, com a expansão da banda larga para o interior, inclusive para a zona rural do país. A inclusão digital ainda é uma realidade distante para a maioria da população brasileira. Apenas cerca de 40% da população tem acesso à internet.

De todo modo, houve significativa evolução, conforme aponta pesquisa realizada pelo Instituto Brasileiro de Opinião Pública e Estatística (IBOPE), maior empresa privada de pesquisa da América Latina, com significativo crescimento do número de internautas domiciliares entre os anos de 2000 a 2012 (ver Fig. 1), atingindo, em junho de 2012, cerca de 41,4 milhões de internautas domiciliares, com uma média de 32:01 horas por mês.⁶

Figura 1 – Internautas domiciliares ativos entre 2000 e 2012



* Pessoas com 2 anos ou mais que navegaram na internet através de computadores no domicílio no mês

**Tempo médio de uso do computador pelos internautas brasileiros ativos no mês

Fonte: <<http://www.cetic.br/usuarios/ibope/tab02-01-cons.htm>>.

⁶ Disponível em: <<http://www.cetic.br/usuarios/ibope/tab02-01-cons.htm>>.

Essas pesquisas apontam para a expansão do acesso, o que amplia a democratização da informação, educação e cultura, sobretudo nas grandes áreas metropolitanas, no que pese a deficiência do interior e zona rural.

Outro dado interessante publicado na Revista Galileu, com dados da comScore, diz respeito ao perfil do internauta brasileiro nas redes sociais, como *Facebook*, *Twitter*, *Orkut* e listas de discussões. Do total, 90,8% dos internautas do país acessam ao menos uma dessas plataformas e gastam em média 4,9 horas mensais na vida social *on-line*. Do universo de internautas que acessam redes sociais, 58,7% são mulheres.

As redes telemáticas, nas quais se inclui a internet, mais do que um meio de comunicação, afiguram-se como um espaço de práticas sociais, novas expressões culturais e de sociabilidade, estabelecidas pelos usuários em suas interfaces. Com efeito, a crescente interdependência entre o ser humano e a máquina, numa interação própria do agora em que as invenções tecnológicas fazem parte do dia a dia, sem as quais a sociedade contemporânea não pode prescindir. O computador tornou-se uma ferramenta indispensável para a realização das tarefas mais diversas desde o trabalho ao lazer.

Passar um período do dia *on-line*, ou seja, conectado com a internet, tornou-se algo necessário na sociedade contemporânea, inexoravelmente adaptada à comunicação instantânea, que diminui as distâncias e incrementa a globalização. Tudo isso aproxima a vida real do mundo cibernético, e parece criar um novo *locus* — o ciberespaço, despertando o interesse da sociedade interconectada, bem como do Direito, face aos perigos e conflitos que surgem com a conectividade.

A sociedade hodierna tem na informática uma ferramenta indissociável para galgar novas metas de desenvolvimento da humanidade e, portanto, não tolera qualquer prática que possa prejudicar tais avanços.

2.1 O DIREITO DE ACESSO À INTERNET COMO NOVO DIREITO HUMANO

A Organização das Nações Unidas (ONU) publicou um relatório sobre promoção e proteção do direito à liberdade de opinião e expressão enfatizando que o acesso à internet deve ser universal e garantido pelos países soberanos.

Segundo a ONU, impedir o acesso à internet é um crime e uma violação dos direitos humanos, por isso, todo cidadão possui direito à liberdade de expressão e de acesso à informação por qualquer tipo de veículo, sendo que impedir o acesso à informação pela *web* constitui infração ao artigo 19, item 3, do Pacto Internacional de Direitos Civis e Políticos, de 1966.

Na linha de fundamentação do Relatório, são referidos casos de países que bloqueiam na rede conteúdos específicos impedindo o acesso de seus cidadãos. Em outros casos, infratores condenados por crime de violação de direitos autorais ou intelectuais são proibidos do acesso à internet, o que para o Relatório da ONU, viola o direito humano de acesso à informação e à internet.

Ainda de acordo com disposições desse Relatório, na hipótese de ter havido transgressão de alguma lei, envolvendo meios de comunicação, o agressor pode sofrer restrições específicas, não sendo aceitável exclusão total ao acesso à informação, ressaltando apenas as hipóteses em que os ilícitos praticados colocarem em risco os direitos e reputações de outras pessoas ou a segurança nacional. Nesse documento, a ONU qualifica como crime impedir o acesso à internet, constituindo violação aos direitos humanos.

Dentro desta concepção, a ONU concita os países que revejam suas leis que estabelecem punições severas contra os acusado de ter cometido violações de direitos autorais ou intelectuais e as punições adotadas, para que não contrariem as diretrizes divulgadas no referido documento da organização.

De acordo com o plano de diretrizes, editado pela ONU, realça-se o direito ao acesso como direito humano com repercussão nos direitos à liberdade de opinião e livre pensamento e expressão, que vem a ser, em última análise, um dos pilares da internet como um bem global livre, constituindo-se num veículo de informação, compartilhamento de conhecimento, de criação de novas tecnologias, divulgação e publicação de estudos, opinião sem fronteiras e que torna o mundo mais conectado, diminuído e ultrapassando as fronteiras. O direito à informação, hoje, perpassa pelo amplo acesso à internet. A Constituição Federal de 1988 erigiu o direito à informação a patamar de direito fundamental, estatuidando no inciso XXXIII do seu art. 5º:

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

Contudo, o direito fundamental à informação não se confunde com um novo direito da pessoa humana já reconhecido por organismos internacionais, qual seja, o direito ao acesso à internet.

Desde a Convenção de Budapeste sobre o Cibercrime, ocorrida em Budapeste em 23 de novembro de 2001, há um consenso de que o acesso à internet deve ser livre e amplo, merecendo ser acolhido e incentivado por todos os países, com a adoção de políticas públicas de inclusão digital, disseminado o acesso de forma respeitosa ao corpo normativo de cada soberania e aos direitos fundamentais.

Caracterizado pelas Nações Unidas como direito humano essencial ao desenvolvimento da personalidade e, também, das pessoas jurídicas e organizações não empresariais e não governamentais, o acesso à internet enseja proteção das ações danosas e das falhas de segurança, a que estão sujeitos os usuários, ante a grande habilidade tecnológica de internautas mal intencionados, em especial dos *hackers* e *crakers* que, em razão de seus conhecimentos técnicos, podem impedir, com um único ataque, milhares ou milhões de internautas e serviços disponibilizados por meio da internet.⁷

A discussão a que nos propomos parte da reflexão da importância contextual e ideológica sobre o direito ao acesso à internet como direito humano de última dimensão, sua repercussão sobre os direitos à liberdade de opinião, livre pensamento e expressão e a sua delicada coexistência com os pilares da internet, vista como um bem global livre, que serve de veículo de informação, compartilhamento de conhecimento, de criação de novas tecnologias, divulgação e

⁷ “Os sites da SSP (Secretaria de Segurança Pública) da Bahia e da Acadepol (Academia de Polícia Civil) da Bahia foram invadidos por hackers neste sábado (8) e estão fora do ar. As páginas tiveram as informações institucionais substituídas por um desenho de um boneco quebrando um computador com um cassete. Também ao abrir a página inicial podia-se ouvir a música “Porcos Fardados”, do cantor Marcelo D2, que faz duras críticas a policiais corruptos. As invasões foram assinadas pelo grupo ‘Slayers Brazil Hackteam’. O grupo tem uma página no Facebook com 976 seguidores. Na fanpage, os hackers mostram diariamente os sites que conseguiram ser invadidos. Na lista estão a prefeitura de São Gonçalo (RJ), Universidade Federal de Pelotas (RS), empresas brasileiras e sites internacionais. Neste sábado, a lista continha os dois sites da Bahia. O site da SSP oferece serviços à população como delegacia virtual, ouvidoria e informações sobre as ações da polícia, que não puderam ser acessadas devido à invasão. Até a publicação deste texto os sites continuavam sem funcionar. Em nota, a secretaria confirmou a invasão e informou que o site ficará fora do ar enquanto a equipe de Tecnologia da Informação ‘estiver trabalhando para normalizar a situação no tempo mais breve possível’.” [...]. Notícia veiculada em 08 mar. 2014. Disponível em: <<http://noticias.uol.com.br/cotidiano/ultimas-noticias/2014/03/08/hackers-invadem-sites-da-secretaria-de-seguranca-e-acadepol-na-bahia.htm>>.

publicação de estudos, manifestação de pensamento sem fronteiras, tornando o mundo mais conectado, diminuído e ultrapassando fronteiras.

Em sua obra *Cibercultura*, Pierre Lévy (2007) aborda diversas experiências relacionadas à internet, com abordagens sociológicas e filosóficas, acerca da tecnologia e da concepção de sistemas de informação inteligentes, com destaque da relação entre a internet e o desenvolvimento humano na sociedade atual, apontando como o grande problema da internet, a dificuldade ao acesso das pessoas.

A dignidade da pessoa em seu aspecto axiológico ganha significativo reforço com o reconhecimento de que o acesso à internet tem um espectro iluminador e de reforço dos demais direitos das diversas dimensões, como o direito à vida, à liberdade e à liberdade de expressão.

Contudo, do mesmo modo que o acesso à internet potencializa a fruição dos direitos fundamentais, os reais riscos que pairam em decorrência das falhas de segurança imputadas às novas tecnologias trazem em si real risco de violação e da negação de fruição desse direito humano de nova geração.

2.2 O DIREITO DE ACESSO À INTERNET NO BRASIL

O Brasil, hoje, conta com a disposição normativa chamada Marco Civil da Internet, prevendo direitos, deveres e responsabilidades de provedores, internautas, empresas, bem como dos poderes Executivo, Legislativo e Judiciário na *web*.

O Projeto de Lei 2.126/2011 foi encaminhado à Câmara dos Deputados, por iniciativa do Ministério da Justiça, após consultas públicas envolvendo diversos segmentos da sociedade civil. Sancionado, o referido projeto deu origem a Lei n.º 12.965, de 23 abril de 2014, que contrapõe à tendência de se estabelecerem restrições, condenações ou proibições relativas ao uso da internet, tornando-se o marco regulatório, concebido com o propósito de dotar o ordenamento jurídico de uma legislação que garanta direitos relativos ao acesso e uso livre da *web*, sem restrições às liberdades de pensamento, opiniões e ao desenvolvimento criativo de novas tecnologias.

Esta lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. O acesso à internet é reconhecido como direito de todo cidadão:

Art. 4º A disciplina do uso da Internet no Brasil tem por objetivos a promoção:

I - do direito de acesso à Internet a todos os cidadãos; (grifo nosso)

II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III- da inovação e fomentar a ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV- da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

O direito de acesso à internet passa a ser tratado como direito essencial ao exercício da cidadania, podendo-se afirmar com segurança, numa interpretação sistemática, partindo-se do marco constitucional, que é pretensão do legislador delinear o direito de acesso à internet como direito universal e essencial ao exercício da cidadania, ferramenta de desenvolvimento social, ganhando *status* de direito fundamental. Neste âmbito, destacam-se as disposições contidas no artigo 7º do Marco Civil da Internet:

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

- XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
- XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
- XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

No que diz respeito à livre manifestação de pensamento, ao direito de privacidade e do sigilo das comunicações do usuário pela internet, a disposição prevista no art. 8º do Marco Civil da Internet reafirma o que já decorre da Carta Constitucional, ao dispor que “a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet.”

O problema, no entanto, grassa a realidade fática no que concerne ao uso inescrupuloso da *web*, com constantes e crescentes ocorrências de crimes cibernéticos, há alguns anos, alvo de preocupações dos países detentores de novas tecnologias e de desenvolvimento econômico e social.

Ocorre que, não obstante permear em todos a necessidade de cuidados básicos quando se navega pela *web*, é alto o grau de riscos que estão sujeitas as redes de computadores e a velocidade com que novas tecnologias são criadas com a finalidade de romper as blindagens digitais, o que constitui uma realidade palpável.

Felizmente, ao contrário do que se apregoa, a esmagadora maioria dos usuários da internet utiliza a rede com boas intenções. Apenas pequena parcela de usuários extrapola a linha da boa-fé, da ética e da urbanidade, violando os basilares direitos à privacidade, ao sigilo das informações, em desrespeito aos diretos e em proveito promíscuo individual e de grupos delinquentes. O problema maior é que, às vezes, em um só ataque cibernético pode-se causar prejuízos econômicos e extrapatrimoniais de proporções imensáveis.

Do ponto de vista de um bem juridicamente relevante, o direito ao acesso à internet mostra-se como o conteúdo ético nas relações virtuais e apresenta-se como forte componente no sentido de ser exigido o desenvolvimento das diversas atividades com a maior acessibilidade e segurança possível.

3 AS RELAÇÕES NO ÂMBITO DO CIBERESPAÇO E DA CIBERCULTURA

Fala-se em um novo mundo, o mundo cibernético. A incrível revolução tecnológica, nas últimas décadas, eclodiu uma nova realidade social nas diversas culturas espalhadas pelos continentes terrestres, insurgindo uma simbiose do mundo real e virtual, que está cada vez mais difícil estabelecer limites, se é que existem, não sendo mais possível dissociar o mundo virtual da realidade cotidiana.

A rede de computadores possibilitou uma multiplicidade de formas de comunicação e de sociabilidades, criando um novo espaço, o espaço virtual, o chamado ciberespaço. A propósito, o professor André Lemos da Universidade Federal da Bahia, afirma que

o ciberespaço é um espaço sem dimensões, um universo de informações navegável de forma instantânea e reversível. Ele é dessa forma um espaço mágico; já que caracterizado pela ubiquidade, pelo tempo real e pelo espaço não físico. Todos esses elementos são característicos da magia como manipulação do mundo (LEMOS, 1996, p. 1).

Apesar das relações cibernéticas trazerem em si um risco alto de práticas delitivas, tal constatação não impediu que a sociedade contemporânea desenvolvesse o sentimento de confiança e encantamento para com a rede mundial de computadores, tanto que passou a utilizá-la para as mais diversas necessidades e relevantes objetivos, pela facilidade, rapidez e relativa segurança.

Com a evolução social proveniente do desenvolvimento tecnológico, surgiram novas relações, mais céleres e muito mais intensas, com o estreitamento das relações sociais, a disseminação de bens, ante a facilidade de transmissão de informações, levando a sociedade a deparar-se com uma nova realidade. Assim, pode-se afirmar que, na contemporaneidade, esse novo paradigma ético tem afetado globalmente a sociedade no sentido da formação de uma nova cultura.

Segundo Pierre Lévy (1999, p. 16),

o neologismo “cibercultura”, especifica aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modo de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço.

Argumenta, ainda, que as implicações culturais do desenvolvimento do ciberespaço levam ao problema do impacto social e cultural decorrentes da utilização das novas tecnologias onde ocorrem movimentos sociais com características peculiares. Na ordem de ideias desse autor, o ciberespaço, também chamado de rede, “é o novo meio de comunicação que surge na intercomunicação mundial de computadores” (LÉVY, 1999, p. 17), sendo que seu significado abrange tanto o “universo oceânico de informações que ele abriga, assim como os seres humanos que navegam e alimentam esse universo” (Ibid., loc. cit.), onde se podem perceber movimentos sociais e culturais como as comunidades virtuais.

É interessante pontuar esse novo fenômeno das comunidades virtuais, a conectividade e oportunidade surgidas com a rede mundial de computadores. Nesse aspecto, Corrêa (2004, p. 5) chama atenção para essa nova forma de relacionamentos interpessoais:

De qualquer modo, o ciberespaço potencializa o surgimento de comunidades virtuais e de agregações eletrônicas em geral que estão delineadas em torno de interesses comuns, de traços de identificação, pois ele é capaz de aproximar, de conectar indivíduos que talvez nunca tivessem oportunidade de se encontrar pessoalmente. Ambiente que ignora definitivamente a noção de tempo e espaço com barreiras.

Observa André Lemos (2003), que a sociedade contemporânea vivencia profundas modificações no espaço urbano, nas formas sociais e nas práticas da cibercultura, com a emergência das novas formas de comunicação.

A cibercultura nada mais é do que a cultura contemporânea em sua interface com as novas tecnologias de comunicação e informação, ela está ligada às diversas influências que estas tecnologias exercem sobre as formas de sociabilidade contemporâneas, influenciando o trabalho, a educação, o lazer, o comércio, etc. Todas as áreas da cultura contemporânea estão sendo reconfiguradas com a emergência da cibercultura. (LEMO, 2003, p. 1).

As relações na sociedade da informação se efetivam através do uso das tecnologias presentes nos dias atuais, definindo uma nova época, e ocorrem na dimensão do ciberespaço. Assim, o espaço físico vem perdendo a importância, frente às novas possibilidades tecnológicas que também influenciam e outras variáveis como o tempo e distância, volumes e medidas.

Na era tecnológica, por exemplo, o ciberespaço abriga uma biblioteca virtual totalmente diferenciada do modelo físico tradicional, onde pode abrigar uma enorme quantidade de obras, em espaço reduzidíssimo, e disponibilizar ferramentas de buscas que faz a pesquisa chegar ao interessado em questão de segundos. Do mesmo modo, em outras áreas científicas, como da nanotecnologia, as novas tecnologias vêm revolucionando as ciências, a exemplo da medicina e da robótica, com constantes anúncios de fantásticas descobertas que contribuem para a saúde e o bem-estar da humanidade.

Neste contexto, o uso crescente de tecnologias digitais, marcadas por uma relação entre a técnica e a vida social propiciou, segundo Corrêa (2004, p. 2), “o surgimento de novas formas de agregação social de maneira espontânea no ambiente virtual, com práticas culturais específicas que constituem a chamada cibercultura”, numa alusão a uma nova realidade que perpassa por transformação e rápidas em simbiose com os avanços tecnológicos:

A revolução tecnológica concentrada nas Tecnologias da Informação e da Comunicação (TICs), que possibilita a conexão mundial via rede de computadores, promove alterações significativas na base material da sociedade, ao estabelecer uma interdependência global entre os países e modificar as relações Estado-Nação e sociedade. O uso crescente de redes como a Internet resultou na criação de uma organização social, a sociedade em rede, que permite a formação de comunidades virtuais, grupos constituídos pela identificação de interesses comuns. (CORRÊA, 2004, p.1).

O mundo cibernético tornou-se um âmbito no qual se descortinam, com muito mais clareza, os diversos campos do conhecimento, numa verdadeira democratização das informações e dos saberes da humanidade.

Inegavelmente, vivenciamos o nascer de uma nova era, a era da revolução da informação e comunicação, através da tecnologia da informação (TI), com inimaginável quebra de paradigmas intelectuais, com visíveis transformações culturais da nova geração conectada e tornando o mundo real e cibernético cada vez uma realidade mais ampla e indissociável, com largo desenvolvimento da humanidade, considerada, por muitos cientistas, maior e muito mais importante e benéfica à humanidade que a revolução industrial.

Portanto, a sociedade contemporânea oferece um mundo tecnológico bastante diversificado e variado no que diz respeito às novidades tecnológicas.

O computador conectado à internet apresenta-se como um valioso e enriquecedor universo, no qual, o processo de ensino e aprendizagem dos internautas se constitui uma fonte inesgotável de possibilidades de relações participativas e cooperativas.

Neste cenário, a problemática ligada ao acesso e ao não acesso, implica nas consequências da inclusão e da exclusão social e digital, no contexto da nova realidade da sociedade em rede, onde se verifica o fenômeno da produção e acesso às informações coletivas num processo semelhante e, possivelmente, mais intenso em fluxo de informações, onde não é mais possível identificar com muita precisão onde se situa o mundo virtual e a realidade.

Assim, a relação do homem com a técnica tem sido marcada pelo fascínio e pelo medo, nos seus aspectos positivos e negativos, despertando posições favoráveis e contrárias, com cada posição carregada de argumentos positivos e destrutivos, a depender da posição.

Por esta razão que, dentro das sociedades dessa época, sugere-se um olhar especial sobre a internet, sobretudo para as questões como a ética, a livre expressão, controle de acesso, internet x computador, entre outras questões, as quais ensejam debates e reflexões da sociedade, como um todo, a titulares e, ao mesmo tempo, destinatários de direitos afeitos à cidadania (LEMOS, 2003).

A formação e o elo ideológico ou apenas de amizade entre essas comunidades virtuais são uma tendência na atualidade, levando a se estabelecer nova forma de relação humana em compasso com a circulação das informações, atingindo dimensões cada vez mais amplas em escala global, só possível diante da capacidade interativa da rede mundial de computadores, o que possibilita considerar que é grande, e ímpar, a oportunidade de aproximação do outro, do vizinho, do colega, do desconhecido, do estrangeiro, enlanguescer, também, a noção de comunidade. Nesta perspectiva:

Para que o sentimento de comunhão se propague, é necessário que haja compartilhamento de saberes, de conhecimento, de opiniões que podem até mesmo ser divergente, uma vez que no interior da comunidade, os participantes podem e devem ter opiniões contraditórias e conflitantes, que é uma forma saudável de verificar o grau de tolerância entre seus membros. Além disso, a existência de ideias conflitantes pode resultar na elaboração de novos saberes, construídos a partir de debates e discussões (CORREIA, 2004, p.8).

A partir do ambiente virtual, formam-se grupos de internautas com interesses comuns, os quais se organizam para trocar experiências, conhecimentos, defenderem crenças, ideologias, expandir os negócios ou, simplesmente, para jogar *videogames* em sua comunidade virtual. De outra banda, ocorre a formação de grupos com propósitos egoísticos e destrutivos.

Nas relações estabelecidas no ciberespaço, estudos sociológicos buscam situar o indivíduo na sociedade contemporânea, em face dos fenômenos como a globalização e os novos paradigmas culturais impostos pela sociedade da informação, intensificando a convivência com a virtualização das relações humanas, que sofrem as nuances ditadas pela urgência desta sociedade pós-moderna, que exige cada vez mais respostas imediatas às suas necessidades que, somente, as facilidades da rede mundial de computadores podem oferecer.

O ciberespaço constitui, assim, um universo paralelo onde flui intenso fluxo de ligações entre o mundo material e o mundo imaterial, o que leva a uma maior compreensão entre ambos os espaços (LÉVY,1999).

É no ciberespaço, onde se desenvolvem as relações entre os grupos de internautas conectados em rede, as chamadas comunidades ou as tribos, que se forma uma cibercultura com novas identidades, linguagem, com elos e sentimento de pertencimento a um grupo, cujos integrantes assumem posturas e comportamentos relacionados àquela comunidade virtual.

3.1 O FENÔMENO DA CRIMINALIDADE NO CIBERESPAÇO

Na contemporaneidade, o desenvolvimento da multiplicidade das relações através da internet propiciou o surgimento de um novo gênero de criminalidade, impulsionado pela sensação de anonimato e liberdade que a internet e a realidade virtual proporcionam a usuários, especialmente aos mais jovens. Atrás de um computador, é possível criar e assumir muitas faces, falsas identidades, mascarando o verdadeiro caráter, podendo qualquer pessoa, com conhecimento médio de informática, passar-se por outra, com o propósito deliberado de praticar ilícitos, nesse agitado e veloz mundo cibernético.

A escalada do cibercrime é um fenômeno mundial. O Brasil, conforme notoriamente noticiado pela imprensa nacional e estrangeira, é um paraíso da pirataria virtual.⁸ E, desde a criação da internet, no final da década de 60, o ilícito cibernético vem crescendo exponencialmente, na mesma proporção da ampliação da *web* pelo globo terrestre.

Lamentavelmente, o cibercrime é uma realidade ocorrente em todos os países que desfrutam de alta tecnologia, sendo que o Brasil, no atual estágio tecnológico, infelizmente, é um território com grande incidência de ataques cibernéticos.

As ações criminosas visam, principalmente, às fraudes de instituições financeiras, empresas com propósitos de desviar dinheiro, espionagem industrial, bem como objetivos outros como pirataria de programas e pornografia infantil, tráfico de bens e mercadorias ilícitas, intolerância racial, dentre outras condutas ou, simplesmente, a diversão de grupos de *cracker*, *haker*, *preacher*.

O chamado cibercrime constitui a exteriorização de condutas ilícitas dos usuários das tecnologias da informação e internautas, cada vez mais recorrentes no ciberespaço, e vem exigindo do Estado brasileiro reação célere e eficaz no seu combate, sob pena dessa omissão do Estado, guardião da segurança pública, desestabilizar a ordem pública, a segurança pública e, até mesmo, a soberania nacional.

Segundo indicadores da Central Nacional de Denúncias de Crimes Cibernéticos, através do portal SaferNet Brasil, criado em 20 de dezembro de 2005, em Salvador-BA, em oito anos de funcionamento do *site*, criado em Salvador e destinado a receber registro de crimes cibernéticos, a SaferNet Brasil recebeu e processou 3.417.208 denúncias anônimas envolvendo 527.061 URLs distintas, escritas em 9 idiomas e hospedadas em 63.673 *hosts* diferentes, conectados à internet através de 34.927 números IPs distintos, atribuídos a 94 países, em 5 continentes. As denúncias foram registradas pela população através dos 7 *hotlines* brasileiros que integram a Central Nacional de Denúncias de Crimes Cibernéticos.

⁸ Segundo notícia veiculada em revista de grande circulação nacional: "Hackers brasileiros são bastante atuantes, ficando atrás apenas dos *hackers* chineses [...]". "O Brasil sofreu o maior ataque de hackers de sua história no início da madrugada da quarta-feira 22, quando os sites da Presidência da República, da Receita Federal e o Portal Brasil ficaram fora do ar por uma hora. O portal da Petrobras também foi invadido. Entre a meia-noite e meia e as três horas da manhã, houve mais de dois bilhões de acessos." "Piratas da computação derrubam sites do governo brasileiro na internet e mostram que o sistema pode ser mais vulnerável do que se pensava." Lúcio Vaz - Revista Isto É, Ed. 2172, 25. jun. 11, 10h56.

Ainda de acordo com a SaferNet Brasil, a central nacional de denúncias de crimes cibernéticos, embora instituição privada que tem a finalidade de atuar com vista a uma internet livre e ética, e única na América Latina e Caribe, recebe uma média de 2.500 denúncias (totais) por dia, envolvendo páginas contendo evidências dos crimes de pornografia infantil ou pedofilia, racismo, neonazismo, intolerância religiosa, apologia e incitação a crimes contra a vida, homofobia e maus tratos contra os animais. Do total de denunciante, 99% escolhem a opção de realizar a denúncia anonimamente. E, ao 1% restante, é garantido total e completo anonimato.

Institucionalmente, a organização afirma que o “projeto representa a resposta brasileira a um esforço internacional, que reúne, atualmente, 22 países empenhados em coibir o uso indevido da Internet para a prática de crimes contra os Direitos Humanos”.⁹

Nas redes sociais que abrigam grupos de pessoas que se aproximam por interesses comuns e compartilhamento de ideias, relacionamentos interpessoais, obtenção de informações e lazer, constantemente são alvos de pessoas mal-intencionadas protagonistas de atos atentatórios a boa convivência social e das mais diversificadas condutas ilícitas.

Os crimes contra a honra, nas modalidades de calúnia, injúria e difamação, ocorrem com bastante frequência nas redes sociais e se alastram com extrema facilidade, pela ágil disseminação das ofensas postadas na rede, potencializando as consequências nefastas para as vítimas, ante as características da circulação dos conteúdos veiculados pela internet. Outros ilícitos graves, como a invasão de privacidade, ameaças, assédio sexual, assédio moral (*Bullying*), têm permeado constantemente os diversos sítios, correios eletrônicos e redes sociais. A falsificação de perfil é o ilícito mais comum em vários tipos de mídias, como *blogs* e *sites* de relacionamento.

Um dos mais terríveis crimes que envolvem a exploração sexual de crianças e adolescentes, a pedofilia virtual consiste em produzir, publicar, vender, adquirir e armazenar pornografia infantil pela rede mundial de computadores, por meio das páginas da *web*, *e-mail*, *newsgroups*, salas de bate-papo (*chat*) ou qualquer outra forma. Compreende, ainda, o uso da internet com a finalidade de aliciar crianças ou adolescentes para atividades sexuais ou para exposição pornográfica.

⁹ Disponível em: <<http://www.safernet.org.br/site/>>. Acesso em: 10 mar. 2014.

A propagação e disseminação de vírus são práticas ilícitas muito utilizadas por criminosos. O vírus, segundo a Cartilha de Segurança para Internet, é um programa ou parte de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas. A propagação e infecção por vírus de computador se dá por vários meios, dentre os quais *e-mail* e telefone celular, com a finalidade de espionar informações pessoais não autorizadas do usuário, senhas, abrir janelas indesejadas, travar ou deixar lento o desempenho da máquina, sempre causando transtornos e prejuízos aos usuários na internet (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012, p. 24).

São conhecidos outros programas e arquivos maliciosos, os códigos maliciosos espalhados pelos atacantes do ciberespaço como *Worm* (verme), *Bot* e *Botnet*, *Spyware*, *Keylogger* (capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador), *Backdoor* (programa que permite o retorno de um invasor a um computador), *Trojan* ou *Trojan-horse* (cavalo de troia – instala outros códigos maliciosos) (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012, pp. 25-27).

Fraudes financeiras são levadas a efeito através de mensagens eletrônicas conhecidas como *Phishing*, quando os golpistas, fazendo-se passar pela instituição bancária, enviam comunicação semelhante ao padrão do banco, para tentar “pescar” senhas e dados financeiros (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012, p. 9).

O envio de grande quantidade de *e-mails* não solicitados, contendo mensagens de conteúdo exclusivamente comercial, prática conhecida como *Spam*, não constitui crime, mas é considerada prática abusiva porque, além de causar congestionamento da rede, importunam o usuário, pelo conteúdo e natureza das mensagens (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012, p. 33).

Percebe-se, assim, que o uso, em larga escala, da internet trouxe consigo novos riscos, dentre os quais o fenômeno do crescimento dos ilícitos cibernéticos, que, além da violação ao direito ao amplo acesso e à segurança digital, vêm causando prejuízos financeiros de toda ordem¹⁰.

¹⁰ O site do Jornal *on-line* Estadão.com.br, traz a seguinte manchete: **Hackers acessam dados de usuários em ataque ao Evernote**, em recente notícia veiculada no dia 4 mar. 2013: “Serviço online terá que redefinir senha de 50 milhões de usuários. SÃO FRANCISCO – O Evernote vai redefinir a senha de 50 milhões de usuários devido ao ataque de hackers que sofreu, informou o serviço de compartilhamento de notas pela internet. A porta-voz do Evernote, Ronda Scott, declarou por e-mail

Como todas as relações que ocorrem no ciberespaço, os ilícitos são condutas humanas que não podem ser tolerados ou ignorados, já que trazem consequências ao mundo real, trazendo às vítimas, prejuízos materiais e sofrimentos, humilhações e toda gama de lesão, situações com as quais o processo civilizatório da humanidade não tolera conviver.

Como fato social relevante, o uso generalizado da internet nas mais básicas e corriqueiras atividades do cotidiano faz surgir para o direito o legítimo interesse de regular as condutas desviantes da normalidade, sobretudo as que atingem bens e valores juridicamente tutelados.

O Cibercrime é uma realidade inerente ao ciberespaço, do mesmo modo que o crime comum está inserido na realidade não virtual. Em decorrência da nocividade dos ilícitos ocorrentes na internet, discutem-se as várias formas de prevenção e punição para os transgressores, normalmente afetas ao campo jurídico penal e à Criminologia, na tentativa de se compreender e coibir tão nefasta prática.

A crescente incidência de ataques aos usuários do ciberespaço para prática de crimes informáticos implica no importante fenômeno da criminalidade cibernética. Segundo os paradigmas teóricos da moderna Criminologia, pode ser identificado um perfil semelhante dos infratores internautas (*hacker, cracker, etc.*), como pertencentes da “teoria da subcultura da delinquência”.

A seguir, aborda-se a problemática da crescente criminalidade no ciberespaço, sob o prisma de algumas teorias criminológicas.

3.2 A CRIMINALIDADE INFORMÁTICA SOB O ENFOQUE DAS TEORIAS CRIMINOLÓGICAS: A SUBCULTURA DA DELINQUÊNCIA CIBERNÉTICA

Para a compreensão da problemática, será feita uma breve abordagem sobre o perfil do internauta infrator e, em seguida, uma breve incursão sobre as teorias

no sábado que o ataque ‘seguiu um padrão similar’ a outros crimes cibernéticos cometidos na últimas semanas contra outras companhias de internet. ‘Em nova investigação de segurança, não encontramos provas de que algum conteúdo armazenado no Evernote tenha sido acessado’, disse a empresa no site. ‘Também não temos nenhuma prova de que informações sobre pagamento de clientes Evernote Premium e Evernote Business tenham sido acessadas’, acrescentou.” Disponível em: <<http://blogs.estadao.com.br/link/hackers-acessam-dados-de-usuarios-em-ataque-ao-evernote/>>. Acesso em: 4 mar. 2013.

criminológicas das subculturas, com a pretensão de contextualizar a problemática da cibercriminalidade e o delinquente virtual.

A necessidade de se adotar políticas públicas criminais destinadas a controlar e prevenir a cibercriminalidade, que se apresenta com características diferenciadas da criminalidade comum, requer uma abordagem criminológica da problemática, considerando a ausência de uma política pública, específica nesta área, baseada em estudos científicos, com visão pluralista e atualizada do fenômeno da ciberdelinquência, com escopo de subsidiar as agências estatais legislativa, executiva e judiciária à compreensão do fenômeno da ciberdelinquência e lidar, eficazmente, para a redução e prevenção do cibercrime.

Os diversos comportamentos dos criminosos tecnológicos vêm sendo objeto de observação de sociólogos e juristas nas diversas legislações estrangeiras, especialmente naquelas que já possuem disciplina legislativa sobre o cibercrime.

No Brasil, são escassos os estudos criminológicos destinados a traçar o perfil criminológico dos delinquentes informáticos, contudo existem algumas abordagens que mesclam os aspectos jurídicos e criminológicos da criminalidade informática. Entende-se por crime de informática a conduta ilícita praticada através do uso de computador em rede ou não que produz dano material como destruição ou corrupção de dados técnicos do equipamento, seus componentes e/ou aos dados e sistemas, bem como dano extrapatrimonial. Segundo Aras (2010, p. 12):

[...] a criminalidade informática, fenômeno surgido no final do século XX, designa todas as formas de conduta ilegais realizadas mediante a utilização de um computador, conectado ou não a uma rede (11), que vão desde a manipulação de caixas bancários à pirataria de programas de computador, passando por abusos nos sistemas de telecomunicação. Todas essas condutas revelam "uma vulnerabilidade que os criadores desses processos não haviam previsto e que careciam de uma proteção imediata, não somente através de novas estratégias de segurança no seu emprego, mas também de novas formas de controle e incriminação das condutas lesivas".

Dentre as práticas ilícitas dos delinquentes cibernéticos de maior frequência, estão as fraudes por meio da apropriação e utilização de senhas para acesso não autorizado de *e-mails*, sites pagos, conexões à rede, comércio ilegal; pornografia infantil destinada à satisfação de pedófilos; racismo; pirataria de áudios, vídeos e programas informáticos, músicas com violação aos direitos autorais; crimes contra a honra, através da divulgação de ofensas, imagens, vídeos nas redes sociais, *blogs*, *sites* de relacionamento, salas de bate-papo ou *e-mails* (COSTA, 1997).

Novas práticas ilícitas surgem numa velocidade proporcional às novas tecnologias, aplicativos e ao desenvolvimento, inovações da tecnologia da informação por internautas, individualmente considerados ou em grupos organizados de delinquentes, através das redes de computadores, à distância com elevados prejuízos para os usuários comuns, corporações, Estado e o comércio internacional.

Os infratores do ciberespaço são conhecidos e designados por nomes distintos para cada tipo de internauta, afeitos às práticas antiéticas e criminais. Os atacantes do ciberespaço mais conhecidos são os *hackers* (fuçadores em inglês), *crackers* (aqueles que quebram) e *phreaker* (especializado em obter informação não autorizada do sistema telefônico), dentre outros.

Os *crackers* apresentam maior potencial ofensivo, quer por puro vandalismo, quer por interesses pessoais, econômicos e até políticos, na medida em que se tratam de meros curiosos. São os infratores dotados de grande técnica, destreza, razoável conhecimento de informática, que buscam não serem notados e não se marcam pela violência, e possuem idade entre 15 e 30 anos e boa formação socioeducacional.¹¹

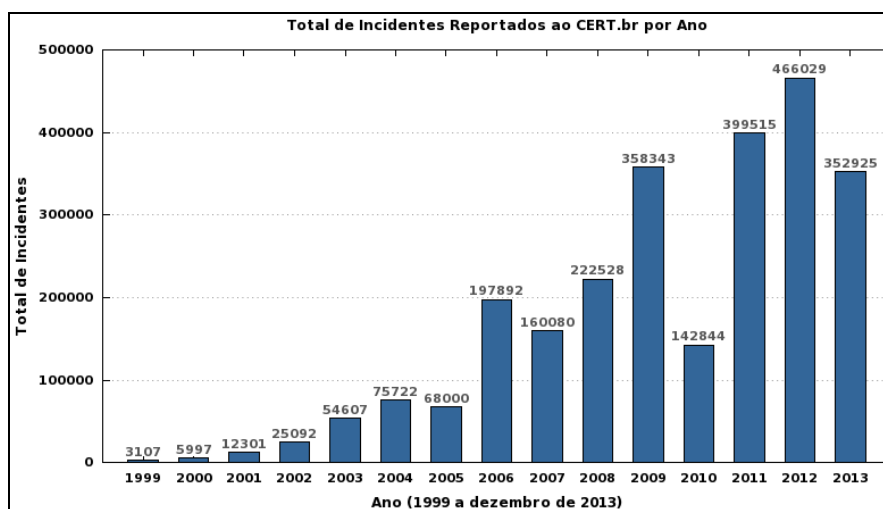
O Comitê Gestor da Internet no Brasil (CGI.br), entidade não governamental, através do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, elaborou uma Cartilha de Segurança para a Internet com recomendações e esclarecimentos sobre a segurança de internautas, com abordagens sobre os riscos de uso desta tecnologia e os cuidados a serem tomados pelos usuários para se protegerem das ameaças. Esclarece a Cartilha que a internet não tem nada de “virtual” e as precauções a serem tomadas devem fazer parte de todas as outras cautelas do dia a dia.

É oportuno declinar que o objetivo de conjecturar sobre um possível perfil dos *hackers*, *crackers*, etc, toma aqui alguns dados do estudo do CGI.br, para a elaboração da Cartilha de Segurança, que, embora, sem a natureza de um estudo sociológico, para o fim de informação da Criminologia, não deixa de constituir fonte confiável para auxiliar no estudo dos infratores ou comunidade de atacantes do ciberespaço que se aventuram pelo mundo das fraudes, golpes ou simplesmente invadem sistemas informáticos, apenas para se vangloriar da proeza.

¹¹ Disponível em: <<http://www.ibccrim.org.br> BuscaLegis>.

Adverte o CGI.br, com base nas estatísticas do seu Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, que os golpes, fraudes e ataques apresentam números estrondosos, cujas estatísticas (ver figuras 2 e 3)¹², a cada ano apresentam novas modalidades de práticas ilícitas *on-line*.¹³

Figura 2 – Estatísticas dos incidentes reportados ao CERT.br. Valores acumulados: 1999 a 2013.

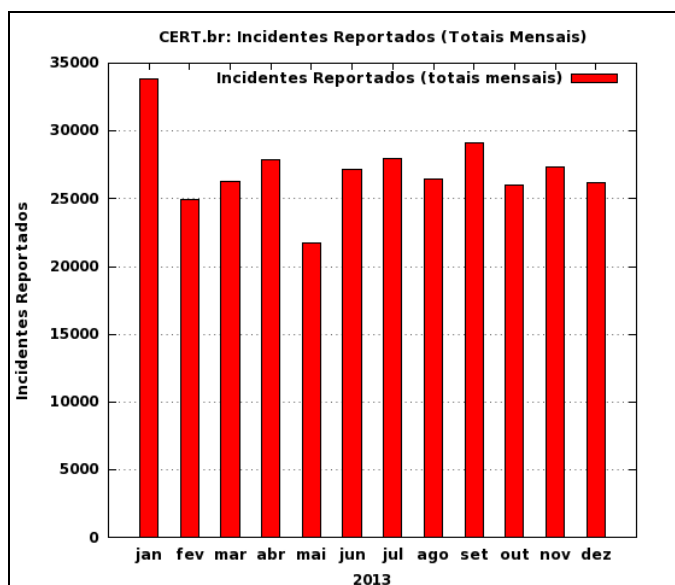


Fonte: <<http://www.cert.br/stats/incidentes/2013-jan-dec/ataques-mensal.html>>.

¹² Disponível em: <<http://www.cert.br/stats/incidentes/2013-jan-dec/ataques-mensal.html>>.

¹³ A 2ª Cúpula Latino-americana de Analistas de Segurança, realizada pela empresa de antivírus Kaspersky no fim de agosto de 2012, na capital equatoriana, revelou dados assustadores (apurados entre janeiro e agosto deste ano). Primeiro, páginas de pornografia e pirataria estão no topo das mais arriscadas. Destacam-se, também, as redes sociais, páginas que apresentam falsas promoções e prêmios e campanhas de pessoas que pedem dinheiro e ajuda. Para os especialistas no evento, a América Latina é o paraíso para os criminosos porque são países em crescimento econômico — principalmente o Brasil — com usuários imaturos e despreparados para as ameaças na web. Notícia veiculada em 4 set. 2012 pelo jornal Correio Brasiliense. Disponível em: <<http://www.correiobraziliense.com.br>>.

Figura 3 – Estatísticas dos incidentes reportados ao CERT.br , por mês, de janeiro a dezembro de 2013.



Fonte: <<http://www.cert.br/stats/incidentes/2013-jan-dec/ataques-mensal.html>>.

As estatísticas são realmente alarmantes, de modo que a Cartilha de Segurança para a Internet resume de forma pedagógica as principais ocorrências que põe o usuário da *web* em permanente vulnerabilidade. De uma forma simples, mas com bastante coerência, a Cartilha traça o perfil de internautas que realizam ataques de exploração de vulnerabilidade.¹⁴

Ataques costumam ocorrer na internet com diversos objetivos, visando a diferentes alvos e usando variadas técnicas. Qualquer serviço, computador ou rede que seja acessível via internet pode ser alvo de um ataque, assim como qualquer computador com acesso à internet pode participar de um ataque. Os motivos são bastante diversos, variando desde a curiosidade, a experimentação, simples diversão até a realização de ações criminosas. Alguns exemplos são:

Demonstração de poder: mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente.

Prestígio: vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar *sites* considerados visados ou difíceis de serem atacados; disputar com outros

¹⁴ “Hackers invadiram e-mails e sistemas de dados do Itamaraty. O Ministério não revelou quais informações foram acessadas, mas técnicos já trabalham para regularizar o sistema. A polícia federal também já iniciou uma investigação para apurar a origem dos ataques.” A reportagem foi exibida pelo canal de Televisão SBT Brasil.UOL Notícias. Disponível em: <<http://tvuol.uol.com.br/video/itamaraty-sobre-ataques-de-hackers-04024C993762D4815326/27/05/2014>>. Acesso: 2 jun. 2014.

atacantes ou grupos de atacantes para revelar quem consegue realizar o maior número de ataques ou ser o primeiro a conseguir atingir um determinado alvo.

Motivações financeiras: coletar e utilizar informações confidenciais de usuários para aplicar golpes.

Motivações ideológicas: tornar inacessível ou invadir *sites* que divulguem conteúdo contrário à opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia.

Motivações comerciais: tornar inacessível ou invadir *sites* e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas. (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012).

Nos últimos anos, em decorrência do crescimento acelerado dos índices dos crimes de tecnologia praticados via computador, houve um aumento vertiginoso dos índices oficiais da criminalidade como um todo. No entanto, é possível identificar e classificar as práticas delitivas que ocorrem através dos sistemas informáticos e/ou em rede, cuja conduta delituosa é atribuída à internauta ou a grupo organizado (quadrilha) de internautas, que apresentam algumas semelhanças em suas condutas, como observa Monteiro Neto (2008, p.112):

O perfil criado e divulgado pela mídia tem o criminoso eletrônico como sendo, em regra, indivíduo do sexo masculino, que trabalha de alguma forma com a utilização de computadores e sistemas eletrônicos, com idade entre 16 e 33 anos de idade, avessos a violência e que possuem inteligência acima da média. São extremamente audaciosos e aventureiros, movidos acima de tudo pelo desejo de conhecimento e de superação à máquina.

Hoje tais delinquentes são, em geral, pessoas que trabalham no ramo ligado a utilização de sistemas eletrônicos, não tão jovens nem inteligentes; são *insiders*, vinculados a empresas (em regra); sua característica central consiste na pouca motivabilidade em relação à norma (raramente se sensibilizam com a punição penal); motivos para delinquir: ânimo de lucro, perspectiva de promoção, vingança, apenas para chamar a atenção etc.

O aumento da criminalidade cibernética, de acordo com Monteiro Neto (2008, p.112), encontra respaldo basicamente em dois fatores. O primeiro fator parte da falsa ideia de que o mundo da tecnologia da informação, em especial a internet, é um mundo sem regras e sanções, dando a falsa impressão de que no mundo virtual “tudo que é praticado na rede, reveste-se do véu de anonimato de um monitor” (Ibid., loc. cit.). O segundo fator refere-se à “mudança de perfil do criminoso de tecnologia”, que passa a agir em grupamentos criminosos organizados que utilizam os recursos tecnológicos para praticarem condutas, objetivando auferir vantagens ilícitas. Outra observação interessante do referido autor é concernente à pluralidade de tratamento normativo conferido pelos Estados à matéria, levando os criminosos a delinquir nos

países de menor capacidade legal e tecnológica para intensificar suas práticas criminosas.

Já Vianna (2001), referindo-se ao estudo criminológico dos autores dos delitos informáticos, enquadra o comportamento de delinquentes cibernéticos segundo as teorias subculturais e as teorias da aprendizagem social (*Social Learning*), para explicar as motivações dos criminosos informáticos. Nesta perspectiva, identifica o comportamento desviante dos *hackes*, subsumindo-o à escola criminológica das subculturas, denominando-a de “Subcultura *cyberpunk*”, afirmando que significativa parcela de *hackers* experientes posta nas páginas da internet uma série de técnicas, com o fim de ensinar os primeiros passos para se tornar um criminoso digital, revelando que

[...] não se trata de um mero aprendizado técnico. Ocorre que na busca pelo conhecimento técnico o indivíduo acaba se influenciando pela **subcultura *cyberpunk*** na qual o reconhecimento de sua capacidade intelectual está diretamente relacionado às suas proezas ilegais. A invasão de *sites* importantes como os do FBI e da NASA garantem a seus autores grande prestígio. As pichações digitais são sinais de poder intelectual dentro da subcultura *hacker* e geram respeito e fama a seus autores. (VIANNA, 2001, p.57, grifo nosso).

Seguindo essa linha de pensamento, Vianna (2001) toma como paradigma as teorias criminológicas, sustentando o enquadramento dos *hackers* delinquentes, inserindo-os nas teorias das subculturas:

As teorias das subculturas criminais com destaques para os trabalhos de SUTHERLAND, *White-Collar Criminality*, e de COHEN, *Delinquent boys: the culture of the gang*, parecem adaptar-se perfeitamente para a explicação do fenômeno *hacker*. (VIANNA, 2001, p. 212).

Reconhece Vianna que, para a correta classificação dos *hackers*, também, é fundamental a realização de estudos específicos do comportamento de cada subgrupo, tendo em mira que o fenômeno da criminalidade tende a se alastrar à medida que mais pessoas se conectam à internet, tornando-se necessário um permanente estudo do comportamento criminoso na internet, objetivando a prevenção de condutas que coloquem em risco o desenvolvimento das relações no ciberespaço, ressaltando que “[...] certamente, o Direito Penal e a Criminologia também não poderão impedir a ação dos *hackers*. Cabe a eles, no entanto, evitar

que a frequência de tais condutas gere uma situação de anomia.” (VIANNA, 2003, p. 13).

As subculturas criminais são representadas por grupos sociais, comunidades que apresentam comportamento transgressor por diversas motivações, como demonstração de poder, obtenção de informações, aplicação de golpes financeiros, ou, simplesmente, para exploração curiosa de vulnerabilidades.

As teorias criminológicas da subcultura parecem explicar bem os fatores que condicionam determinados grupos que possuem alguma ligação, como vizinhança, preferências culturais, ideológicas, a exemplo das torcidas organizadas, imigrantes moradores da periferia, simpatizantes de movimento cultural ou de contracultura como *ravares*, *funks*, etc.

Em outro trabalho que enfoca as teorias criminológicas, com o título *O desvio social na rede mundial de computadores, aspectos sociológicos e psicológicos dos indivíduos pertencentes às subculturas criminais da internet*, Lucena (2012, p. 11) sustenta que, nesta modalidade delitiva, quando se fala em “cibercrime, em geral, pode ser constatado que, em relação ao perfil dos infratores, a maioria deles surge das camadas médias e altas da sociedade, sendo indivíduos com grandes habilidades e conhecimentos neste meio e, na sua maioria, jovens.”

Segundo a autora do referido estudo sociológico e psicológico, o fenômeno pesquisado pelo psicanalista John Suler é chamado de “efeito desinibitivo *on-line*”, que constatou, de fato, uma dissociação do comportamento do mundo virtual e do mundo físico, os fatores que interagem e dão origem a esse efeito: anonimato dissociativo, invisibilidade, assincronismo, introjeção solipsista, imaginação dissociativa e mineralização da autoridade. Sob o ponto de vista criminológico, a articulista equipara esse quadro ao que se denomina “subcultura criminal do mundo virtual” (LUCENA. 2012. p.14).

Os primeiros são, em geral, simples invasores de sistemas, que atuam por espírito de emulação, desafiando seus próprios conhecimentos técnicos e a segurança de sistemas informatizados de grandes companhias e organizações governamentais. No início da cibercultura, eram tidos como heróis da revolução informática, porque teriam contribuído para o desenvolvimento da indústria do *software* e para o aperfeiçoamento dos computadores pessoais e da segurança dos sistemas informáticos.

A moderna criminologia, inaugurada por Baratta (1999), trata da Criminologia Crítica e Crítica do Direito Penal, enfocando um panorama das teorias sociológicas sobre o crime e o controle social, os princípios da ideologia da defesa social, desconstruindo o discurso da Sociologia Criminal, que estuda o crime como uma realidade ontológica pré-constituída, bem como a Sociologia do Direito Penal, focada no processo de criminalização, no sistema penal e nos elementos constitutivos do crime e “o *status* social de criminoso” (BARATTA, 2004, p. 19).

Sob o enfoque das discussões preconizadas por Baratta, a criminologia crítica trabalha a ideia do desvio social, percebendo os processos de criminalização e os mecanismos de rotulação de criminosos a partir da mudança de paradigma. Os criminólogos devem compreender as forças sociais que moldam o crime e o criminoso.

Nessa perspectiva, ultrapassadas as concepções das Teorias Clássica e Positivista, e a comum ideologia da defesa social, Baratta (1999) separa as escolas criminológicas conforme o pensamento das teorias do consenso e as teorias do conflito. Neste sentido, ensina Shecaira (2011, p. 150):

Podemos agrupar duas visões principais da macrossociologia que influenciaram o pensamento criminológico. À primeira visão, de corte funcionalista, mas também denominada de teorias da integração, damos o nome mais amplo de teorias do consenso. A segunda visão, argumentativa, pode-se intitular, genericamente, de teorias do conflito. A escola de Chicago, a teoria da associação diferencial, a teoria da anomia e a teoria da subcultura delinquente podem ser consideradas teorias do consenso. Já as teorias do *labelling* (interacionista) e crítica partem de visões conflitivas da realidade.

Conforme a visão argumentativa de Shecaira (2011), nas teorias consensuais, a finalidade da sociedade é alcançada com o pleno funcionamento das suas instituições, “de forma que os indivíduos compartilham os objetos comuns a todos os cidadãos, aceitando regras vigentes e compartilhando as regras sociais dominantes.” (SHECAIRA, 2004, p. 151).

Com efeito, a estrutura social em funcionamento é baseada em um consenso entre seus membros, a estrutura e os valores, devendo todos contribuir para a manutenção do sistema. Ao passo que, na teoria do conflito, “a coesão e a ordem na sociedade são fundadas na força e na coerção, na dominação por alguns e sujeição dos outros; ignora-se a existência de acordos em torno de valores de que depende o próprio estabelecimento da força,” em consequência, toda a sociedade

está permanentemente sujeita a processos de mudança social o que leva ao conflito social (SHECAIRA, 2004, p. 150).

A Escola de Chicago, nas décadas de 30 e 40, contribuiu para a criação da moderna criminologia, rompendo a ideologia positivista. Desta escola destaca-se a Teoria da Subcultura Delinvente, que foi lançada através da obra de Albert Chohen (SHECAIRA, 2004).

A grande contribuição da Escola de Chicago são os estudos criminológicos sob a perspectiva interdisciplinar que considera os conceitos básicos ecológicos, considerando que a cidade não é apenas um amontoado de homes individuais, mas

[...], a cidade é um estado de espírito, um corpo de costumes e tradições e dos sentimentos e atitudes organizadas, inerentes a esses costumes e transmitidos por tradição [...]. As subculturas criminais são representadas por grupos sociais, comunidades que apresentam comportamento transgressor. [...] que é determinado um subsistema de conhecimento, crenças, e atitudes que possibilitam, permitem ou determinam formas particulares de comportamento transgressor em situações específicas [...]. (SHECAIRA, 2004, p. 151).

Conforme Cohen, a subcultura delinquecial caracteriza-se por três fatores: não utilitarismo, malícia da conduta e seu negativismo. O não utilitarismo revela-se na dispensabilidade da conduta ou do produto do crime, que são praticados mais para afirmar-se perante o grupo ou por mero prazer, estando ínsita a malícia do ato, impingindo repulsa ou hostilidade em outros jovens que não fazem parte da gangue. O negativismo é a característica que está ligada à polaridade e contradição entre a subcultura delinvente e os valores e normas da cultura em geral. (*apud* SHECAIRA, 2011, p. 252).

Ainda segundo Shecaira (2011), dentro das correntes da Escola de Chicago, destaca-se, também, a Teoria da Anomia, derivada da teoria social formulada por Durkheim, que trata da ausência de reconhecimento dos valores inerentes a uma norma, fazendo com que esta perca sua coercibilidade, de modo a levar o infrator a não reconhecer a legitimidade na sua imposição. A contribuição da teoria durkheimiana foi considerar o crime um fenômeno normal na sociedade, e sempre haverá quem não acate a autoridade da norma.

Para a Teoria da Anomia, esse não reconhecimento da norma é funcional e necessário para a reflexão dos valores normatizados face às mudanças sociais, o que é positivo no processo de criminalização e descriminalização de condutas.

Refinada por Merton, que afirma ser a anomia um sintoma do vazio produzido quando o meio socioestrutural não satisfaz às expectativas culturais da sociedade, e, assim, a falta de oportunidades induz à prática de atos irregulares ou ilegais para atingir os objetivos desejados.

A delinquência informática começa a ser detectada nos Estados Unidos, no final da década de 60, quando foram registrados casos de uso do computador para prática de delitos de manipulação de dados, sabotagem, espionagem e uso abusivo da ferramenta, pirataria.

Conforme declinado nesse estudo, os atacantes do ciberespaço, principalmente os *hackers* e o *crackers*, formam uma subcultura identificável pela mesma escala de valores, atitudes, desafios, prazeres, atuação antiética e delinquente, com liames axiológicos próprios, dissociados de valores da sociedade vigente.

Em reforço de argumentação, trasladando-se para a ciberdelinquência, merecem destaque as colocações de Baratta (2004, p. 76) a respeito da estratificação e pluralismo cultural dos grupos sociais:

Tanto a teoria funcionalista da anomia, quanto a teoria das subculturas criminais contribuíram, de modo particular, para esta relativização do sistema de valores e de regras sancionadas pelo direito penal, em oposição à ideologia jurídica tradicional, que tende a reconhecer nele uma espécie de *mínimo ético*, ligado às exigências fundamentais da vida da sociedade e, frequentemente, aos princípios de toda convivência humana.

A teoria da anomia põe em relevo o caráter *normal*, não patológico, do desvio, e sua função, em face da estrutura social, enquanto a teoria das subculturas criminais mostra que os mecanismos de aprendizagem e de interiorização de regras e modelos de comportamento, que estão na base da delinquência e, em particular, das carreiras criminosas, não diferem dos mecanismos de socialização através dos quais se explica o comportamento normal.

Com efeito, diante da influência destes mecanismos de socialização, o peso específico da escolha individual ou da determinação da vontade, como também o dos caracteres (naturais) da personalidade, é muito relativo. Deste último ponto de vista, a teoria das subculturas constitui não só uma negação de todas as teorias normativa e ética da culpabilidade, mas uma negação do próprio princípio de *culpabilidade*, ou responsabilidade ética individual, como base do sistema penal.

O quadro de teorias das subculturas criminais aqui apresentado não pode ser senão sumário. Contudo, interessa sublinhar o núcleo teórico contido nessas teorias, que se opõe ao princípio da ideologia da defesa social acima denominado *princípio da culpabilidade*. [...] A teoria das subculturas criminais nega que o delito possa ser considerado como expressão de uma atitude contrária aos valores e às normas sociais gerais, porém, é possível vislumbrar a existência de valores e normas específicos dos diversos grupos sociais (subcultura).

Só, aparentemente, está à disposição do sujeito, escolher o sistema de valores ao qual adere. Em realidade, condições sociais, estruturas e

mecanismos de comunicação e de aprendizagem determinam a pertença de indivíduos e subgrupos ou subculturas, e a transmissão aos indivíduos de valores, normas, modelos de comportamento e técnicas, mesmo ilegítimos.

Vianna (2003, p. 9), afirma que a realidade da maioria dos *hackers* adapta-se perfeitamente à teoria de Cohen, segundo a qual a marginalização de um grupo acaba gerando a criminalidade, e acrescenta que:

As teorias das subculturas criminais com destaques para os trabalhos de SUTHERLAND, *White-Collar Criminality*, e de COHEN, *Delinquent boys: the culture of the gang*, parecem adaptar-se perfeitamente para a explicação do fenômeno *hacker*. SUTHERLAND elaborou uma teoria conhecida como Teoria das Associações Diferenciais para explicar os crimes de colarinho branco na qual analisou as formas de aprendizagem do comportamento criminoso. *A hipótese aqui sugerida em substituição das teorias convencionais, é que a delinquência de colarinho branco, propriamente como qualquer outra forma de delinquência sistemática, é aprendida; é aprendida em associação direta ou indireta com os que já praticaram um comportamento criminoso, e aqueles que aprendem este comportamento criminoso não tem contatos freqüentes e estreitos com o comportamento conforme a lei. O fato de que uma pessoa torne-se ou não um criminoso é determinado, em larga medida, pelo grau relativo de freqüência e de intensidade de suas relações com os dois tipos de comportamento. Isto pode ser chamado de processo de associação diferencial.* (VIANNA, 2001, p. 182).

Os crimes informáticos, por suas características, exigem estudo de técnicas que permitam o domínio do computador para utilizá-lo na conduta criminosa, o que confere a atividade criminosa do *hacker* seja aprendida, ao contrário dos crimes clássicos como homicídio, furto e estupro, que não exigem qualquer tipo de conhecimento para serem cometidos. (VIANNA, 2001, p. 182).

Pontua Túlio Vianna que o *hacker* inserido no mundo digital desenvolve seus próprios códigos e valores criados dentro da subcultura. Suas façanhas são admiradas e respeitadas, mas discriminam aqueles que não possuem conhecimento necessário para ser um *hacker*, e muitos desprezarem os que agem com fins econômicos. Revela, ainda, que pesquisas indicam a existência na comunidade *hacker* de sua própria hierarquia: *elite*, *ordinary* e *darksiders*. Os *hackers* de elite são aqueles que desenvolvem seus próprios programas e ferramentas de ataque. *Hackers* comuns são os indivíduos que utilizam-se destas ferramentas criadas pelo grupo de elite. E os *darksiders* são aqueles envolvidos em atividades maliciosas, predatórias ou de fins econômicos. (VIANNA, 2001, p.178).

Contextualizando as teorias criminológicas sob a ótica das teorias do consenso da Escola de Chicago, considerando as características da teoria da anomia e a teoria da subcultura criminal, é possível vislumbrar melhor a adequação da teoria da subcultura aos internautas infratores, considerando a maior conexão com seus traços delineadores, bem mais visíveis do que a teoria da anomia, com a qual a subcultura da delinquência virtual também possui afinidade, mas em geral prevalecem os pontos de desencontros.

Reforça esse entendimento o visível fenômeno da globalização com a intensificação das relações sociais, culturais e comerciais no ciberespaço e, concomitantemente, o aumento da criminalidade informática crescente na mesma proporção que a internet se alastra pelo globo terrestre. Todo esse processo de visíveis progressos da rede mundial de computadores trouxe à sua margem uma legião de internautas que desafiam e desprezam qualquer noção de um agir ético e estabelecem seus próprios códigos e ideologias lesivas. A título ilustrativo transcreve-se a seguir a “oração dos hackers”, de autoria desconhecida extraída da internet¹⁵:

“Byte nosso de cada dia que nos trói hoje
Falsificado seja o vosso registro
Venha a nós o vosso password
Seja pirateada a vossa integridade
Assim na Web como no UNIX
O script nosso de cada dia que nos auxiliai hoje
Crackei os nossos programas
Assim como nós hackeamos aqueles que os tem obtido
Não nos deixeis cair na prisão
Mas nos livrai dos log files,
Disconnected.”

Apesar da distância, da diversidade de idiomas e peculiaridades culturais dos mais longínquos países, os internautas, individualmente considerados ou organizados em quadrilhas, atuam com certa semelhança nas técnicas de ataques e intenções lesivas, apresentando uma interconectividade sociocultural impulsionada pela facilidade de acesso e movimentação das informações no mundo virtual, formando, segundo o enfoque criminológico, uma criminalidade diferenciada que

¹⁵ Disponível em: <<http://forum.imasters.com.br/topic/349848-orao-hacker/>>. Acesso em: 20 jun. 2014.

atua no ciberespaço, proporcionando características de uma subcultura da delinquência cibernética.

Em síntese, de acordo com os paradigmas teóricos da moderna Criminologia, é perfeitamente possível identificar um perfil semelhante dos infratores internautas (*hacker, cracker, etc.*), como pertencentes à subculturas criminais, representadas por grupos sociais, comunidades que apresentam comportamento transgressor por diversas motivações, como demonstração de poder, obtenção de informações, aplicação de golpes financeiros ou, simplesmente, para exploração curiosa de vulnerabilidades e diversão.

4 O CIBERCRIME: ASPECTOS CONCEITUAIS

Nesta parte da dissertação, abordaremos os aspectos conceituais e classificatórios do cibercrime, a questão do *nomem juris* e as razões pelas quais são utilizados os termos relacionados aos delitos ocorrentes no ambiente virtual.

As condutas ilícitas praticadas no meio cibernético são as mais diversas possíveis, passando por condutas antiéticas à prática de crime propriamente considerado, como conduta antijurídica, lesiva e punível. São, portanto, incontáveis as condutas ilícitas possíveis de ocorrer no meio cibernético ou, através dele, abrangendo larga gama de delitos possíveis de se cometer na realidade física.

No entanto, há alguns procedimentos ilícitos que só podem ser realizados através dos meios eletrônicos, por sua especificidade, ou como na maioria dos casos, porque o bem juridicamente relevante é fruto dessa revolução tecnológica e só existe nesse espaço imaterial. Certo é que existem grande diversidade e infinidade de crimes virtuais, muitos ainda desconhecidos em seus caracteres ou o *modus operandi*, que sequer foram objeto de investigação por absoluto desconhecimento do grande público internauta ou das autoridades públicas.

Os ilícitos, através das redes telemáticas (*internet*) assumem várias nomenclaturas, tais como cibercrime, crime digital, crime informático, crime informático-digital, *cybercrime*, crimes eletrônicos, delitos de computador, delitos computacionais, crime de computação, etc. Todas essas nomenclaturas, às vezes, apontam para alguma especificidade, contudo não há consenso em relação ao *nomem juris*, nem quanto à definição, nem quanto à classificação destes crimes.

Sem consenso na doutrina, a expressão “crime digital” seria ampla demais por comportar muitas condutas e um número também grande de bens jurídicos afetados. O termo “Cibercrime” tem a preferência por se referir às novas tecnologias, inclusive é a nomenclatura utilizada pelo Acordo Internacional do Conselho da Europa, sobre o Cibercrime. (CRESPO, 2011, p. 50).

Segundo Aras (2001, p. 06), embora sejam empregadas várias expressões para designar ou aludir aos ilícitos virtuais, as mais recorrentes são crimes informáticos ou crimes de informática, ou cibercrime, pontuando que “crimes telemáticos” ou “cibercrimes” são expressões “mais apropriadas para identificar

infrações que atinjam redes de computadores ou à própria Internet ou que sejam praticados por essas vias.”

Embora a nomenclatura mais difundida internacionalmente seja “cibercrime”, originada do inglês *cybercrime*, no presente trabalho, os termos cibercrime, crime digital, crime informático, delitos virtuais são utilizadas como sinônimos. Contudo, é preciso distinguir os crimes comuns praticados por meio da tecnologia computacional daqueles que só ocorrem no ambiente virtual.

De um modo geral, a atividade criminosa, que pode ocorrer pelos meios comuns, utiliza do aparato tecnológico informático, para a prática de tipos penais adredemente previstos na norma incriminadora penal, a exemplo do estelionato e outras fraudes (art. 171 do Código Penal). Já os crimes informáticos próprios ou puros são figuras típicas que só podem ser praticados através de um sistema computadorizado, envolvendo as novas tecnologias de dados e informação.

Em verdade, os crimes de computador são, na maior parte das vezes, os crimes comuns cometidos com o auxílio de um computador, podendo os crimes de furto, apropriação indébita, estelionato ou dano ser cometidos por esse meio com consideráveis prejuízos patrimoniais. Entretanto, há algo além de um nova ferramenta, de um novo meio, de um novo *modus operandi* para o cometimento de crimes: estamos também diante de novas condutas não tipificadas. (FERREIRA, 2005, p. 32).

O Código Penal Brasileiro, em vigor desde 1940, evidentemente, não previa as condutas ilícitas que violam os novos direitos que surgiram na era digital, daí porque a necessidade de tipificar, e assim proteger, através da tutela penal, esses novos direitos, mormente os direitos de acesso à internet, à privacidade, o direito à informação, consubstanciado nos dados disponíveis e arquivados no ambiente virtual, de modo que a criminalização das condutas sem avaliar que essas tipificações são necessárias do ponto de vista da orientação dos princípios do direito penal mínimo.

Com o desenvolvimento civilizatório, cada vez mais surgem bens juridicamente relevantes e tutelados pela ordem constitucional sem que haja previsão de uma figura típica penal para a sua tutela.

Há uma gama de comportamentos ilícitos, conhecidos, que causam enormes transtornos e prejuízos na vida daqueles que baseiam suas atividades por meio eletrônico. As mais comuns são o furto de dados, a falsificação de documentos e a

invasão de sistemas. No mundo virtual distinguem-se as condutas inadequadas consideradas apenas comportamentos antiéticos, dos ilícitos civis, daquelas mais graves que a norma penal enquadra como contravenção ou crime.

De um modo geral, definição sobre criminalidade informática, sobre crime de computador, cibercrime, dentre outras terminologias, guardam, de certa forma, uma conectividade atrelada às novas tecnologias, exigindo do campo jurídico a redefinição ou criação de novos institutos e novos conceitos, ao tempo em que impõe uma ligação ente o Direito e a Ciência da Tecnologia da Informação, agregando ao Direito nova órbita de conceitos, definições e novos bens e interesses a serem tutelados juridicamente com o suporte do novo Direito da Informática.

No entendimento de Costa (1997), grande parte da doutrina define o *crime de informática* pelo bem jurídico protegido:

É a conduta que atenta contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar. Isto posto, depreende-se que o *crime de informática* é todo aquele procedimento que atenta contra os dados, que o faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão.

Para este autor, o crime de informática pressupõe dois elementos indissolúveis: “contra os dados que estejam preparados às operações do computador e, também, através do computador utilizando-se ‘software’ e ‘hardware’, para perpetrá-los.” Concluindo em seguida com o seguinte exemplo:

aquele que atea fogo em sala que estiverem computadores com dados, com o objetivo de destruí-los, não comete *crime de informática*, do mesmo modo, aquele que, utilizando-se de computador, emana ordem a outros equipamentos e cause, por exemplo, a morte de alguém. Estará cometendo homicídio e, não *crime de informática*. (COSTA, 1997).

Por seu turno, Aras (2001, p. 6) traz a definição elaborada desde 1986, pela OECD — *Organization for Economic Cooperation and Development*, no relatório publicado sobre o problema da criminalidade informática e a necessidade de tipificação de certas condutas, como fraudes financeiras, falsificação documental, contrafação de *software*, interceptação de comunicações telemáticas, dentre outros, de onde extraiu a definição de crime de computador:

“qualquer comportamento ilegal, aético ou não autorizado envolvendo processamento automático de dados e, ou transmissão de dados”, podendo implicar a manipulação de dados ou informações, a falsificação de programas, a sabotagem eletrônica, a espionagem virtual, a pirataria de programas, o acesso e/ou o uso não autorizado de computadores e redes. (ARAS, 2001).

Não é demais anotar que o cibercrime é o fato típico no direito interno, ou seja, previsto na legislação penal, cuja conduta exige o recurso aos sistemas eletrônicos e às novas tecnologias de informação.

Sob o ângulo da criminalidade informática, a atividade delituosa pode ser considerada como toda conduta ilícita, omissiva ou comissiva, em que o computador serve de meio para atingir um objetivo criminoso, ou em que o computador é alvo da conduta. Assim, constitui crime de informática qualquer atividade não autorizada com o fim de obter a cópia, o uso, a transferência, a interferência, o acesso ou a manipulação de sistemas de computador, de dados ou de programas de computador.

4.1 CLASSIFICAÇÃO DO CIBERCRIME

Os crimes informáticos são, preponderantemente, os crimes comuns cometidos com o auxílio de um computador. Contudo, existem crimes específicos que só ocorrem num sistema informático.

A sistematização de uma classificação dos delitos informáticos parte dos primeiros estudos dos países precursores do desenvolvimento tecnológico, ou seja, os países mais ricos e tecnológicos do mundo. Entretanto, no Brasil, já foram iniciadas algumas pesquisas interdisciplinares e literatura jurídica a respeito do tema.

As classificações, segundos os múltiplos enfoques interdisciplinares, se revelam úteis diante da necessidade de um tratamento jurídico adequado e alinhado com a filosofia de liberdade do mundo cibernético e a concepção de que a intervenção penal deve guardar estreita congruência com o Princípio do Direito Penal Mínimo.

Além da classificação, é necessário que se busque individualizar as espécies de delitos de informática, assim instrumentalizar-se-ia o aprofundamento do objeto

jurídico a ser protegido, bem como a aplicação da norma adequada e a pena adequada ao delito.

Baseado na classificação de Ulrich Sieber (1986), Lima (2011) enuncia uma classificação geral, tomando o bem jurídico atingido, com a seguinte divisão:

- 1) crimes econômicos;
- 2) ofensas contra direitos individuais e
- 3) ofensas contra interesses supraindividuais.

Na primeira categoria, estariam os ilícitos praticados contra os sistemas de processamento de dados com o propósito de obter proveito econômico. Ex.: invasão de sistemas, furto de tempo¹⁶, espionagem informática. Na segunda classificação, estariam a invasão de dados pessoais para manipulação, destruição ou divulgação, enquanto que, na terceira classificação, temos como exemplo a manipulação de dados das instituições públicas, afetando a interesses coletivos. (LIMA, 2011, pp. 16-19).

Merece nota a classificação apresentada por Vianna (2003, pp.13-26):

- a) crimes informáticos impróprios: aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados), como por exemplo, os crimes contra a honra (calúnia, injúria e difamação), praticados nas redes sociais ou através do envio de um e-mail.
- b) crimes informáticos próprios são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados). Ex. a interceptação telemática ilegal, prevista no art. 10 da lei 9.296/96.
- c) delitos informáticos mistos: são crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa.
- d) crimes informáticos mediatos ou indiretos: é o delito-fim não informático que herdou esta característica do delito-meio informático realizado para possibilitar a sua consumação.

Outra classificação, citada por Ferreira (2010), parte do objeto material dos crimes de informática, categorizando-os de puro, misto e comum. Identifica-se um crime informático puro quando a conduta ilícita do delinquente atinge o sistema de informática da vítima, seus programas e/ou a parte física dos computadores. No “misto”, o objetivo da conduta não é diretamente o sistema ou dados, mas o infrator tem que, essencialmente, utilizar a informática para alcançar seu objetivo, por exemplo, no estelionato através de cartões de crédito em transações comerciais

¹⁶ Furto de tempo: “utilização indevida de instalações de computadores por empregados desleais ou de estranhos.” (CRESPO, 2009).

pela internet. Na modalidade “comum”, é aquele delito já previsto na legislação penal, e que foi realizado através da informática, porém não necessariamente necessita da informática para alcançar seu resultado. (FERREIRA, 2010, pp. 102-104).

Para Crespo (2011, p. 63), a melhor classificação, apesar de não ser a mais técnica, é a adotada por Ivete Senise Ferreira (2000) e Vicente Greco Filho (2000), por ser mais objetiva e possível de enquadrar as condutas ilícitas mais modernas: (a) condutas perpetradas contra um sistema informático e (b) condutas perpetradas contra outros bens jurídicos.

Essas classificações são importantes do ponto de vista científico e dos estudos criminológicos, na busca de um tratamento jurídico adequado aos infratores, bem como na compreensão do fenômeno do crescimento da criminalidade informática.

Alguns países regulam, especificamente, os crimes cibernéticos no sentido próprio ou puro, a exemplo da Alemanha, Austrália, Canadá, Espanha, Estados Unidos, Holanda, Itália, quase todos os Estados sul-americanos, dentre os quais Argentina, Brasil, Chile e Venezuela.

Embora cada país tenha liberdade dentro de sua soberania para definir as condutas típicas de crimes de informática, a sincronia e as semelhanças na definição das condutas ilícitas contribuem para a questão da persecução penal. Este é o espírito da Convenção de Budapeste sobre o Cibercrime, tanto que, em seu Preâmbulo, consita os países membros e possíveis signatários a estudar os mecanismos penais mais eficazes, tornando o ordenamento jurídico mundial mais harmônico quanto a esses ilícitos, evitando que um Estado trate mais benevolamente um delito, que outro.

São conhecidas várias condutas consideradas antiéticas ou ilícitas, já consideradas crimes em muitos países do mundo, como as condutas descritas na Convenção de Budapeste, praticadas contra confiabilidade, integridade e disponibilidade de um sistema e dados informáticos, além das condutas há muito previstas na legislação penal, que utilizam os meios informáticos para prática delituosa.

A título enunciativo, citam-se os crimes informáticos de acesso não autorizado a sistema informatizado protegido por restrição (senhas), tais como: obtenção, transferência ou fornecimento não autorizado de dado ou informação; divulgação,

utilização, comercialização e disponibilização de dados e de informações pessoais contidas em sistema informatizado; destruição, inutilização, deterioração de dado eletrônico alheio; inserção ou difusão de código malicioso ou vírus em sistema informatizado; estelionato eletrônico (difundir código malicioso para facilitar ou permitir acesso indevido a sistema informatizado); atentado contra a segurança ou o funcionamento de serviço de água, luz, força, calor, informação, telecomunicação ou outro serviço de utilidade pública; interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou sistemas informatizados; falsificação total ou parcial de dado eletrônico ou documento público ou particular.

O Brasil vem, gradativamente, introduzindo em nosso ordenamento jurídico, tipos penais de crimes de informática, o que será objeto de abordagem nos próximos capítulos.

4.2 ESPECIFICIDADES DO CIBERCRIME

Os benefícios da internet são indiscutíveis. O trânsito de informações e transações através da *web* confere aos internautas grande comodidade nas cidades com problemas de mobilidade ou num lugar longínquo do planeta desde que conectada à internet. Quem está conectado tem a sensação de inteiração e compartilhamento com amigos, família e trabalho. Realmente, hoje, a internet é um instrumento tanto de trabalho quanto de lazer.

Como já pontuado, ao lado dos benefícios da internet, o cibercrime apresenta seu lado nefasto, já que, como todo fenômeno humano, não há nada imune às ações perniciosas do delinquente, seus ataques constituem os riscos inerentes às tecnologias da informação.

Do mesmo modo que a rede mundial de computadores se espalhou pelo globo terrestre, a criminalidade informática absorveu as características da transnacionalidade, universalidade e ubiquidade, considerando que a prática de delitos cibernéticos pode ocorrer em qualquer país, em qualquer lugar que utilize sistemas e redes computacionais, sejam públicos ou privados.

Dentro das peculiaridades da cibercultura, a criminalidade virtual apresenta certas características que a diferenciam dos delinquentes comuns, tais quais eram

identificados na época em que não havia o uso ostensivo de computadores. Contudo, é de fácil percepção que os valores econômicos circulantes pela rede mundial de computadores são astronômicos, o que atrai cada vez mais a criminalidade comum, na expectativa de ganhos expressivos e com maior impunidade.

Diante da alta tecnologia e dos recursos circulantes, as relações através da internet apresentam várias características, dentre as quais a instantaneidade, superando as barreiras de tempo e espaço; a aparente igualdade dos internautas, ressalvadas as condições pessoais quanto aos conhecimentos tecnológicos pessoais; a infinidade e diversidade de informações em texto, sons, imagens, isoladamente ou em um mesmo documento (hipertexto) e a sensação de anonimato. (FURLANETO NETO; SANTOS; GIMENES, 2012, p. 13).

Os ilícitos cibernéticos podem ser realizados na privacidade das residências, dos escritórios ou, sem muita dificuldade, em qualquer lugar em que se possa ter acesso à rede mundial de computadores. A respeito da característica do anonimato, Vera Elisa Marques Dias, em sua dissertação de mestrado na Universidade de Lisboa, afirma que:

Inegavelmente, o anonimato, a camuflagem ou o uso de identidade falsa é a característica mais aliciadora, tentadora e propulsora para a iniciação da prática criminosa na internet. É, também, a característica mais assegurada, recorrendo os infractores mais especializados ou as organizações através deles a técnicas que lhes permitam ocultar ou dissimular a sua identidade e as suas condutas, como a técnica de *spoofing*, programas de anonimização e codificação, que diariamente são aperfeiçoados e transformados. Para além de se assegurar o anonimato do autor também se pode ocultar a própria informação através de mecanismos de cifra forte ou de encriptação, como a estenografia, e outros disponíveis gratuitamente na rede⁶⁵. Podem, assim, os cibercriminosos diminuir ou eliminar o risco de ser descoberto ou condenado, apagando todas as provas do ciberrastro. (DIAS, 2010, p. 16).

São, também, características importantes dos delitos virtuais, além da transnacionalidade, a deslocalização, a *a-temporalidade*, a permanência, o automatismo, a repetição, o anonimato, a alta tecnologia, a disseminação e a potenciação de danos. (DIAS, 2010, pp. 13-17).

Facilidades advindas do âmbito da internet proporcionam práticas criminosas em virtude da possibilidade de reiteração delitiva, conjugada ao sentimento de anonimato. Tais fatores contribuem para a migração da criminalidade comum, que utilizava os métodos tradicionais, e de outras pessoas que, normalmente, não se

envolveriam com práticas criminosas pelos métodos tradicionais, sobretudo, pela alta possibilidade de anonimato e facilidades de cometimento desses ilícitos nos refúgios privados de suas casas, escritórios, ou por rede sem fio (*Wi-Fi*), smartphones, dentre outros meios tecnológicos.

Influencia, também, de forma importante, na problemática da crescente cibercriminalidade, a insuficiência de conhecimentos a respeito da alta tecnologia, na maioria das vezes, não compreendida pela grande massa dos internautas, o que configura a vulnerabilidade dos usuários que operam o acesso à internet, sem qualquer educação preventiva quanto aos riscos da *web*.

O desconhecimento a respeito do caráter automático, veloz, repetitivo e instantâneo das ações criminosas, amplia sobremaneira o sucesso da ação criminosa, sem contar que as novas tecnologias voltadas para o cometimento de fraudes e outros ilícitos são rapidamente atualizadas com o auxílio de programas especializados, altamente sofisticados em camuflar a atuação dos criminosos, dificultando a investigação quanto à identificação dos autores e prova da materialidade delitiva.

Os delinquentes são tão velozes que, ao perceber que estão sendo investigados, apagam qualquer vestígio, camuflando os resultados econômicos ou de qualquer natureza, dificultando a ação investigativa das autoridades públicas.

Assim, o fenômeno da criminalidade informática torna-se mais preocupante em decorrência da vulnerabilidade potencial de todos os usuários frente à alta tecnologia, dentre as quais a técnica “deslocalização” no ambiente da internet de conteúdos, de um servidor para outro, principalmente para um servidor de conteúdo localizado num país em que a sua conduta não seja tipificada como crime ou que não exista legislação que preveja ou sejam insuficientes os instrumentos de investigação criminal, favorecendo a impunidade do delinquentes cibernéticos. Esses servidores são chamados “servidores *off-shore*,” “zonas francas” ou “paraísos cibernéticos”. (DIAS, 2010).

Segundo a pesquisadora portuguesa Vera Elisa Marques Dias, o caráter transfronteiriço, ou extraterritorialidade da internet, aponta a dimensão planetária da rede. O mundo virtual global, onde o utilizador das redes informáticas consegue aliar a quantidade à velocidade, com enormes transferências de dados e informação, por todo o globo, à velocidade de segundos, possibilita ao delinquente, no conforto do seu lar, atingir qualquer pessoa em qualquer país, citando, como exemplo, a

hipótese de um pedófilo em Portugal poder vender imagens pornográficas de menores, através de um servidor americano, a todos os países com acesso à internet, porque a “distância continental entre pessoas, dados e serviços, reduz-se a um simples clique.” (DIAS, 2010).

Vale destacar outra peculiaridade relativa à possibilidade da prática ilícita a distância, com hora marcada, por controle remoto, o que confere o caráter “a-temporal”, com a possibilidade de interrupção ou anulação da prática delitiva antes da materialização do resultado. (DIAS, 2010).

Estas peculiaridades levam ao exponencial agravamento dos danos resultantes das condutas criminosas, com potencial risco de massivamente vitimar internautas incautos em qualquer localidade.

Outra questão tormentosa consiste em saber o lugar e em definir onde ocorreu a consumação do delito cometido por meio da rede mundial de computadores. Pelo princípio da territorialidade, aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional. O direito penal brasileiro adota a teoria da ubiquidade (mista ou da unidade), considerando lugar do crime aquele onde ocorreu a ação ou omissão, no todo ou em parte, e aquele onde se produziu ou deveria produzir-se o resultado. No crime, por exemplo, de publicação de pornografia envolvendo criança e adolescente, previsto no art. 241 do Estatuto da Criança e do Adolescente, as imagens pedófilo-pornográficas são acessíveis em qualquer local do mundo em que se disponha de um computador conectado à internet.

Em consequência, a discussão sobre a competência territorial é uma questão ligada à soberania e às leis de cada país, tornando-se, muitas vezes, severamente espinhosa, sobretudo quando as soberanias envolvidas não possuem tratado ou acordo de cooperação de prevenção e repressão ao cibercrime.

Internamente, no Brasil, a questão não é menos controvertida. A competência territorial é definida pelo art. 70 do Código de Processo Penal, estabelecendo que, em regra, a competência será determinada pelo lugar da consumação do delito.

É justamente a diversidade de locais onde seja possível acessar esse conteúdo ilícito que gera a dificuldade de se identificar o local da consumação do delito, ao tempo em que revela uma legislação processual penal desatualizada frente às inovações tecnológicas, tornando a referida regra geral de fixação de competência, prevista no art. 70 do Código de Processo Penal, insatisfatória para

fixar a competência nas hipóteses de multiplicidade da localidade onde o ilícito pode ser considerado consumado.

Grande parcela de cibercriminosos, nas hipóteses de crimes à distância, nos quais, o lugar onde o agente cometeu o crime é diferente do lugar onde o resultado é produzido, escapa do poder punitivo estatal em decorrência do princípio da territorialidade.

O princípio da territorialidade não atende mais às peculiaridades de muitas das novas práticas delitivas que surgiram com a disseminação do uso da internet, recebendo da doutrina especializada críticas aguçadas ante a desatualização da legislação que inibe ou anula a persecução penal dos delitos à distância, culminado com a frustração da persecução, deixando à própria sorte as vítimas da criminalidade cibernética. (FERREIRA, 2010).

No entanto, esta questão da necessidade de se repensar e redefinir o princípio da territorialidade pode ser vista como uma consequência da mundialização ou globalização, consoante adverte Octávio Iunni (2000), conquanto a sociedade nacional, ao adotar o projeto de capitalismo transnacional, desenvolve não só a “transnacionalização” mas, também, “a alienação de centros decisórios”, impossibilitando-se de “colocar em prática qualquer projeto nacional que dependa da vigência efetiva do princípio jurídico-político da soberania nacional”. Nesta perspectiva, afirma que

este é um fato novo e fundamental, com diversas e profundas implicações nas relações Estado e Sociedade civil: o novo ciclo de globalização do capitalismo solapa as bases econômicas e políticas da soberania e atinge inclusive as suas bases sociais e culturais. A soberania, como instituto jurídico-político nuclear do Estado-nação perde vigência, ou trans-forma-se em uma ficção da retórica política e dos ordenamentos jurídicos, mas sem condições de vigência efetiva na definição de algum projeto nacional, na formulação de diretrizes político-econômicas e sócio-culturais relativas ao nacional; no estabelecimento das condições e possibilidades de tradução das inquietações e reivindicações de setores sociais subalternos em compromissos e diretrizes de governo, das políticas que se adotam no âmbito do poder estatal. É tal a envergadura da transformação qualitativa do Estado-nação, devido às injunções do globalismo, que os governantes já não conseguem mais se apresentar como estadistas; parecem muito mais funcionários dóceis traduzindo para a língua “nativa” o que se dita no idioma das corporações transnacionais e das organizações multilaterais; sendo que alguns parecem figurações de um teatro mundial de títeres. (IANNI, 2000, p. 6).

Todas essas questões políticas e jurídicas aliadas ao conjunto das peculiaridades do cibercrime dificultam e, às vezes, impossibilitam a investigação

necessária à obtenção da prova da materialidade delitiva. Aliás, não é apenas a dificuldade de identificação e localização do criminoso, mas também das vítimas, somadas às questões ligadas ao ineditismo de alguns delitos perante a legislação, à transnacionalidade, dentre outros problemas. Enfim, a persecução e a prevenção são atividades extremamente complexas, de difícil execução.

4.3 CIBERCRIME NA LEGISLAÇÃO PENAL BRASILEIRA

Em decorrência do princípio da legalidade ou da anterioridade da lei penal, a insuficiência ou a ausência de norma penal tipificando os crimes digitais limita a função punitiva estatal, possível fator que influencia na sensação de insegurança e impunidade, com repercussão negativa para a sociedade brasileira e, em especial, para a comunidade internacional, que há mais de uma década vem chamando a atenção para a necessidade e urgência de controle e prevenção de condutas delituosas no ciberespaço.

O mundo cibernético tornou-se um âmbito no qual o ordenamento jurídico brasileiro ainda se surpreende com situações para as quais não há precedentes, eis que padece de lacunas nesta seara, muito embora, nos últimos dois anos, o Congresso Nacional tenha editado duas importantes leis que tratam de cibercrime, as Leis n.º 12.735 e 12.737, de 30 de novembro de 2012, e, recentemente, a disposição normativa que regula as relações civis na internet, Lei n.º 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, conhecida como Marco Civil da Internet.

Embora o Brasil tenha alcançado um bom desenvolvimento na área tecnológica e das telecomunicações, com franca expansão para a utilização de tecnologia que permite a utilização da internet, cada vez mais rápida, o que significa o aumento e sofisticação de condutas delitivas, a questão do cibercrime, não obstante a relevância, não tem sido objeto de intensas discussões, ao contrário dos países que dispõem de tecnologia avançada que, desde o início dos anos 90, vem desenvolvendo todo um arcabouço jurídico e meios tecnológicos com vistas à adoção de políticas de controle da criminalidade virtual.

No contexto da realidade brasileira, diante da constatação inarredável de que a criminalidade cibernética cresce na mesma proporção das novas tecnologias digitais, a ausência de uma legislação penal específica, para tratar das novas condutas ilícitas praticadas no ambiente virtual, constitui um privilegiado elemento catalisador e estimulador da prática de ilícitos que, em última instância, atinge o direito fundamental à segurança, compromete o papel estatal da prevenção e da persecução penal e, enfim, conduz ao descontrole e à impunidade.

Nesta perspectiva, não parece razoável que o Brasil, um Estado Democrático de Direito,¹⁷ fique omissos ou lenientes frente ao fenômeno do cibercrime e da criminalidade virtual, ante a magnitude do alcance das ações danosas, bem como da ameaça aos bens e interesses das pessoas e instituições usuárias das novas tecnologias informáticas.

Não obstante, o princípio da legalidade previsto no art. 5.º, XXXIX, da Constituição Federal enuncia que “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”. Este princípio constitucional, corresponde ao art. 1.º do Código Penal, de quase idêntica redação, contém dois princípios distintos: o da reserva legal e o da anterioridade. De tal modo, respectivamente, somente a lei em sentido estrito pode criminalizar uma conduta (reserva legal), ao tempo em que, a lei penal deve ser anterior ao fato pretende incriminar (princípio da anterioridade).

Na esfera infraconstitucional, os princípios da reserva legal e da anterioridade regem todo arcabouço penal e fundamentam os pilares sobre os quais está acentuado o poder punitivo do Estado brasileiro, tanto no aspecto da positivação da conduta incriminadora, quanto proibindo e limitando o poder punitivo, se não há previsão legal. Em consequência, no tocante ao cibercrime, e da complexidade do fenômeno da criminalidade cibernética, o poder punitivo do Estado afigura-se tímido nas diversas questões ligadas à segurança digital, à proteção dos direitos de privacidade, informação, tutela aos bens jurídicos afetados pela delinquência cibernética, espalhada de forma difusa pelos mais diversos cantos do mundo conectados pela *World Wide Web* - (WWW), ou simplesmente “Web”, que, a cada dia, surpreende com novas condutas ilícitas na mesma medida que novidades tecnológicas afloram.

¹⁷ Constituição da República Federativa do Brasil: “Art. 1.º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: [...]”.

Há que se considerar, ainda, que a criminalidade cibernética é formada predominantemente por jovens e, de acordo com as infrações que cometem, é preciso distinguir se são apenas jovens aventureiros e curiosos que praticam ações antiéticas, ou internautas que, eventualmente, praticam um delito, ou se são daqueles que fazem dos delitos informáticos uma prática diária para obter vantagens ilícitas.

O princípio da legalidade, de gênese liberal, permaneceu hígido na atual fase do Estado Constitucional de Direto, tendo a Constituição Federal de 1988, em seu art. 5º, XXXIX, expressamente consignado, como corolário do direito de igualdade e liberdade para todos os cidadãos e estrangeiros residentes no País, que não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal, sintetizado no postulado do *nullum crimen, nulla poena sine praevia lege*, também aplicável aos crimes informáticos. E é indispensável à segurança jurídica e à garantia de liberdade, com escopo de impedir que alguém seja condenado por um comportamento que não era considerado delituoso à época de sua prática, evitando a aplicação de penas arbitrárias e sem prévios limites.

O Supremo Tribunal Federal firmou entendimento negando a pretensão de se preencher, por analogia, uma lacuna da lei penal. Numa decisão paradigmática, o Supremo Tribunal Federal teve o seguinte posicionamento, conforme Informativo 453/2006, divulgado no sítio do STF:

Em conclusão de julgamento, o Tribunal, por maioria, rejeitou denúncia apresentada contra Deputado Federal, em razão de ter despendido quantia em dinheiro na tentativa de obter, por intermédio de cola eletrônica, a aprovação de sua filha e amigos dela no vestibular de Universidade Federal, conduta essa tipificada pelo Ministério Público Federal como crime de estelionato (CP, art. 171), e posteriormente alterada para falsidade ideológica (CP, art. 299) — v. Informativos 306, 395 e 448. Entendeu-se que o fato narrado não constituiria crime ante a ausência das elementares objetivas do tipo, porquanto, na espécie, a fraude não estaria na veracidade do conteúdo do documento, mas sim na utilização de terceiros na formulação das respostas aos quesitos. Salientou-se, ainda, que, apesar de seu grau de reprovação social, tal conduta não se enquadraria nos tipos penais em vigor, em face do princípio da reserva legal e da proibição de aplicação da analogia in malam partem. (Informativo STF n. 453/2006).¹⁸

¹⁸ “Vencidos os Ministros Carlos Britto, Ricardo Lewandowski, Joaquim Barbosa e Marco Aurélio, que recebiam a denúncia. Inq 1145/PB, rel. orig. Min. Maurício Corrêa, rel. p/ o acórdão Min. Gilmar Mendes, 19.12.2006. (Inq-1145)”. Disponível em: <<http://www.stf.jus.br/arquivo/informativo/documento/informativo453.htm>>.

A doutrina também vinha mantendo o entendimento, segundo o qual a grande maioria dos crimes praticados por meio da internet já está tipificada no Código Penal, o que autoriza a persecução e a punição dos responsáveis pela prática criminosa.

Entretanto, no que se refere às condutas ilícitas, relativas aos crimes puramente informáticos, a inexistência de lei penal incriminadora impossibilita o poder punitivo estatal, por contrariar princípio constitucional da reserva legal, previsto no art. 5º, XXXIX, da Constituição Federal.

O princípio penal da legalidade traz ínsito a limitação e a taxatividade, o que significa dizer que as leis que tipificam condutas como crime devem ser claras e precisas quanto à delimitação da conduta que pretende incriminar, não sendo permitidas leis vagas ou imprecisas, os chamados tipos penais abertos. (DELMANTO, 2002, p. 4).

Do mesmo modo, constitui corolário da legalidade a proibição de julgamento com emprego da analogia ou da interpretação com efeitos extensivos para incriminação, ou, ainda, exasperar a pena, vedando-se pelos princípios gerais que regem o direito penal a aplicação da analogia jurídica, ou a analogia *in malam partem*, ou seja, nas hipóteses em que prejudica o réu. A propósito, Mirabete (2005, p.115) afirma que a “tipicidade é a correspondência exata, a adequação perfeita entre o fato natural concreto e a descrição contida na lei”. Assim, para efeito do controle repressivo, é requisito de validade dos atos de persecução a da tipicidade penal, e somente esta autoriza punir os crimes puramente informáticos.

Como já mencionado, no Brasil, as questões ligadas à repressão do cibercrime vêm sendo alvo de discussões, um tanto atrasadas em relações aos países da Europa Ocidental, Estados Unidos da América, Canadá, China e Coreia. De qualquer modo, o tema tornou-se objeto de estudos de muitos grupos interessados e do Poder Legislativo, que, recentemente, editou duas leis e ainda conta com alguns projetos em tramitação que têm como objeto a criminalização de condutas ilícitas no âmbito do ciberespaço e em sistemas computadorizados.

Gradativamente, foram introduzidas no Código Penal Brasileiro e em leis esparsas dispositivos que incriminam algumas práticas ilícitas através de tecnologias informáticas e internet. Crespo (2009) destaca as seguintes disposições:

- a) Art. 153, §1º-A – Divulgação de segredo – que incrimina a conduta de quem divulga informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informação ou banco de dados da Administração Pública;
- b) Art. 313-A – Inserção de dados falsos em sistema de informação – que incrimina a inserção ou facilitação da inserção de dados falsos ou modificação de dados verdadeiros em sistemas de informação da Administração Pública, com o fim de obter vantagem indevida para si ou para outrem, ou para causar dano;
- c) Art. 313-B – Modificação não autorizada de sistema de informação – que tipifica a conduta do funcionário que altera sistema de informação ou programa de informática sem autorização;
- d) Art. 325, I – Violação de sigilo profissional – que prevê o ilícito de facilitar ou permitir o empréstimo ou uso de senha para acesso de pessoas não autorizadas a sistemas de informação da Administração Pública;
- e) Lei 8069/90, arts. 241 a 241-E – que incriminam condutas como as de armazenar fotos com pornografia infantil, garantir o acesso a tais fotos, trocar, possuir, armazenar, adquirir, fotos igualmente pornográfico-infantis, entre outras condutas.
- f) Lei 8137/90, art. 2º, V – que proíbe utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública;
- g) Lei 9296/96, art. 10 – Interceptação não autorizada – que tipifica realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.
- h) Lei 9504/97, art. 72 – que incrimina o acesso não autorizado a sistemas da justiça eleitoral bem como a criação e inserção de vírus computacional nos sistemas de apuração e contagem de votos, ambos com o intuito de alterar o resultado do pleito.

É oportuno fazer referência à Lei 9.609, de 19 de fevereiro de 1998, conhecida como Lei do Software, que dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, criando na disposição prevista no art. 12 o crime de violação de direitos de autor de programa de computador.

A seguir enfocaremos os principais aspectos dos novos diplomas legais, no caso a Lei n.º 12.735 e a Lei n.º 12.737, ambas de 30 de novembro de 2012, que introduzem no ordenamento penal os crimes informáticos.

4.3.1 Crimes Informáticos: Leis n.º 12.735 e n.º 12.737/2012

No decorrer de duas décadas, tramitaram no Congresso Nacional vários projetos com a finalidade de criminalizar delitos digitais. O Projeto de Lei n.º 84, de

1999, proposto pelo deputado Luiz Piauhyllino, que também ficou conhecido como “Lei Azeredo”, resultou de um projeto de 1996, desarquivado e alterado. Interessante pontuar que a redação inicial do PL 84/99 apresentava problemas com relação à sua abrangência e imprecisão, o que levou a acalorados debates e às suas sucessivas alterações por substitutivos.

Segundo o Relatório de Políticas da Internet do CGI – Comitê Gestor da Internet no Brasil¹⁹, o que diferenciou esse PL 84/99 dos demais foi a grande mobilização popular ao seu redor, conjugado com a excessiva criminalização de “condutas tidas como cotidianas, banais ou indispensáveis à inovação na rede”, com posterior aceleração em seu processo de tramitação, impulsionado, especialmente, pela bandeira do combate à pedofilia e à pornografia infantil.

Segundo o referido Relatório, o projeto apresentava diversos problemas em sua redação, contendo incongruências que iam além de criminalizar condutas graves no âmbito da rede, continha previsão de disposições que extrapolavam a intenção de criminalizar, criava obrigações de vigilância por parte dos provedores de acesso e de conteúdo, além de obrigações de disponibilização de dados independentemente de ordem judicial, com clara ameaça à garantia de direitos fundamentais dos usuários, no que tange aos direitos à privacidade e ao devido processo legal, ampliando demasiadamente os poderes de investigação da polícia. Nesse contexto, afirma o Relatório de Políticas da Internet do CGI – Comitê Gestor da Internet no Brasil, elaborado em 2012, em seu primeiro capítulo, intitulado *Crimes na Internet: o Projeto de Lei n.º 84/99*:

As críticas feitas ao PL 84/99 apontaram ainda que, considerando o contexto atual da legislação nacional e a redação do projeto, sua aprovação traria riscos consideráveis ao desenvolvimento pleno da Internet no Brasil. Esses riscos se traduzem tanto em um desincentivo à existência de um ambiente propício à inovação, no qual os agentes empreendedores contam com previsibilidade jurídica e lidam com regras civis claras e preestabelecidas, como também por representar uma ameaça à garantia de direitos fundamentais dos usuários, fato que levou alguns ativistas a denominar o projeto como “AI-5 Digital”, em referência ao decreto da época da ditadura militar que suspendeu as garantias constitucionais. [...] Adicionalmente, a redação fruto de má técnica legislativa, criminalizava o acesso não autorizado a um sistema informatizado – tipo que por si inviabilizaria a engenharia reversa, que é fundamental ao processo de aprendizado e de inovação tecnológica (art. 285-A). De modo geral, ainda que fosse importante coibir a prática de crimes como a pedofilia, disseminação de vírus, dentre outras práticas aviltantes no âmbito da rede mundial de computadores, a redação do PL 84/99 apresentava problemas

¹⁹ Disponível em: <www.cgi.br/media/docs/publicacoes/1/relatorio-politicas-internet-pt.pdf>.

com relação à sua abrangência e imprecisão, que podiam gerar efeitos colaterais graves. (p. 17)

Com significativa participação popular nas discussões sobre a regulação da internet brasileira, formando uma “rede de ativismo digital”, ocorreram audiências públicas, em novembro de 2011, inclusive com intervenções através do *Twitter*.

Com o Projeto de Lei 2.793/2011, do deputado Paulo Teixeira, do Partido dos Trabalhadores, foram incorporadas sugestões elaboradas pelo Centro de Tecnologia e Sociedade da FGV Direito Rio²⁰, cujo estudo sobre tipificação criminal de delitos informáticos, partia da ideia de criminalizar o mínimo necessário para coibir práticas graves cometidas através da internet e, assim, deixar outras matérias relativas à liberdade da rede e direitos dos usuários para outro projeto da regulação da rede, o Marco Civil da Internet, que ainda estava em tramitação. (Relatório..., 2012, p. 18).

Seguindo a concepção de que as normas penais constituem a *ultima ratio*, devendo ser criadas apenas quando as regras civis se mostrarem insuficientes, o PL 2.793/2011 tentou restringir, ao mínimo necessário, a criação de novos crimes, circunscrevendo essas tipificações às condutas absolutamente indispensáveis, e, ainda, com a redução das penas de cada crime.

Tal postura reducionista vem de encontro ao princípio da subsidiariedade da norma penal, do minimalismo penal. Segundo Raúl Zaffaroni, o princípio do direito penal mínimo nega a legitimidade dos sistemas penais atuais e propõe alternativa mínima que a considera como mal menor necessário e indispensável para evitar males piores em uma sociedade igualitária. (ZAFFARONI, 1991).

Com a inserção destes novos diplomas legais, o ordenamento jurídico nacional passa a contar com novas disposições penais destinadas a coibir as ações maléficas que impedem ou causam transtornos e prejuízos aos que usufruem dos avanços tecnológicos largamente utilizados pelos usuários da internet, no sentido de estabelecer regras claras quanto à lesividade de tais práticas ilícitas, com propósito de reduzir a cibercriminalidade.

Do ponto de vista da norma penal tipificadora de condutas delitivas, o legislador nacional, mesmo que de forma mais lenta que em outros países, vem, gradativamente, introduzindo no Código Penal Brasileiro novos dispositivos

²⁰ Disponível em: <<http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/7719/coment%C3%A1rios%20ao%20substitutivo%20PL%2088-99.pdf?sequence=1>>. Acesso em: 14 jun. 2014.

tipificando como crime informático algumas práticas ilícitas que ocorrem no ciberespaço e sistemas computadorizados. Finalmente, após mais de 12 anos de tramitação, foram sancionadas as Leis n.º 12.735 e n.º 12.737, ambas de 30 de novembro de 2012 e com *vacatio legis* de 120 dias.

Os referidos diplomas legislativos têm a finalidade de suprir a omissão normativa a que a doutrina e jurisprudência nacional se referiam quando se travava o debate sobre a inaplicabilidade da analogia para a condenação de um acusado de cometer crime através de computador ou das novas tecnologias informáticas, subsumindo esta conduta num dos tipos previstos no Código Penal.

A Lei n.º 12.735/2012, denominada “Lei Azeredo”, inicialmente, trazia proposições para caracterizar crimes informáticos os ataques praticados por *hackers* e *crackers*, como as alterações de *home pages* e a utilização indevida de senhas mediante uso de sistema eletrônico, digital ou similares, contra sistemas informatizados e teve quase todas as suas disposições vetadas, permanecendo, apenas, dois artigos.

A primeira disposição aprovada, prevista no art. 4º, determina aos órgãos da polícia judiciária estruturar setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. Ou seja, o comando normativo é no sentido de que a polícia judiciária crie e estruture delegacias especializadas, ou setores e equipes específicos para o combate e investigação de condutas ilícitas relacionadas aos sistemas informatizados.

A segunda disposição da Lei n.º 12.735/2012, aprovada, diz respeito a cessação imediata das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio, na hipótese de ocorrer induzimento ou incitação à discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.

A tipificação de delitos digitais ficou a cargo da Lei n.º 12.735/2012, que introduziu no Decreto-Lei n.º 2.848, de 7 de dezembro de 1940 – Código Penal, os chamados “delitos informáticos”, acrescentando os artigos 154-A e 154-B, positivando um novo tipo penal denominado de “Invasão de dispositivo informático”. Outrossim, através do acréscimo do § 1º ao art. 266, criminalizou-se a conduta de interromper “serviço telemático ou de informação de utilidade pública”, e inseriu o parágrafo único ao art. 298 do Código Penal, estabelecendo que configura também

o crime de falsidade de documento particular (art. 298), a conduta de falsificar ou alterar cartão de crédito ou de débito.

A referida Lei n.º 12.737/2012 ficou conhecida como Lei Carolina Dieckmann, em decorrência do episódio da divulgação de imagens em *sites* de pornografia, após *hackes* terem invadido os arquivos e acessado, indevidamente, os dados da vítima, atriz brasileira, que se recusou à chantagem de despendar quantia em dinheiro para que suas fotografias em poses íntimas não fossem ilicitamente divulgadas.

Este episódio, segundo a imprensa nacional²¹, acelerou a tramitação do PL 2.793/2011, de autoria do Deputado Paulo Teixeira, de São Paulo, com previsão de alguns tipos de delitos cibernéticos, levando a Câmara dos Deputados a aprovar o projeto em regime de urgência. No entanto, a matéria, objeto do processo legislativo, vinha sendo exaustivamente debatida, com várias alterações das proposições originais, por isso, não se justifica o apelido conferido pela imprensa a esse diploma legal, com o nome da famosa atriz, embora, lamentavelmente, vítima do covarde ataque cibernético. Aos menos desavisados cidadãos que não acompanharam o desenrolar da longa e tormentosa tramitação dos projetos perpassa a impressão que a referida lei é casuística e elaborada, açodadamente, sem a necessária discussão.

Este diploma normativo, a Lei n.º 12.737/2012, dispõe sobre a tipificação criminal de delitos informáticos, em explícita pretensão de atualização da legislação penal codificada, evitando introduzir no ordenamento jurídico nacional, mais uma lei penal esparsa, contribuindo, desse modo, para a sistematização e a unificação das disposições que criminalizam tais condutas, otimizando a compreensão do cidadão comum, no que tange ao caráter pedagógico da legislação repressiva criminal, e ainda, do trabalho hermenêutico e aplicação pelo Poder Judiciário.

4.3.1.1 Invasão de dispositivo informático

O tipo penal de “Invasão de Dispositivo Informático”, previsto no art. 154-A do Código Penal, introduzido pelo art. 2º da Lei 12.737, de 30 de novembro de 2012, descreve como conduta ilícita:

²¹ Disponível em: <<http://veja.abril.com.br/noticia/brasil/roubo-de-fotos-de-carolina-dieckmann-acelera-tramitacao-de-projeto-de-lei-sobre-crimes-ciberneticos>>. Acesso em: 30 maio 2014.

Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

A pena prevista para o crime na modalidade simples é de detenção de três meses a um ano e multa. Na forma qualificada na hipótese do § 2º, aumenta-se a pena de um sexto a um terço, se da invasão resulta prejuízo econômico.

Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão à terceiro, a qualquer título, dos dados ou informações obtidos. E, ainda, exaspera-se a pena de um terço à metade, se o crime for praticado contra Presidente da República, Governadores e Prefeitos; Presidente do Supremo Tribunal Federal; Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Este tipo penal foi inserido no capítulo que trata dos crimes contra a liberdade individual (artigos 146 a 154, CP), em sua Seção IV – Dos Crimes contra a inviolabilidade dos Segredos (artigos 153 a 154-B, CP), razão pela qual o bem jurídico tutelado é a liberdade individual, a privacidade e a intimidade das pessoas físicas e jurídicas, direitos esses já protegidos pelo inciso X do art. 5º da Constituição Federal.

Segundo Cabette (2013), para a configuração do crime simples de “Invasão de Dispositivo Informático”, é necessário, apenas, a invasão ou a instalação de vulnerabilidade, sendo que a obtenção de dados ou informações, ou mesmo destruição, adulteração ou vantagens ilícitas, constituem exaurimento do crime. Assim, a forma qualificada ocorre quando o agente conseguir obter, efetivamente, dados ou informações com a invasão ou vulneração.

O crime é formal tanto na conduta de invadir o sistema como de instalar vulnerabilidades, de modo que, eventual obtenção de dados ou informações, adulteração ou destruição, bem como a obtenção de vantagem ilícita, constituirão mero exaurimento. O crime se consuma com a simples invasão ou instalação de vulnerabilidades, por exemplo, quando se introduz código malicioso para a obtenção de senhas. Embora formal, o ilícito é plurissubsistente e, assim, admite tentativa, o

que ocorre quando iniciada a invasão de um sistema ou a instalação de vulnerabilidades, a ação não se consuma por motivos alheios à vontade do agente. (CABETTE, 2013).

O sujeito ativo é qualquer pessoa, física ou jurídica, incluindo as pessoas jurídicas de direito público ou privado, que tenham seus dados ou informações, sigilosas ou não, em computadores interligados em rede, ou à rede mundial de computadores. A conduta pode ocorrer por diversas razões: por mero prazer em superar desafios técnicos de segurança, por vontade de invadir a privacidade alheia, inclusive com acesso a informações sigilosas, ou, na hipótese mais grave, com intenção de manipular, defraudar, adulterar, sabotar e/ou devassar dados, ou por motivação econômico-financeira.

Na figura típica de invasão de dispositivo informático, o elemento subjetivo do ilícito é o dolo específico, sem previsão, a modalidade culposa. O dolo é específico e fica caracterizado quando a invasão tem o fim de “obter, adulterar ou destruir dados ou informações” ou “instalar vulnerabilidades para obter vantagem ilícita”. Qualquer das condutas é suficiente para a subsunção do tipo, mesmo que não seja obtida a vantagem ilícita ou adulteração ou destruição, basta que haja a invasão do dispositivo ou sistema informático.

Como dispositivo informático, pode ser entendido qualquer computador ou aparelho com capacidade de armazenar dados ou informações passíveis da violação prevista no tipo penal, como PC pessoal, de empresas ou institucionais, incluindo-se os dispositivos móveis como *notebooks*, *tablets*, celulares e *smartphones*, com recursos de informática e telemática, ligados ou não à internet, inclusive novos equipamentos ou aparelhos informáticos que venham a ser lançados no mercado.

Outra especificidade interessante que constitui elemento normativo do tipo é que o “dispositivo informático alheio” esteja protegido por com “mecanismo de segurança”, como antivírus, *firewall* e senhas, dentre outros mecanismos de proteção. Neste aspecto, Cabette (2013), assevera ser importante ressaltar que

não é qualquer dispositivo informático invadido que conta com a proteção legal. Para que haja o crime é necessário que o dispositivo conte com “mecanismo de segurança” (v.g. antivírus, “firewall”, senhas etc.). Assim sendo, o dispositivo informático desprovido de mecanismo de segurança não pode ser objeto material das condutas incriminadas, já que o crime exige que haja “violação indevida de mecanismo de segurança”. Dessa maneira, a

invasão ou instalação de vulnerabilidades em sistemas desprotegidos é fato atípico. [...] Sinceramente não se compreende essa desproteção legislativa exatamente aos mais desprotegidos. É como se o legislador considerasse não haver violação de domicílio se alguém invadissem uma casa que estivesse com as portas abertas e ali permanecesse sem a autorização do morador e mesmo contra a sua vontade expressa! Não parece justo nem racional presumir que quem não instala proteções em seu computador está permitindo tacitamente uma invasão, assim como deixar a porta ou o portão de casa abertos ou destrancados não significa de modo algum que se pretenda permitir a entrada de qualquer pessoa em sua moradia. A forma vinculada disposta no tipo penal (“mediante violação indevida de mecanismo de segurança”) poderia muito bem não ter sido utilizada pelo legislador que somente deveria chamar a atenção para a invasão ou instalação desautorizadas e/ou sem justa causa. Isso seria feito simplesmente com a locução “mediante violação indevida” sem necessidade de menção a mecanismos de segurança.

O tipo objetivo do crime previsto do artigo 154-A do Código Penal apresenta dois núcleos de conduta: invadir ou instalar, bastando apenas uma conduta e, ainda que ocorram as duas, o agente responde por crime único.

Na instalação de vulnerabilidades, o tipo subjetivo deve coincidir com o intuito de obtenção de vantagem, seja econômica, como a obtenção de senhas de contas bancárias, ou, simplesmente, para romper a segurança. Na figura equiparada prevista § 1º, art. 154-A, do Código Penal, o legislador incrimina com a mesma pena do *caput* a conduta do agente que “produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*”, exigindo dolo específico e concernente à vontade de praticar os comportamentos previstos no *caput* do art. 154-A.

Conforme previsão do art. 154-B, a ação penal é pública condicionada à representação, exigindo-se para desencadear a persecução penal a manifestação de vontade da vítima à autoridade competente. Porém, se o crime é cometido contra a administração pública direta ou indireta da União, Estados, Distrito Federal ou Municípios e contra empresas concessionárias de serviços públicos, a ação penal será pública incondicionada.

4.3.1.2 *Interrupção ou perturbação de serviço informático*

A Lei n.º 12.357/2012 alterou o art. 266 do Código Penal, acrescentando que constitui crime a interrupção de serviço telemático ou de informação de utilidade

pública, bem como impedir ou dificultar-lhe o restabelecimento, estipulando penas que variam de um a três anos de reclusão e multa, que são aplicadas em dobro em caso de calamidade pública. Trata-se da conduta ilícita agora criminalizada de ataque de denegação de serviço DOS/DDOS.

Por ser crime de forma livre, essa prática ilícita pode ser realizada de várias formas, tanto pode ocorrer pela destruição física de uma determinada rede, ou mediante um ataque virtual. Segundo Nota Técnica publicada no Portal do Ministério Público de São Paulo, através do Centro de Apoio Operacional Criminal, no Brasil, hoje

é crime a conduta denominada ataque de denegação de serviço (DOS/DDOS). O DOS (*denial of service*) não constitui geralmente uma invasão de sistema alvo, mas uma sobrecarga de acessos que fazem com que o fluxo de dados da rede seja interrompido. É chamado de ataque de denegação de serviço difundido ou DDOS (*distributed denial of service*) quando o criminoso infunde por meio de seu computador (mestre) vulnerabilidades ou programas maliciosos em vários computadores (zumbis), fazendo com que contra a vontade ou mesmo sem que os usuários afetados percebam, acessem simultaneamente ou sequencialmente o serviço que pretende ser travado.²²

De acordo com o glossário da Cartilha de Segurança para Internet do Comitê Gestor da Internet – CGI, a negação de serviço consiste na atividade maliciosa na qual o atacante utiliza um computador para tirar de operação um serviço ou um computador conectado à internet.

Os ataques DDoS (*Distributed Denial of Service*) podem ser definidos como ataques diferentes partindo de várias origens, disparados simultânea e coordenadamente sobre um ou mais alvos, em larga escala. Notícia o portal Info Wester que os ataques DDoS ocorrem há tempos, causando prejuízos para várias empresas, bastante conhecidas, atingindo servidores que ficaram inoperantes por algumas horas. Foram vítimas de ataques DDoS as empresas CNN, Amazon, Yahoo, Microsoft e eBay. Em dezembro de 2010, por exemplo, os *sites* da Visa, Mastercard e Paypal sofreram ataques DDoS de um grupo defensor da liberdade e da não existência de "censura" na internet. Em fevereiro de 2012, foram atacados *sites* de bancos brasileiros por motivos semelhantes.²³

Os termos "informática" e "telemática" passaram a figurar no arcabouço jurídico através do art. 10 da Lei 9.296/1996, que introduziu o crime de

²² Disponível em: <http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas>.

²³ Disponível em: <<http://www.infowester.com/ddos.php>>.

“interceptação de comunicações telefônicas, de informática ou telemática,” com objetivos não autorizados em lei.

4.3.1.3 Falsificação de cartão de crédito ou débito

Com a Lei n.º 12.737/2012, foi acrescentado o parágrafo único ao art. 298 do Código Penal, criando a figura equiparada de cartão magnético a um documento particular, para que a falsificação de cartões de débito e crédito, seja incursa nas mesmas penas do crime de falsidade de documento particular (reclusão, de um a cinco anos, e multa).

Na hipótese de o agente realizar a clonagem do cartão e com ele efetuar saques na conta bancária da vítima, pratica apenas furto mediante fraude, ficando, em princípio, absorvida a falsidade. Do mesmo modo, pratica estelionato ao realizar compras em estabelecimentos comerciais.

A inserção do delito de falsificação de cartão de crédito no art. 298 veio com o escopo de proteger a fé pública, contudo se com a duplicação da tarja magnética de crédito ou débito, e sua utilização, a falsidade possivelmente será absorvida pelo delito de estelionato, tendo em vista o princípio da consunção, na esteira da Súmula n.º 17 do STJ.

Nas transações bancárias através da *internet banking* para a aquisição de senhas dos cartões e compras através do mercado eletrônico, fica caracterizado o ilícito informático pela utilização de programas maliciosos, a introdução de vulnerabilidades com o fim de obter vantagem.

De acordo com a jurisprudência, é pacífico que os crimes de saques sem o consentimento da vítima, por meio de clonagem de cartão de crédito ou fraude eletrônica via internet, configuram a conduta tipificada no art. 155, § 4º, II, do Código Penal, tendo em vista a utilização da fraude como meio de burlar a vigilância da vítima e subtrair o bem sem o seu consentimento. A consumação do delito de furto mediante fraude ocorre no lugar onde se localiza a agência do correntista, pois a inversão da posse acontece quando o bem sai da esfera de disponibilidade da vítima, gerando prejuízo. (TRF2, Relatora Liliane Roriz, Conflito de Jurisdição nº. 2010.02.01.002399-0. DJ 04/05/2010).

Assim, a retirada de numerário de contas bancárias com cartão magnético “clonado”, por meio de aparelhos que copiam dados ('chupa-cabras'), constitui furto qualificado, crime patrimonial e não crime informático.

Contudo, a princípio, configura o delito de estelionato, conforme entendimento do Superior Tribunal de Justiça, quando a obtenção de vantagem ilícita se dá através de compra, em estabelecimentos comerciais, utilizando-se de cartões de crédito clonados, o qual se consuma no momento de realização das operações. (CC 101.900/RS, Rel. Ministro Jorge Mussi, Terceira Seção, julgado em 25/08/2010, DJe 06/09/2010).

5 DESAFIOS DE UMA POLÍTICA CRIMINAL DE PREVENÇÃO AO CIBERCRIME

Na construção deste último capítulo pondera-se as questões cruciais sobre controle social, a segurança digital, política de segurança pública, realçando a necessidade de discussão para concepção de políticas públicas específicas visando à prevenção do cibercrime, passando-se a desvelar proposições de Política Criminal, indicativas de caminhos, instrumentos, mecanismos e medidas preventivas jurídicas e extrajurídicas para a prevenção e redução da criminalidade.

O debate sobre a segurança pública envolve um olhar disseminado sobre vários campos do conhecimento ante a complexidade do objeto, não podendo prescindir dos conceitos, definições e princípios que regem as ciências correlatas e que, de um modo ou de outro, se ocupam do crime, seus atores e seus efeitos jurídicos e sociais. Assim, o Direito Penal, a Ciência Política, a Sociologia, a Psicologia, a Medicina, o Direito Administrativo, a Criminologia são fontes de informações que municiam e informam as decisões na formulação de uma política pública de combate à criminalidade.

A partir da Constituição Federal de 1988, o Estado Brasileiro instituiu, com *status* constitucional, o direito à segurança como direito fundamental (art.5º, *caput* da CF) e, por outro lado, atribuiu ao próprio Estado o dever de fornecedor segurança pública, estabelecendo, assim, o marco constitucional da segurança pública, na esfera de atribuições estatais.

No campo legislativo infraconstitucional, a produção de normas punitivas representa apenas um aspecto do controle social, carecendo de maior discussão as normas que definem e estabelecem uma política de segurança voltada não apenas para a repressão, mas, sobretudo, para a solução dos conflitos, antes da judicialização.

A política de segurança pública e a política criminal têm origem constitucional e encontra fundamento nos princípios que norteiam as garantias e os direitos fundamentais, base do Estado Social e Democrático de Direito, embora cada uma possua especificidades e objetos distintos.

A seguir, abordaremos questões relevantes sobre política de segurança pública, política criminal e de prevenção do cibercrime.

5.1 POLÍTICA DE SEGURANÇA PÚBLICA

A Constituição Federal estabelece no art. 144, que a segurança pública é dever do Estado, direito e responsabilidade de todos, exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através da polícia federal, polícias civis, polícias militares e corpos de bombeiros militares.

Segundo dados do Conselho Nacional de Justiça (CNJ), publicados em 28 de setembro de 2010, o Brasil possui a terceira maior população carcerária do mundo, ficando atrás apenas dos Estados Unidos e da China. Ainda, conforme a referida pesquisa do CNJ, em 2010, o Brasil contava com 494.598 presos, sendo que, de acordo com dados do Ministério da Justiça, 44% do total são presos provisórios, o que significa que 219.274 pessoas aguardavam, na prisão, o julgamento de seus processos.

A informação publicada no portal do CNJ²⁴ traz outros números que impressionam por retratar a problemática do sistema prisional. As estatísticas demonstram a fragilidade da política criminal carcerária brasileira. Os mecanismos de controle são questionáveis, mormente quando em confronto constante com a superlotação dos estabelecimentos prisionais, rebeliões, enfim, do alto índice de criminalidade intramuros, o que leva à sociedade a sensação de insegurança, impunidade e a clamar pelo endurecimento das normas penais.

Inexiste um sistema coerente no Brasil, as políticas criminais se misturam, de acordo com os anseios da opinião pública, conduzindo o legislador, muitas vezes, por leis próprias do sistema “ordem pública” e “segurança pública”, a oscilação ente a criação de leis que exasperam as penas, ora optam por políticas criminais que flexibilizam a execução de penas, acolhendo as mais variadas correntes da doutrina e jurisprudência.

Todas essas vacilações e incapacidades de produzirem bons resultados nas políticas criminais levam a sociedade ao descrédito das instituições estatais, criando uma crise de credibilidade em termos de lei e ordem e, ainda, pela incapacidade de desenvolver um sistema de justiça viável aos propósitos do controle social.

²⁴ Disponível em: <<http://www.cnj.jus.br/noticias-gerais/9874-brasil-tem-terceira-maior-populacao-carceraria-do-mundo>>. Acesso 25 mar. 2014.

Por outro lado, ante a criminalidade crescente, o legislador, pressionado pela opinião pública, em resposta, edita leis cada vez mais punitivas, como a Lei dos Crimes Hediondos e, mais recentemente, a Lei Maria da Penha.

As estatísticas apontam para altos índices de violência urbana e de novos tipos de criminalidade em plena ascensão e continuam mostrando resultados insatisfatórios, sugerindo que se repense o problema da segurança pública, a partir de abordagens científicas, pautadas na adoção de medidas e práticas que podem ser bem sucedidas após profunda profilaxia das possíveis origens históricas, sociológicas e políticas da criminalidade.

Os efeitos do crime na sociedade, as nefastas consequências lesivas provocadas às vítimas, no grupo familiar e, em determinados grupos especiais, como crianças, idosos, portadores de necessidades especiais, na provocação da dor, dos sofrimentos, angústias, humilhações e de modo mais enfático o medo, o pavor são sentimentos que repugnam a consciência e o princípio da dignidade humana.

Na obra *Polícia e Sociedade*, a professora Ivone Freire Costa (2005) assegura que, na contemporaneidade, com a insegurança, o processo de degradação da ordem social é visível e se torna uma rotina, percebendo a urgência na mudança desse estado de coisas, alertando que

de forma geral, a violência tem sido vista mais comumente como ato físico ou verbal contra uma pessoa, ou como crime contra o patrimônio, quando se refere apenas a um dos seus aspectos: a criminalidade. Todavia, a sua noção é muito mais ampla do que esse sentido restrito da delinquência e das suas consequências. (COSTA, 2005, p. 199).

Na análise da problemática da insegurança social, decorrente da violência e da exclusão, Ivone Costa (2005), chama a atenção para outros fatores de degradação social, como o racismo, as questões éticas de um modo geral, a crise de valores e descrença nas instituições públicas, o individualismo negativo, o não assumir os deveres sociais, a transferência de responsabilidades para *outros*, no cômputo geral, tudo isso se transforma em práticas cotidianas de vida, contribuindo para a insegurança social, alertando para a percepção de que, no mundo atual,

a violência social pode ser pensada como efeito macro-sociológico da *anomia*, — ou melhor, como ausência total de referências nas relações sociais; como também ser vista como *formas concretizadas de poder* e,

ainda, como ausência de *ética*, que envolveria a dimensão da alteridade. Entende-se que estes diferentes sentidos da violência não são excludentes entre si, ao contrário, todos eles expressam dimensões de uma realidade social. Compreende-se assim, a ideia de ser uma construção política, aquela que resulta do jogo de interesses em confronto com a vida social. (COSTA, 2005, p 199).

O aspecto econômico do crime é outra variável a ser considerada em qualquer política criminal preventiva, além do sentimento de insegurança cada vez maior dos cidadãos e empresas, a violência gratuita e os crimes patrimoniais levam ao aumento dos custos com equipamentos de segurança, seguros, dentre outros gastos pelos cidadãos e empresas e, ainda, conduz o poder público a deslocar para a área de segurança, as receitas que, em situação de índice de criminalidade aceitável, seriam encaminhadas para a educação, saúde e investimentos em infraestrutura.

Em consequência, observa-se que, no Brasil, o sistema penal é excessivamente caro. Segundo os dados levantados em 2013, pelo Senado, o custo com cada presidiário por ano é de 40 mil reais, custo este que é cerca de três vezes mais o que se investe por ano por estudante de nível superior.²⁵

Criador nato das políticas criminais, o Poder Legislativo vacila ante a urgência ditada pelo aumento da criminalidade e as correntes sociológicas, filosóficas, criminológicas e jurídicas que pendem para a adoção de medidas alternativas no tratamento do delinquente ocasional.

Em igual perspectiva, o Poder Executivo anuncia o aumento dos investimentos na construção de presídios e do efetivo policial em busca de soluções imediatas para o controle do crime sem, entretanto, obter êxito significativo, vez que, no geral, os índices de criminalidade só aumentam.

No julgamento de um Recurso Especial,²⁶ a Ministra Ellen Grace, do Supremo Tribunal Federal, assevera que o direito à segurança é prerrogativa constitucional indisponível, garantido mediante a implementação de políticas públicas, impondo ao Estado a obrigação de criar condições objetivas que possibilitem o efetivo acesso a tal serviço, contudo é possível ao Poder Judiciário determinar a implementação pelo

²⁵ Reportagem de Ricardo Setti, publicada pela Revista Veja, Editora Abril, de 2 jun. 2013. Disponível em: <<http://veja.abril.com.br/blog/ricardo-setti/tag/custo-por-ano-do-presidiario/>>. Acesso em: 10 mar. 2014.

²⁶ STF, RE 559.646-AgR, Rel. Min. Ellen Gracie, julgamento em 7-6-2011, Segunda Turma, DJE de 24-6-2011.

Estado, quando inadimplente, de políticas públicas constitucionalmente previstas, sem que haja ingerência em questão que envolve o poder discricionário do Poder Executivo. As cortes de justiça têm lançado mão do conceito aberto de “boa política criminal”²⁷ para reconhecer aos acusados o direito de responder ao processo em liberdade e na fase processual à diminuição de penas e até absolvição. Do mesmo modo, aos condenados, na fase de execução da pena aplicada, a jurisprudência tem vinculado à boa política criminal a concessão de benefícios ao apenado como progressão da pena e indultos, dentre outros benefícios. Na escolha da política criminal de controle, é necessário o estudo de muitas variáveis. Não é coerente uma política que não considere, sobretudo, a necessidade de novos enfoques em relação à prevenção. Não basta atender apenas à leitura dos dados, constatando-se o aumento da delinquência. É preciso ir além para pesquisar novas espécies de criminalidade, quais os fatores que desencadearam a reiterada delinquência e as repercussões do delito para as vítimas e a sociedade.

Um bom começo para apresentação de uma resposta à sociedade seria a definição da política de segurança adequada e proporcional à atual conjuntura. Ou, ainda, quais as políticas que se quer e são possíveis de serem programadas, mas é imprescindível que o Poder Público defina, planeje e limite as diretrizes e ações da política de segurança que está obrigado a executar.

O constitucionalista José Afonso da Silva (2010) esclarece que segurança pública “consiste numa situação de preservação ou estabelecimento dessa convivência social que permite que todos gozem de seus direitos e exerçam suas atividades sem perturbação de outrem”.

Na definição de Filocre (2008, p. 62.), o Direito de Segurança Pública “é o tratamento *jurídico que se dá à política de segurança pública*. É o conjunto normativo

²⁷ PENAL - PROCESSO PENAL: FURTO - PRISÃO EM FLAGRANTE - AGENTE TECNICAMENTE PRIMÁRIO – [...] Os autos demonstram que o mesmo foi preso em flagrante delito em 22/02/00, nada mais justificando a sua manutenção no cárcere, devendo, pois, ser medida de **boa política criminal** tentar evitar contato e a permanência do paciente. Com os reais e perigosos criminosos que praticam crimes mais graves e sérios. Um jovem que ainda está ingressando nos caminhos do crime pode ser recuperado pela autoridade, desde que se tenha em mente que o cárcere nos dias de hoje certamente não é o melhor caminho para plena recuperação daquele que caiu pela primeira vez nas malhas da criminalidade, e que os dias já passados na prisão sirvam de lição para quem comete o seu primeiro crime. O agente em comento merece uma oportunidade de mostrar seu arrependimento pelo ato praticado, voltando a reintegrar-se na sociedade com os olhos voltados para o futuro honesto, sendo de salientar-se que à luz do que até aqui consta dos autos não constato a presença dos requisitos legais para a cautela. (TJ-DF - HC: 20000020010963 DF , Relator: P. A. Rosa de Farias, Data de Julgamento: 06/04/2000, 1ª Turma Criminal, Data de Publicação: DJU 28/06/2000 Pág. : 45) (grifos nossos)

e principiológico que formata juridicamente as políticas de segurança pública do Estado.” Sobre a definição das políticas de segurança, assevera Filocre (2007, p. 15) que

não ter uma política de segurança pública declarada e definida é, por si só, uma escolha política. É uma opção do Estado que se expõe ao risco de não ter mecanismos de controle da criminalidade ou, tendo-os, não saber acioná-los nos momentos adequados ou na dosagem certa para a manutenção da ordem pública. Consequentemente, menos garantidas estão a *segurança jurídica* e a *segurança material* da sociedade sem política de segurança pública.

Ressalte-se que as iniciativas de política criminal no Brasil não tinham uma tradição de embasamento técnico científico coordenado nos diversos estados da federação, consentânea com os dias atuais. Somente, a partir da implantação do Sistema Único de Segurança Pública – SUSP e do Programa Nacional de Segurança Pública com Cidadania – Pronasci, observa-se uma mudança de paradigma na criação de políticas de segurança pública que melhor se amoldar à realidade nacional.

Com efeito, o crescimento da criminalidade, não obstante a adoção de algumas políticas de combate à criminalidade em nível de políticas repressivas estaduais, apesar do modelo federativo, levou o Governo Federal, à recente implantação do Sistema Único de Segurança Pública – SUSP, como um programa de combate à criminalidade e defesa dos direitos humanos no País, constituindo um programa de política pública com objetivo de articular as ações federais, estaduais e municipais na área da segurança pública e da justiça criminal, cuja coordenação, a cargo do Pronasci, caminha para a concretização de uma política pública social de prevenção e de minimização dos efeitos da criminalidade

O Programa Nacional de Segurança Pública com Cidadania – Pronasci²⁸, criado por lei e regulamentado, em execução pelo Ministério da Justiça, visa ao enfrentamento do fenômeno da criminalidade crescente no país através da articulação de políticas de segurança com ações sociais, priorizando a prevenção, e busca atingir os grupos sociais mais sujeitos aos nefastos efeitos da violência decorrente da criminalidade relevante. Entre os principais eixos do Pronasci,

²⁸ A Lei n.º 11.530, de 24 de outubro de 2007, instituiu o Programa de Segurança Pública com Cidadania – PRONASCI. Ministério da Justiça. Disponível em: <<http://portal.mj.gov.br/pronasci>>.

destacam-se a valorização dos profissionais de segurança pública, a reestruturação do sistema penitenciário, o combate à corrupção policial e o envolvimento da comunidade na prevenção da violência.

Além dos profissionais de segurança pública, o Pronasci tem, também, como público-alvo, jovens de 15 a 24 anos, à beira da criminalidade, que se encontram ou já estiveram em conflito com a lei, presos ou egressos do sistema prisional e, ainda, os reservistas, passíveis de serem atraídos pelo crime organizado em função do aprendizado em manejo de armas, adquirido durante o serviço militar.

O Pronasci constitui o reconhecimento de que medidas estritamente repressivas e implementadas exclusivamente pelas instituições tradicionais de combate ao crime – polícia, justiça e sistema carcerário – não têm demonstrado eficácia no tocante à prevenção e à recuperação com a inserção do condenado ao convívio social com dignidade. É preciso que os projetos de prevenção primária e secundária da violência tornem-se uma realidade palpável.

Para tanto, é preciso que o Pronasci concretize os programas previstos nos seus quatro eixos de medidas preventivas e de longo prazo, implementando as medidas estruturantes com investimentos na formação dos agentes de segurança, com a integração dos jovens aos programas de formação e apoio às famílias, urbanização e projetos educacionais, dentre outros.

Este programa governamental, de difícil implementação em algumas metas programáticas, representa o começo de mudança de paradigma no trato das políticas criminais de controle social.

A tomada de posição quanto às políticas de segurança pública, também, envolve enorme complexidade. No entanto, dentro do arcabouço normativo constitucional, o Estado deve escolher aquela que, dentro da sua discricionariedade relativa, possa alcançar melhor resultado. Nesta perspectiva:

A segurança pública nada mais é que operação estatal de mecanismos reguladores. Um mecanismo regulador essencial da sociedade é a norma jurídica. E a norma jurídico-política por meio da qual se dá a manutenção e o alcance da ordem pública, ou seja, a manutenção e o alcance do estado de estabilidade dinâmica da sociedade que confere aos indivíduos relações livres é a norma jurídica da política de segurança pública, quando em sede de controle da criminalidade. (FILOCRE, 2010, p. 25).

A respeito do tema, o mesmo autor, discorrendo sobre o combate à criminalidade genérica ou de combate à criminalidade específica, sugere que:

A elaboração de política de segurança pública que tenha por finalidade o combate a criminalidade genérica ou específica não decorre do dado quantitativo tomado isoladamente. A política de segurança pública é elaborada e implementada para combater a criminalidade que possa alterar ou efetivamente altera o equilíbrio e estabilidade social. Vale-se, pois, do dado quantitativo conjuntamente com outras avaliações qualitativas por meio das quais se detecte os efeitos sobre a ordem pública. Há que se considerar a hipótese de que uma criminalidade específica comprometa o equilíbrio social mesmo que não tenha expressão quantitativa por si só relevante. (FILOCRE, *ibid.*, p.97).

A política criminal, inserida no programa maior da política de segurança pública, constitui-se na sua dinâmica de uma atividade de vigilância, prevenção e repressão de condutas delituosas, contendo um conjunto de diretrizes e ações que tem fundamento num marco legislativo de segurança pública, porém pode envolver entidades não governamentais em sua atuação.

A respeito da definição de Política Criminal, Flávio Cardoso Pereira (2007), pontua que, embora não seja fácil definir de forma integral a Política Criminal, numa primeira visão, no âmbito penal, a Política Criminal é:

um conjunto de medidas e critérios de caráter jurídico, social, educativo, econômico, estabelecidos pelos Poderes Públicos para prevenir e reagir frente ao fenômeno criminal, com a finalidade precípua de manter, no mínimo possível, os limites toleráveis dos índices de criminalidade em uma determinada sociedade. (PEREIRA, 2007, p. 4).

Adverte Pereira (2007) sobre a importância do estudo da política criminal como referencial imprescindível a um correto conhecimento das bases de um Direito Penal, no Estado Democrático de Direito, ressaltando que a Política Criminal se distingue de forma clara de outras duas vertentes afetas às ciências penais – a Dogmática Penal e a Criminologia –, explicando que:

Dito de forma didática, e colacionando os ensinamentos de Luiz Regis Prado, a Política Criminal objetivaria, primordialmente, a análise crítica (metajurídica) do direito posto, no sentido de bem ajustá-lo aos ideais jurídico-penais e de justiça. Já a Dogmática Penal teria por escopo elaborar e desenvolver o sistema, visando a interpretar e aplicar o Direito Penal, de modo lógico (formal e material) e racional. Por fim, a Criminologia consistiria em uma ciência empírica, de cunho interdisciplinar, que estuda o fenômeno criminal utilizando-se do método causal-explicativo. Ocupa-se das circunstâncias humanas e sociais relacionadas com o surgimento, a prática e a maneira de evitar o crime, assim como do tratamento dos criminosos. (PEREIRA, 2007).

Na implementação de uma política criminal, não se pode olvidar que o Estado de Direito reconhece a segurança pública como um dos objetivos fundamentais, merecendo o cuidadoso trabalho e análise crítica do fenômeno da criminalidade, à luz das diversas correntes jurídicas e sociológicas ligadas à criminologia, com a finalidade da produção de conhecimento, de estudo sustentável da criação e adequação das normas que criminalizam condutas, inserindo os crimes no sistema penal punitivo, sua eficácia e reflexos do ponto de vista da vítima, do criminoso e da sociedade.

Do mesmo modo, a escolha da política criminal não pode desprezar que o Direito Penal rege-se pelo princípio da intervenção estatal mínima, razão pela qual a criminalização de uma conduta só se justifica para a proteção de determinado bem jurídico quando os demais ramos do direito se mostrarem insuficientes para a proteção e pacificação dos conflitos, o que denota o caráter subsidiário do Direito Penal, ao tempo em que representa garantia dos direitos fundamentais, um instrumento contra o excesso de intervenção estatal.

O Direito Penal moderno, reconhece o Supremo Tribunal Federal, tem a finalidade de tutelar os bens jurídicos mais relevantes, observando que a intervenção penal deve ter o caráter fragmentário, protegendo apenas os bens jurídicos mais importantes e em caso de lesões de maior gravidade. Neste sentido, referindo-se ao princípio da insignificância, o Min. Celso de Mello do STF, no julgamento do HC n.º 84.412, publicado no DJU de 2/8/2004, afirmou que

considera necessária, na aferição do relevo material da tipicidade penal, a presença de certos vetores, tais como (a) a mínima ofensividade da conduta do agente, (b) a nenhuma periculosidade social da ação, (c) o reduzidíssimo grau de reprovabilidade do comportamento e (d) a inexpressividade da lesão jurídica provocada.

O poder punitivo estatal, através do controle de condutas, busca levar à sociedade a sensação de segurança e previsibilidade, editando o Direito Penal, que representa uma espécie de freio aos transgressores dessas normas e, ao mesmo tempo, impõe um limite ao próprio Estado em sua função repressiva, garantindo os direitos dos cidadãos contra as agências executivas estatais (polícia, administração penitenciária, etc.).

Toda política criminal possui dois focos distintos, um repressivo e outro preventivo. Do ponto de vista repressivo, a criminalização e a persecução

necessitam de norma penal incriminadora e que imponham a pena, segundo os princípios da anterioridade da lei penal e da cominação da pena. No que diz respeito ao controle preventivo, a política de segurança pública não se limita apenas ao policiamento, mas a uma série de políticas outras que possam influenciar nos fatores que contribuem para a prática do crime, com programas e estratégias que podem evitar a ação desviante.

Enfatiza o sociólogo pesquisador Túlio Kahn que, para inibir o crescimento da criminalidade, tanto no Brasil como em outros países, é necessário ir além da visão penal-repressiva, vez que a mesma é limitada como método de compreensão da realidade, em razão de fazer uma “leitura descontextualizada e individualizadora dos conflitos sociais”, intervindo somente “no nível sintomatológico dos conflitos, respondendo, reativamente a ações puníveis de indivíduos” e, portanto, insuficiente como instrumento de produção de segurança diante da criminalidade e do fenômeno da insegurança, conforme alerta o referido autor:

Em contraposição ao conceito usual de segurança pública, a questão criminal passa a ser vista como somente uma das vertentes do fenômeno da insegurança. Não se trata apenas de reduzir a criminalidade, mas também de reduzir insegurança, inclusive subjetiva, que tanto preocupa a população. Para isto, além do crime, é preciso focar também nas pequenas contravenções, nas incivildades do cotidiano, no modo como as agências governamentais ligadas à justiça e a criminalidade tratam com a população. Estar seguro é não apenas estar livre do risco de tornar-se vítima de crimes, mas também livre do medo, livre da violência gratuita, livre do risco de ser destrutado pela polícia e pela justiça. (KAHN, 2002, p. 6).

Como visto, o ordenamento brasileiro ressenete-se de um conjunto normativo que defina com clareza as políticas públicas de segurança, constituindo tanto o SUSP como o Programa Nacional de Segurança Pública com Cidadania – Pronasci apenas um arcabouço com diretrizes programáticas a serem implantadas e não há, neste manancial programático, referência à adoção de políticas de segurança pública relativamente à criminalidade informática.

5.2 POLÍTICA CRIMINAL DE PREVENÇÃO AO CIBERCRIME

Dentre os temas contemporâneos na área de criminologia e sua dialética face ao Estado e seu poder punitivo, a cibercriminalidade apresenta-se como fenômeno de grande relevância, justificando-se, assim, a discussão da problemática por imposição dos apelos da segurança pública interna e da comunidade internacional, com vistas ao enfrentamento do problema da escalada do crime informático e o fenômeno da ciberdelinquência.

Desde a Convenção de Budapeste sobre o Cibercrime, ocorrida em 23 de novembro de 2001, há um consenso de que o acesso à internet deve ser livre e amplo, devendo os países, do mesmo modo que devem promover a aplicação da lei e o respeito aos direitos fundamentais, incrementar políticas públicas de inclusão digital.

Na era da informação, a administração pública e a sociedade passam a depender cada vez mais da tecnologias e da segurança digital. Basta citar a dependência das atividades bancárias e de cartão de crédito, das quais milhares de transações financeiras são concomitantemente realizadas graças aos sistemas informáticos de redes, os quais podem ser alvos de um único ataque capaz de provocar estrondosos prejuízos.

Afirma Crespo (2011, p. 126) que, desde a expansão da internet na década de 80, a comunidade internacional percebeu a necessidade de prevenir ilícitos digitais, tendo a ONU, em 1994, expedido a Resolução sobre os crimes cibernéticos, com a publicação do Manual sobre prevenção e controle do delito informático, que enfatiza a necessidade de cooperação internacional diante do caráter transnacional dos delitos informáticos. Sob este enfoque, o Preâmbulo da Convenção de Budapeste sobre o Cibercrime, (2001) enuncia que

reconhecendo a importância de intensificar a cooperação com os outros Estados partes da presente Convenção. Convictos da necessidade de prosseguir, com caráter prioritário, uma política criminal comum, e com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional; Conscientes das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas; Preocupados com os riscos de que as redes informáticas e a informação eletrônicas, sejam igualmente utilizadas para cometer infracções criminais e de que as provas dessas infracções sejam armazenadas e transmitidas através dessas redes.

Assim, a referida Convenção de Budapeste de 2001, enfatiza a necessidade de cooperação internacional diante do caráter transnacional dos delitos informáticos, explica que a ausência de acordos de cooperação e para a extradição, a ausência de uma legislação que defina como crime as condutas delitivas, a insuficiência dos meios materiais e o despreparo das polícias, do Ministério Público e do Poder Judiciário contribuem para a ineficácia de políticas de proteção e persecução ao cibercrime. (CRESPO, 2011, p. 126).

Neste contexto, as discussões a respeito do fenômeno cibercrime com o escopo da persecução e prevenção tomaram impulso, sobretudo, no cenário internacional. Esta mobilização resultou na Conferência Mundial sobre o Cibercrime, conhecida como Convenção de Budapeste, de 2001²⁹. A orientação para a criação e a implantação de uma política criminal de prevenção e combate à cibercriminalidade está minuciosamente detalhada no estatuto da Convenção de Budapeste de 2001. E, ao firmarem esta Convenção, os Estados membros do Conselho da Europa e os Estados signatários ajustaram dar o caráter prioritário e estabelecer uma política criminal comum com o objetivo de proteger a sociedade dos delitos praticados no ciberespaço, adotando legislação adequada baseada na cooperação internacional.

Essa convenção é um tratado internacional de direito penal e direito processual penal, que tem como objetivo definir de forma harmônica, no continente europeu e países signatários, os crimes praticados no ambiente da internet e as formas de persecução. Basicamente, trata das violações de direito autoral, fraudes relacionadas a computador, pornografia infantil e violações de segurança de redes e invasão de computadores.

A referida Convenção sobre Cibercrime, assinada em Budapeste, surgiu como o primeiro instrumento internacional sobre esse tipo de criminalidade, visando à harmonização das legislações nacionais dos Estados na área do cibercrime, bem como facilitando a cooperação internacional e as investigações de natureza criminal.

Em seus eixos temáticos, a Convenção define crimes contra a confidencialidade, integridade e disponibilidade dos sistemas de computadores, crimes referentes aos conteúdos e crimes informáticos. Contém disposições que

²⁹ A Convenção e sua Minuta do Relatório Explicativo foram adotados pelo Comité de Ministros do Conselho da Europa na Sessão 109 de 8 de novembro de 2001. Foi aberta à assinatura em Budapeste, em 23 de Novembro de 2001, e entrou em vigor em 1º de julho de 2004. Até 2 de setembro de 2006, 15 Estados haviam assinado, ratificado ou aderido à Convenção, enquanto mais 28 Estados a assinaram, mas não a ratificaram.

visam à proteção das crianças e aos direitos de autor na internet e, no seu protocolo adicional, cuida da discriminação na internet, por meio do racismo e da xenofobia. Inclui, também, medidas processuais, de investigação e cooperação internacional com vista a regular os mecanismos probatórios e de preservação dos dados de conexão, para fins processuais penais.

Com a adesão às suas cláusulas, os Estados-Parte estabeleceram o dever de criminalizar algumas condutas violadoras de direitos e de bens jurídicos afetados pelo uso abusivo, antiético e ilícito, recorrentes no ciberespaço, bem como seguir a determinação de que cada parte deve adotar uma política criminal dentro das balizas traçadas pelo documento.

Mais de trinta países assinaram a Convenção de Budapeste, também conhecida como CETS 185, além dos países do Conselho da Europa, assinaram o texto os Estados Unidos da América, o Canadá, a África do Sul e o Japão, sem ratificá-lo, enquanto a Argentina, o Chile, a Costa Rica, o México e a República Dominicana já manifestaram interesse oficial de ratificar o tratado.³⁰ Comentando acerca do tema Vladimir Aras (2001) chama a atenção para os seguintes aspectos:

A Europa em peso, ao lado dos Estados Unidos, segue uma dupla via: prevê os direitos do ciberespaço, especialmente a liberdade e a privacidade, e procura estabelecer, também neste cenário de interação humana, um ambiente de segurança e justiça. Não por outro motivo dezenas de democracias ratificaram a Convenção sobre Cibercriminalidade (Budapeste, 2001), já em vigor internacional.

O Brasil, ainda, não é signatário da Convenção de Budapeste e coloca como empecilho o fato de não ter participado da formulação da convenção. Entretanto, isso não é impeditivo, uma vez que várias disposições legais já foram inseridas no ordenamento jurídico em vigor, tratando de ilícitos informáticos, como se verá adiante.

Embora um tanto lento, o Brasil caminha para assinar a Convenção de Budapeste, considerando que, em termos de política legislativa, foram sancionadas importantes leis que estão em plena harmonia com os fins da Convenção do Cibercrime. No âmbito da legislação penal que introduz, gradativamente, novos tipos

³⁰ Fonte: Treaty Office on <http://conventions.coe.int> Situação em: 18 mar. 2013.

penais de crimes informáticos, ressalvadas as dificuldades decorrentes das controvérsias de interesses que permeiam essa seara e da ausência de políticas públicas de segurança pública de controle do cibercrime, merecem referência duas novas leis em vigor, a Lei n.º 12.735/2012 e a Lei n.º 12737/2012, já exploradas anteriormente neste trabalho, e que versam, respectivamente, sobre a criminalização de algumas condutas ilícitas, tipificando-as como crimes informáticos e a criação de órgãos públicos especializados no combate e prevenção ao cibercrime.

A Lei n.º 12.737/2012, como já visto antes, dispõe sobre a tipificação criminal de delitos informáticos e acrescenta ao Código Penal o art. 154-A, o qual passa a prever o delito de "invasão de dispositivo informático", criminalizando a invasão de dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem a autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita, cominando à pena de detenção, de três meses a um ano, e multa.

Já a recente Lei n.º 12.735/2012, resultante do projeto de lei PL 84/2.001, do Deputado Eduardo Azeredo, após a tramitação que durou treze anos, foi aprovada com vários vetos, mas restou incólume o seu art. 4º, que trata da criação e implantação de estruturação perante as polícias judiciárias de órgão e departamentos voltados a possibilitar a investigação e o combate à delinquência cibernética. O referido dispositivo legal tem a seguinte redação:

Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

A partir desta disposição (art. 4º da Lei 12.735/2012), instituiu-se o marco legislativo que autoriza polícias públicas de combate às condutas delituosas na redes de computadores.

A instalação de delegacias especializadas na persecução dos crimes cibernéticos tem papel importante para as vítimas, que, por ausência e inércia do órgão policial, ou descrédito, não aciona o aparato policial por descrença de que haverá qualquer investigação ou punição dos infratores.

Mesmo antes da definição de uma política pública de segurança voltada ao combate ao cibercrime, algumas Secretarias de Segurança Pública, a exemplo do Paraná, instalaram delegacias especializadas na investigação de crimes informáticos. Tais iniciativas otimizam o tempo de investigação e coleta de provas, apreensão, perícias nas redes e computadores, com o fito de identificação da autoria e materialidade, pressupostos sem os quais não se pode passar à fase da persecução criminal perante a Justiça Criminal.

Na concepção de Política Criminal de controle, não basta uma legislação que incrimine certas condutas ilícitas e a persecução penal. A criação de um programa de política criminal de prevenção primária, fundamenta-se na educação, na inclusão social e melhoria da qualidade de vida, que capacita o cidadão a evitar ou superar de forma civilizada e eventuais conflitos.

Na seara da criminalidade cibernética, é preciso conceber políticas públicas voltadas à segurança digital, investindo-se nos programas que desenvolvem tecnologias de proteção digital do fluxo de conexões no ciberespaço. Ao mesmo tempo, são necessárias políticas públicas de inclusão digital, com educação informacional, destinadas à atual e futuras gerações de usuários da internet.

A conscientização de um agir ético perante a *web*, campanhas educativas e informação de que as diversas infrações digitais constituem crime passível de efetiva punição, certamente, inibirão alguns internautas mal intencionados, mas é possível que não surtam qualquer mudança ética dos delinquentes virtuais que devem ser alvos de persecução de agentes estatais bem preparados, com o mesmo nível de conhecimento tecnológico e equipamentos informáticos e eletrônicos de última geração.

Para concepção dessas políticas preventivas são muitas as variáveis a serem avaliadas, exigindo-se participação interdisciplinar nos campos do Direito, da Tecnologia da Informação, da Sociologia, da Criminologia, e a Política Criminal, dentre outros, ponderadamente discutidos para fundamentar as escolhas e os programas a ser cumpridos, vez que, seus efeitos e resultados, serão alcançados a médio e longo prazo.

No capítulo seguinte abordaremos a questão da criminalização de condutas ilícitas ocorrentes no ciberespaço, sob o enfoque de política de prevenção aos ilícitos cibernéticos.

5.2.1 A criminalização de ilícitos informáticos e prevenção

Em termos de política pública de prevenção, impõe-se questionar se a criminalização de novas condutas ilícitas no âmbito do ciberespaço constitui uma boa política de prevenção à crescente cibercriminalidade. A questão é deveras complexa. A noção moderna de prevenção aparece timidamente com a Escola Clássica, segundo a qual a pena exerce uma importante função de intimidação geral, mas tem a sua verdadeira origem na Escola Positiva de finais do século XIX.

A concepção de tipificar, reprimir e penalizar, segundo a dogmática clássica, constitui a opção voltada a tutelar os bens jurídicos, desestimulando a prática de crimes, tornando desinteressante a atividade ilícita. Contudo, segundo os princípios do Direito Penal clássico, a prevenção vem em segundo plano, e só vai surtir efeitos para o caso de condenados, influenciando como desestímulo para a reincidência. Em consequência, uma política atual de enfretamento da criminalidade informática não pode ser embasada apenas nos mesmos postulados de uma política criminal positivista, concebida para uma criminalidade comum, cuja a incidência não alarmava.

Sob a vertente sociológica, na esteira Criminologia Crítica, segundo Baratta (1999, p. 215), os problemas ligados ao fenômeno da criminalidade, não serão resolvidos com uma receita aviada pela criminologia, mas argumenta que a grande contribuição e a primeira tarefa da Criminologia Crítica é problematizar a questão criminal, o sistema penal, os mecanismos de seleção, fornecendo uma análise político-econômica para avaliar e fornecer as respostas possíveis a situações sociais estudadas, com escopo de indicar alternativas dos problemas sociais relacionados com o fenômeno da criminalidade, sem a garantia de que os estudos e alternativas indicadas ofereçam as respostas imediatas ao problema criminal como, equivocadamente, pretendia a criminologia de base etiológica.

Enquanto produção de conhecimento que identifica os princípios que orientam a ação política de combate ao crime, a política criminal pode se valer da Criminologia Crítica, na sua vertente dialética, voltada para a problematização dos mecanismos e funcionalidade de atuação do sistema penal, subsidiando-o com suas propostas teóricas.

Assim, nas escolhas, tanto na criminalização primária quanto secundária e na perspectiva do poder político de definição do bem jurídico a ser protegido pela norma penal incriminadora, a política criminal poderá filtrar com o fim de subsidiar o legislador que exerce o poder político de eleger o que é crime e como punir. Mormente, a relação entre a criminologia, a política criminal e o direito penal pode ser vista como de interdependência.

No campo da criminalidade comum, a Criminologia Crítica tem condições científicas de apontar um programa alternativo de política criminal, concebido para reduzir o direito penal e para humanizar o sistema penal, estruturando-o conforme conhecimento integrado das Ciências Sociais, que possibilita a abordagem mais ampla e aprofundada do controle punitivo, considerada sua complexidade e a inarredável relação com a estrutura social.

No entendimento de Gomes e Cervini (1997, p. 26), para uma fundamental postura da legitimante do controle punitivo, dentro da política criminal que se propõe a ser diretriz da vontade jurídica, deve ter sua fundamentação baseada nos estudos criminológicos, transformando o plano programador e o plano operacional do sistema penal.

Neste conjunto de ideias, a criminologia seria fornecedora de conhecimento para a construção de uma política criminal de postura legitimadora de um controle punitivo, guiada por vetores valorativos democráticos, que respeitem as garantias fundamentais e operacionalizem um sistema penal com menor potencial estigmatizante e ineficaz nos propósitos da recuperação do apenado.

A busca de uma política criminal mais justa e humanizada deve ir além da esfera estatal, envolvendo de forma participativa a sociedade que, em última análise, sofre os efeitos deletérios da criminalidade.

Do mesmo modo, a concepção atual de prevenção não pode prescindir do trabalho educacional, de formação de uma cultura menos beligerante, de modo que produzam real impacto social na formação de uma cultura massificada que leve a uma convivência mais harmônica e educada no sentido de evitar práticas lícitas. De outra banda, em relação à prevenção, observa-se certa imprecisão e inadequação do significado desse termo. São várias as concepções sobre o que deve ser uma ação preventiva.

Atualmente, com a emergência de novos riscos sociais, há uma tendência de instituição de política criminal que alarga a incidência de normas penais, com a

criação de novos tipos de intervenção. Assim, por exemplo, em face de interesses preventivos aumentam-se as cominações penais e expandem-se os meios de coação na instrução criminal para o combate de crimes organizados, tráfico de drogas, lavagem de dinheiro, dentre outras infrações penais.

Nesta linha de entendimento, são muitas as vozes que se levantam contra a inflação de criminalização, que, ao final, podem coadunar resultados indesejáveis. Anote-se, por oportuno, a opinião do Procurador de Justiça da Bahia, Rômulo Moreira:

Tenho insistentemente pugnado contra o excesso de criminalização de condutas em nosso País, transformando aquilo que deveria ser a **ultima ratio** em **prima ratio**, basicamente pelo fato de que ao longo dos anos a ineficiência da pena de prisão mostrou-se de tal forma clara que chega a ser difícil qualquer contestação a respeito. Em nosso País, por exemplo, muitas leis penais puramente repressivas estão a todo o momento sendo promulgadas, quase sempre para satisfazer a opinião pública (previamente manipulada pelos meios de comunicação), sem que se atente para a boa técnica legislativa e, o que é pior, para a sua constitucionalidade. E, mais: o encarceramento como base para a repressão. Assim, por exemplo, ao comentar a lei dos crimes hediondos, Alberto Silva Franco afirma que ela, *“na linha dos pressupostos ideológicos e dos valores consagrados pelo Movimento da Lei e da Ordem, deu suporte à idéia de que leis de extrema severidade e penas privativas de alto calibre são suficientes para pôr cobro à criminalidade violenta. Nada mais ilusório.”*[3]

Continua Moreira (2012) afirmando que, na imensa maioria das vezes, de nada adiantam leis severas, criminalização excessiva de condutas, penas mais duradouras ou mais cruéis, citando o Ministro aposentado do Supremo Tribunal Federal Evandro Lins e Silva, que afirmou:

“Muitos acham que a severidade do sistema intimida e acovarda os criminosos, mas eu não tenho conhecimento de nenhum que tenha feito uma consulta ao Código Penal antes de infringi-lo.”[...] “precisamos despenalizar alguns crimes e criar punições alternativas, que serão mais eficientes no combate à impunidade e na recuperação do infrator (...). Já está provado que a cadeia é a universidade às avessas, porque fabrica criminosos, ao invés de recuperá-los.” “A prisão avilta, degrada e nada mais é do que uma jaula reprodutora de criminosos”, informando que no último congresso mundial de direito criminal, que reuniu mais de 1.000 criminalistas de todo o mundo, “nem meia dúzia eram favoráveis à prisão.”

Mas é necessária a criação de norma penal mínima que enumere, de forma mínima, pelo menos, os tipos penais mais importantes que já estão previstos no Direito Penal Comparado, introduzindo o país na rede internacional de enfrentamento à cibercriminalidade. Todavia, seria imprudente a criação de novos

tipos penais de cibercrime, sem alinhar-se com as normas penais sancionadoras dos países subscritores da Convenção de Budapeste, que consideram a criminalização de certas condutas ilícitas praticadas na rede como forma de controle e prevenção.

Ocorre que, na seara da nova criminalidade informática, a estrutura jurídica do tradicional direito penal se mostra insuficiente para enfrentar a realidade dos fatos que ocorrem no ciberespaço. Nota-se grande desinformação neste campo, pois a informática é uma ciência nova e poucos possuem conhecimentos de seu objeto.

A ausência de uma política criminal definida de enfrentamento e prevenção de crimes informáticos, além da indefinição de concepções sobre o que deve ser a ação e os métodos preventivos neste campo, deixam muitos questionamentos e insegurança, sobretudo indefinição sobre os objetivos da polícia, se prevenção, repressão ou detecção dos delitos cometidos no ciberespaço.

Destarte, uma política criminal voltada para o controle da cibercriminalidade deve levar em consideração as premissas da “Nova Criminologia” que, segundo Silena Jaime (2006), possuem os seguintes postulados:

- a) abolição da pena privativa de liberdade, inútil como meio de repressão do delito e como forma de ressocialização do delinquente. A prisão funciona apenas enquanto seu caráter estigmatizante;
- b) a criminalidade deve ser considerada segundo a classe social de que provenha – proletária ou dominante, e a Política Criminal deve ser orientada nesse duplo sentido;
- c) a adoção de um processo de socialização alternativo, um projeto gradual e intenso de descriminalização, despenalização e desjudicialização, transferindo do Estado para a comunidade o controle das condutas criminosas de natureza leve;
- d) criminalização dos comportamentos que causem dano ou ameacem os interesses essenciais da comunidade: criminalidade ecológica, econômica, ofensas à qualidade de vida, à saúde pública, à segurança e higiene no trabalho e outras condutas assemelhadas;
- e) intensa propaganda, visando a denúncia das desigualdades do sistema vigente, e a obtenção do apoio popular aos métodos e à ideologia da Nova Criminologia.

Dentro desta concepção, sobressai a forte tendência de superação do entendimento de política criminal única e exclusivamente de caráter repressivo, qual seja, aquela baseada apenas na política legislativa de criminalização de condutas, na persecução, judicialização e execução penal, aspectos que envolvem política penal, indo em direção à multidisciplinaridade de ações e políticas compatíveis com uma sociedade pluralista e democrática que fomenta a proteção dos direitos fundamentais do cidadão.

Neste diapasão, a política criminal de enfrentamento da violência e criminalidade teria uma amplitude maior que a política penal, que, segundo Baratta, é “uma resposta à questão criminal circunscrita ao âmbito do exercício punitivo do Estado”, enquanto a política criminal é concebida “em sentido amplo, como política de transformação social e institucional”. (BARATTA, 1999, p. 201).

Do ponto de vista de uma agenda de política criminal de prevenção da criminalidade cibernética, a importância dessa distinção entre política penal e política criminal cinge-se a expor a limitação das normas penais positivadas que tipificam delitos informáticos para inibir de forma significativa a delinquência cibernética, sem o auxílio de uma política criminal que conjugue outros mecanismos de prevenção.

Nesta mesma linha, são poucos os recursos humanos e materiais destinados à prevenção. Sem a definição de políticas preventivas, não se atribui aos órgãos oficiais (policiais, promotores, juízes, defensores), a formação especializada para lidar com o problema, ficando as agências e agentes à margem dos conhecimentos técnicos e os métodos preventivos. Não se deve perder de vista que é de fundamental importância a definição das atribuições, a coordenação entre os órgãos que se ocupam da prevenção, bem como a continuidade nas ações empreendidas. São, portanto, urgentes e inadiáveis as inovações para incremento de medidas preventivas e eficientes destinadas ao enfrentamento da nova criminalidade.

É de fundamental importância, também, discutir e definir quais os eixos e instrumentais dessa política de prevenção, as estratégias e ações nacionais e de cooperação internacional, tendo em vista o caráter transacional do cibercrime, aliando, ainda, políticas estruturais com aquisição de aparato tecnológico compatível para lidar com o crime cibernético.

No âmbito desta delinquência, persistir com política criminal baseada apenas na finalidade repressiva pode ser um equívoco, diante da destreza e nível intelectual do delinquente cibernético em confronto com a seletividade do poder punitivo tradicional, sem aparato investigativo adequado, somado à natureza das penas, que, de todo modo, não levará ao encarceramento, o que não é ruim.

Punir um delinquente virtual é tarefa árdua, a persecução penal não está preparada. Outro grande problema reside na chamada “cifra negra”, que, no cibercrime, é muitíssimo mais elevada do que a oficialmente denunciada. Segundo Ferreira (2010, p. 124), estima-se que nos Estados Unidos apenas 1% dos ilícitos informáticos cometidos é descoberto e somente chegam aos Tribunais de Justiça

em torno de 14%, dos quais apenas 3% são julgados com a condenação de pena privativa de liberdade, confirmando que, excetuada a cifra negra, a punição dessa criminalidade é inexpressiva diante do alcance social de uma política criminal preventiva bem planejada e executada.

Alguns ordenamentos jurídicos europeus tipificam alguns fenômenos surgidos com a internet, conhecidos como *cracking*, *cyberpunk*, *preakers*, *smiffers*, *spanmming* e *hacking*, contudo, como observa Ferreira (Ibid., p. 104), alguns doutrinadores entendem que algumas destas condutas deveriam ter suas respostas jurídicas fora da legislação penal.

Num olhar panorâmico sobre as condutas criminalizadas através da Lei 12.737/2012, observa-se que as penas, de um modo geral, são cominadas segundo o critério do menor potencial ofensivo, o que implica a judicialização perante o sistema dos Juizados Especiais Criminais, regidos pela Lei 9.099, de 26 de setembro de 1995. Em decorrência, no sistema dos Juizados Especiais, invariavelmente, é possível a aplicação da transação penal, o que não deixa de ser um aspecto positivo conforme o novo pensamento da criminologia que coloca a pena privativa de liberdade, segundo Baratta (1999, p. 59), como “a forma mais extremada de controle penal”. Contudo, considerando o pouco tempo de vigência, não se têm dados para uma nova reflexão acerca dos efeitos, em relação à repressão e prevenção, e, portanto, seria apressada a avaliação dos propósitos dessas disposições no combate à criminalidade cibernética, no território nacional.

De qualquer modo, a positivação legislativa destas condutas tem o efeito simbólico de estabelecer a ilegalidade e a punição de tais condutas ilícitas, o que atende ao primeiro estágio da prevenção, convergindo com os apelos da comunidade internacional, que entende necessária a criminalização de certas ações perniciosas no ciberespaço.

Em outra ponta, é preciso abrir-se a reflexão sobre o posicionamento dos teóricos da Criminologia Crítica a respeito da criminalização de determinadas condutas que pode funcionar como um complicador a mais do problema do controle social, propugnando que proibir, tornar ilegal e criminalizar aumentam o problema. Tal postura está em diapásão com o direito penal mínimo e, ainda, com a natureza da internet, preservada na Lei n.º 12.965/2013, que instituiu o Marco Civil da Internet, embasado nos postulados da liberdade de expressão, da neutralidade da rede e a proteção à vida privada dos usuários.

Com esteio nessas ideias, no âmbito do ciberespaço, grande parcela das condutas antiéticas e ilícitas pode ser tratada fora do alcance de norma penal, com sanções cíveis de interdição de atividades, imposição de obrigação cominatória de fazer ou não fazer, além da reparação pecuniária dos danos material e moral, se o ilícito assim recomendar.

Ressalte-se, por derradeiro, que uma Política Criminal de prevenção destinada à criminalidade informática ultrapassa os objetivos puramente formais de caráter repressivo e, secundariamente preventivo, da lei penal incriminadora, na perspectiva de que, para atualidade e eficácia de qualquer política de redução da delinquência, deve passar, necessariamente, pelo discurso da problemática da excessiva criminalização, ante as melhores perspectivas da implantação de uma Política Criminal, preponderantemente preventiva, aliando-se às circunstâncias da conveniência e da oportunidade, do momento social e político da concepção da Política Criminal, pelo Legislador.

5.2.2 As Leis 12.735 e 12.737/2012 sob o enfoque da prevenção

Do ponto de vista da prevenção, a Lei n.º 12.735/2012 representa o marco legislativo que fundamenta e estabelece a obrigatoriedade dos órgãos da polícia judiciária estruturar delegacias e treinar equipes para lidar com essa nova realidade.

A estruturação de departamentos de polícia especializados na investigação de crimes digitais se faz necessário diante da complexidade do *modus operandi* dos infratores, com utilização de mecanismos e equipamentos que exigem conhecimentos técnicos diferenciados. Com a mesma técnica e acuidade deve ser formada e constantemente atualizada a equipe de agentes policiais, treinados para lidar com o delito tradicional.

Apresenta-se como prática inovadora e consentânea com o mundo digital, o inquérito policial eletrônico. Como defendem Furlaneto Neto, Santos e Gimenes (2012, p. 126), não se justifica mais “a ação penal informatizada e o inquérito policial em seu arcaico formato de papel”. As diligências e perícias da fase inquisitorial devem ser realizadas através dos meios eletrônicos, com a adoção de um sistema que confira autenticidade, integridade e confiabilidade, em conformidade com as

políticas de segurança e com a constante atualização tecnológica do sistema, da mesma forma que foi instituída a informatização do processo judicial pela Lei n.º 11.419, de 19 de dezembro de 2006.

As delegacias físicas e/ou virtuais são necessárias ao acesso da vítima, ao aparato de persecução, de orientação sobre a *notitia criminis*, a aquisição e preservação da prova do fato delituoso e representação nos casos de ação pública e queixa-crime para desencadear a persecução penal.

Contudo, merece contextualizar o certo descrédito à efetividade da persecução penal, nos delitos informáticos, sob o aspecto da sanção. As penas cominadas aos delitos informáticos, em sua maioria, para os delitos de menor potencial ofensivo, de competência do Juizado Especial Criminal, nos termos do art. 61 da Lei n.º 9.099/95.

Nos crimes de competência do Juizado Especial Criminal, o instrumento de apuração do fato utilizado pela autoridade policial é o termo circunstanciado (art. 69 da Lei n.º 9.099/95). Entretanto, nos casos do art. 154-A do CP, a simplificação do termo circunstanciado, em maiores aprofundamentos nos métodos de investigação, é provável que haja certa dificuldade em apurar a autoria e a materialidade do delito, sem cercar-se de diligências próprias de inquérito policial, com a realização de perícias mais sofisticadas, apreensão de máquinas, solicitações de informações a provedores, etc.

A discussão que ainda está em plena ebulição é justamente a que polariza os adeptos de maior cobertura de condutas que criminalizam ilícitos virtuais e os que entendem que a internet não deve ser regulada, sob pena de inibir sua expansão.

Há quem defenda que os diplomas legislativos Lei n.º 12.735/2012 e Lei n.º 12.737/2012 foram editados com a pretensão de preencher o vazio normativo existente na legislação penal brasileira, de modo que, os novos tipos penais são suficientes para reprimir as condutas ilícitas mais recorrentes praticadas por meio das redes informáticas. Por outro lado, há o posicionamento, segundo o qual, a tipificação criminal de delitos informáticos através da Lei n.º 12.737/2012 deixa de fora do alcance da legislação penal alguns importantes ataques cibernéticos, para os quais não há previsão legal.

Perfilhando deste último posicionamento, o Ministério Público de São Paulo também faz críticas à nova lei dos crimes cibernéticos através de Nota Técnica,³¹ publicada em sua *home page*:

[...] Como visto, a Lei nº 12.737/2012, embora represente certo avanço ao tipificar crimes cibernéticos propriamente ditos, contém inúmeras deficiências e confrontos com o sistema penal e processual penal vigente, o que deve merecer a atenção dos aplicadores.

Os crimes cibernéticos propriamente ditos são a porta de entrada para outras condutas criminosas, facilitando a utilização do computador como instrumento para cometer delitos.

O legislador não contemplou a invasão de sistemas, como os de *clouding computing*, optando por restringir o objeto material àquilo que denominou dispositivo informático, sem, contudo, defini-lo.

Atividades de comercialização de *cracking codes* e de engenharia reversa de software também não foram objeto da norma.

Além das imperfeições na redação dos tipos, as penas cominadas na nova lei são ínfimas se considerada a potencial gravidade das condutas incriminadas, bastando dizer que um ataque de denegação de serviço pode colocar em risco vidas de uma população inteira.

Implicam, por outro lado, a competência do Juizado Especial Criminal, cujo procedimento sumaríssimo é incompatível com a complexidade da investigação e da produção da prova de crimes de alta tecnologia (perícia no dispositivo informático afetado, por exemplo).

Na visão da professora Érica Lourenço de Lima Ferreira, de um modo geral, os crimes passíveis de serem realizados pelos internautas, podem ser enquadrados em vários tipos penais já existentes no ordenamento pátrio, considerando que, na sua maioria, utilizam do sistema informático apenas como mais um meio de alcançar o resultado ilícito. (FERREIRA, 2010, p. 32).

Portanto, existem vários delitos que podem ser cometidos por meio da internet, no entanto encontram sua previsão legal em disposições criminais que tratam diversas matérias, como no Estatuto da Criança e do Adolescente, quando trata do crime de pedofilia, o que pode gerar discussões acerca do enquadramento, podendo gerar a impunidade de seus agentes ou o indiciamento equivocado.

Quanto ao delito de invasão de dispositivo informático, embora seja considerado crime digital propriamente dito, frequentemente pode ser o crime meio para a realização de tantos outros crimes.

O legislador optou por não identificar as demais condutas, por questão de política criminal, o que para alguns juristas, a ausência de tipificação inviabiliza seu combate, ocasionado certa insegurança jurídica.

³¹ Disponível em: <http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%20CIBERN%20C3%89TICOS%20ENTRA%20EM%20VIGOR.pdf>.

Segundo Parker (2013), o Estado avançou prevendo algumas condutas criminosas, contudo uma proteção estatal efetiva, em se tratando do “espaço digital”, demandaria outros tipos penais, o aumento das penas e um aparato que permita uma investigação mais eficaz, afirmando que o enquadramento dos crimes como pequeno potencial ofensivo não se coaduna com a proteção dos ativos intangíveis, a pedra angular da sociedade da informação, colocando como exemplo a situação na qual a apropriação indevida de dados pode ser mais prejudicial que um furto comum, ou na hipótese de espionagem que favorece à concorrência desleal. Segue a especialista em direito digital afirmando que

essas leis não esgotaram os tipos penais digitais, pois é impossível que não se considere como crime a indisponibilidade de sistemas de informação de entidades privadas, como sites de comércio eletrônico ou bancos, ou a disseminação de vírus e outros códigos maliciosos, em razão da sociedade inteira estar cada vez mais interconectada. Também não houve cuidado do legislador ao indicar que a invasão necessita de obtenção, modificação ou exclusão de dados, pois a bisbilhotagem ou envio de dados para terceiros podem desviar do tipo penal, além de considerar que invadir dispositivo sem mecanismo de segurança também não é crime. Sem mencionar que a falta de obrigação de guarda de *logs* de conexão e acesso pode inviabilizar a instrução criminal pela dificuldade em se identificar o agente. Por fim, para que haja proveito da lei para a proteção dos seus dispositivos, é indispensável utilizar proteção com senha, código ou dados biométricos para impedir o acesso não autorizado. Isso vale para computadores de mesa, *notebooks*, *tablets*, *smartphones* e reprodutores de áudio ou vídeo portáteis. É importante deixar um sistema de firewall ou detecção de intrusão sempre ativo e com perfil de atividades maliciosas sempre atualizado e refinado para evitar falsos positivos. (PINHEIRO, 2013)

Sob esse enfoque, percebe-se que o texto legal padece de clareza, implicando em dificuldades para a investigação dos crimes digitais, considerando a complexidade da prova da autoria, o tempo e o lugar do cibercrime. Todos esses fatores contribuem para a problemática do controle do cibercrime, que não é apenas do Estado brasileiro, mas uma realidade global.

Em outra ponta, há quem acredite que essa realidade vem aos poucos se modificando e, em linhas gerais, o Brasil, já dispõe de um arcabouço normativo compatível com as diretrizes da Convenção do Cibercrime, o que possibilitará a atuação da persecução penal. (FERREIRA, 2010, p. 176).

Diante do contexto, sob o enfoque do controle social, pode-se afirmar que o Estado brasileiro não dispõe de meios suficientes para coibir a prática de crimes no ciberespaço, por ausência de criminalização de alguns ataques cibernéticos considerados importantes como, também, da carência de estrutura da polícia judiciária para realizar investigações ou, ainda, pela morosidade da Justiça.

Apesar disso, em oposição à perversidade seletiva do sistema penal, na busca de respostas político-criminais ao fenômeno da cibercriminalidade, analisando-a em um prisma mais amplo, nas suas relações sociais, considerando o propósito da transformação da estrutura social, na perspectiva política e econômica em relação à punição penal, a prevenção apresenta-se como a melhor política criminal.

É importante ressaltar que a prevenção constitui o principal paradigma para o enfrentamento do preocupante problema da cibercriminalidade. Sob a ótica da prevenção, podem ser planejadas e delineiam-se os eixos de atuação e investimentos em medidas destinadas à segurança das informações que circulam na rede, visando evitar a violação dos direitos dos cidadãos que se utilizam dos meios informáticos como conquistas civilizatórias, evitando-se, em consequência, prejuízos de várias ordens. Neste desiderato da prevenção, a educação e a inclusão digital ocupam lugar de destaque, como defende os pesquisadores:

E no mesmo caminho, no meio social, seriam válidas as medidas preventivas de inclusão digital, com a conscientização das pessoas quanto ao uso racional e seguro dos meios informáticos. Isso sem falar no aspecto criminal que deverá ser obviamente aperfeiçoado para tratar das novas realidades sociais, mas sempre deixando claro que é necessária a observância, por parte do Estado, da ideia de proporcionalidade, que nas palavras de Ingo Wolfgang Sarlet se traduz em dupla dimensão, ou seja, proibição de excesso estatal na aplicação da pena, mas também proibição de insuficiência da punição. (MACHADO; SILVA, 2013, p. 15).

Diante das mudanças causadas pela revolução tecnológica, nas últimas duas décadas, uma nova realidade sociológica se exterioriza e conduz à perspectiva de que a prevenção constitui uma diretriz a ser seguida na adoção de política criminal de controle da nova criminalidade que surgiu com a intensificação das relações no ciberespaço.

5.3 POLÍTICAS PREVENTIVAS INOVADORAS

O *Manual sobre a prevenção e controle do delito informático*, publicado pela ONU em 1994, coloca a criminalidade informática como um problema supranacional, transnacional, e não apenas nacional, ensejando esforços destinados à cooperação internacional.

No âmbito nacional, entre as medidas voltadas à prevenção, indica-se a formação de grupos de trabalho formada de especialistas das diversas áreas do conhecimento, para desenvolver e promover éticas informáticas em todos os setores da sociedade, especialmente, em instituições educativas.

O referido manual também recomenda “educar as pessoas sobre a necessidade de promover princípios éticos informáticos, normas e medidas de segurança.” (CRESPO, 2011, p. 129).

A seguir, abordaremos a problemática da segurança digital, a educação informacional e ética, consideradas importantes bases para a criação de políticas públicas, destinadas a prevenção dos ilícitos no ciberespaço.

5.3.1 Política de segurança digital

A vulnerabilidade do tráfego de informação constitui o grande problema da segurança digital. Apesar da recente aprovação do chamado Marco Civil da Internet, a Lei nº 12.965, de 23 de abril de 2014, norma que regula o uso da Internet no Brasil, por meio da previsão de princípios, garantias, direitos e deveres dos usuários da rede, bem como da definição de diretrizes para a atuação do Estado, o governo brasileiro ainda não definiu, nem elaborou política voltada a arrefecer a vulnerabilidade das redes que operacionalizam as comunicações dos órgãos públicos e usuários em geral, assim como operacionalize a fiscalização as empresas que atuam na prestação de serviços de banda larga.

Em termos de delinquência patrimonial, conforme estudo realizado por Danielle da Rocha Cruz, as vítimas dos ataques informáticos mais frequentes “são, em geral, grandes empresas ou instituições financeiras”, através de ataques em forma de sabotagem, espionagem e de fraude. (Cruz, 2006, p 18).

As instituições públicas, igualmente, são vítimas da espionagem cibernética.

Para ilustrar a grandiosidade do problema que afeta a soberania dos países envolvidos, merece destaque, o recente episódio divulgado em julho de 2013, na imprensa internacional, relativo ao ex-agente da Agência Central de Inteligência (CIA), dos Estados Unidos da América, o norte-americano Edward Joseph

Snowden,³² que denunciou a espionagem realizada pelo governo americano em comunicações e tráfego de informações de vários países.

No caso brasileiro, além da espionagem dos cidadãos comuns, a inescrupulosa prática teve como alvo a conta de e-mail da Presidente da República, Dilma Rousseff,³³ causando indignadas reações de setores políticos.

Em pronunciamento na Câmara dos Deputados em, 17/07/2013, o Deputado Eduardo Azeredo, resaltou o despreparo do Brasil para o enfrentamento da chamada guerra digital, especialmente com relação à segurança de dados, afirmando em seu discurso as seguintes evidências:

[...], “quero voltar ao assunto da questão da segurança digital, segurança virtual, dizendo inicialmente que evidentemente as ações de espionagem expedidas pelos Estados Unidos a instituições e cidadãos brasileiros constituem uma prática inaceitável. Mas é importante mostrar que essa ação de espionagem foi realizada com vários outros países, divulgada primeiro em relação à França, e não é só em questão de Internet, mas de ligações telefônicas. Entretanto, é inaceitável que o Brasil não tenha até

³² Segundo matéria divulgada em 9 jul. 2013, no *site da Associação do Ministério Público de Minas Gerais*, extraída do jornal O Globo, conforme denúncias, com base em documentos secretos divulgados do norte-americano Edward Snowden, “cidadãos e empresas que usam no Brasil a rede mundial de internet são espionados pela Agência de Segurança Nacional dos Estados Unidos, a NSA, em conjunto com a CIA. Na segunda-feira (8), o ministro das Comunicações, Paulo Bernardo, pediu que a Anatel e a Polícia Federal investiguem quando e como ocorreram as espionagens e se as agências tiveram apoio de empresas que atuam no Brasil. No dia 6 de junho, o jornal britânico The Guardian, primeiro a divulgar os vazamentos de Snowden, informou como opera a NSA. Um programa de computador dá à agência acesso a e-mails, chats online e chamadas de voz dos usuários dos serviços da Apple, Facebook, Google e Microsoft, entre outros, e tem parceria com uma grande telefônica dos Estados Unidos que mantém relações de negócios com serviços telefônicos no Brasil e noutros países. Segundo O Globo, em janeiro passado o Brasil ficou pouco atrás dos Estados Unidos, que teve 2,3 bilhões de telefonemas e mensagens espionados. Hoje está absolutamente claro que a soberania do país e a privacidade do cidadão brasileiro estão em xeque, afirmou na segunda a ministra da Secretaria de Relações Institucionais, Ideli Salvatti”,[...]. Disponível em: <<http://amp-mg.jusbrasil.com.br/noticias/100599512/espionagem-americana-ameaca-a-soberania-do-brasil>>.

³³ Segundo o jornal O Globo, em notícia divulgada em 01/09/2013 a “Agência de Segurança Nacional dos Estados Unidos (NSA) monitorou o conteúdo de telefonemas, e-mails e mensagens de celular da presidente Dilma Rousseff e de um número ainda indefinido de “assessores-chave” do governo brasileiro. [...], o ministro da Justiça, Eduardo Cardozo, classificou a espionagem como um fato “gravíssimo” e afirmou que, se confirmado o monitoramento das comunicações da presidente Dilma e de seus assessores, o episódio terá sido uma “clara violação à soberania” brasileira.” Disponível em: <<http://oglobo.globo.com/brasil/eua-espionaram-dilma-9782118#ixzz3HZB1b2Rc>>.

hoje adotado práticas de combate a esse tipo de delito, os chamados crimes cibernéticos. As ações de espionagem evidenciam, para além de qualquer interferência inaceitável, que o ciberespaço brasileiro não tem qualquer tipo de segurança, que está totalmente vulnerável a invasões. [...]O que dizer, então? Que nós temos um total despreparo no Brasil para esse assunto da chamada *cyber war*. O Governo destinou 90 milhões do seu Orçamento para a segurança digital, mas aplicou apenas 9% desse valor. Se 90 milhões já era pouco, aplicou apenas 9% desse valor! Sem dizer que o Brasil não é signatário de nenhum acordo internacional de combate a esses crimes cibernéticos, uma especialidade de delito que sabidamente desconhece fronteiras. Particularmente, defendo a adesão do País à Convenção Internacional sobre o Cibercrime, a Convenção de Budapeste, que hoje é o principal tratado internacional de Direito Penal e Processual e que define de forma harmônica essas questões. Mais de 60 nações de todo o mundo, Sr. Presidente, só para concluir, são signatárias desse tratado, mais de 40 membros do Conselho da Europa, além dos Estados Unidos, África do Sul, Canadá, Japão; na América do Sul, Colômbia e Chile já são membros. O Brasil continua indiferente e não está, pelo que pude ver no Senado, semana passada, em depoimento do Ministro Patriota, envolvido nessa questão.” (BRASIL, 2013).

A quantidade de incursões ilícitas em relação à grande massa de internautas é de pessoas que confiam nas relações cibernéticas e não pretendem causar qualquer prejuízo material ou moral e esperam contar com sistemas de segurança que lhes garantam o uso seguro. Na verdade, conforme reconhecem os especialistas em segurança digital, a maioria esmagadora dos internautas navega pelo ciberespaço buscando informações, comunicações através de *e-mails*, diversão dos jogos eletrônicos em rede, pesquisas escolares, divulgação de seus negócios e empresas.

Como salientado, a grande problemática reside justamente na nocividade das condutas ilícitas, que, em decorrência da alta tecnologia e disseminação pelo globo terrestre, apresentam elevado potencial ofensivo.

O acesso à internet e à segurança digital são direitos sociais de última dimensão, aspectos indissociáveis do mesmo direito fundamental à informação e expressão, restando saber o papel dos atores do mundo digital, de quem é a responsabilidade pela segurança dos internautas.

Embora seja de certa complexidade a questão, numa análise sem maior profundidade quanto ao envolvimento da alta tecnologia inerente à operacionalidade técnica, pode-se inferir, a princípio, que a segurança digital é uma obrigação a ser compartilhada por todos aqueles que, de uma forma ou de outra, se utilizam desse meio de comunicação e de informação, que acontece em sistemas computadorizados e perante a *web*. Indústrias que produzem equipamentos

tecnológicos, empresas, governos, organizações não governamentais e o cidadão internauta são responsáveis pela segurança nas suas atividades no ciberespaço.

A segurança digital é vital para a garantia do direito à informação, ao acesso digital das redes informáticas e ao próprio desenvolvimento social e tecnológico. Com efeito, não obstante permear a todos a necessidade de cuidados básicos quando se utiliza as redes informáticas, o alto grau de riscos a que estão sujeitas e a velocidade com que novas tecnologias são criadas com a finalidade de romper as blindagens digitais constituem uma realidade palpável.

Além das empresas e organismos que trabalham com essas tecnologias, os governos passaram a identificar a necessidade de conceber políticas criminais de combate aos crimes informáticos, com a percepção de que, muitas vezes, o ilícito cibernético possui o caráter da extraterritorialidade e, em consequência, a prevenção e a persecução penal de forma rápida e eficaz só poderão ocorrer se houver tratados, acordos ou convenções internacionais com os países soberanos, nos quais são praticadas as ações delitivas ou onde a ação criminosa provoque a lesão à(s) vítima(s).

Na era da informação, estado e sociedade passam a depender cada vez mais das tecnologias e da segurança digital. Basta citar a dependência das atividades bancárias e de cartão de crédito, das quais milhares de transações financeiras são concomitantemente realizadas graças aos sistemas informáticos de redes, os quais podem ser alvos de um único ataque que poderá causar estrondosos prejuízos. Segurança digital é imprescindível para o regular funcionamento da rede mundial de computadores, e de todos os serviços que, hoje, dependem da *web*, sua expansão e o desenvolvimento de mais novas tecnologias.

Desde a origem da produção de equipamentos tecnológicos, empresas, governos, organizações não governamentais e o cidadão internauta, são todos responsáveis, de uma ou de outra forma pela segurança, nas suas atividades no ciberespaço. Em razão da velocidade dos ataques cibernéticos, com alto potencial ofensivo aos direitos humanos fundamentais e aos bens públicos e particulares, as precauções com a segurança e a inclusão digital são necessárias e, por isso, é preciso manter vigilância incessante, através de programas e políticas de Segurança da Informação.

Mas falta recurso do poder público para o combate ao cibercrime, conforme constata o Juiz de Direito Marcelo Mesquita Silva (2012), na dissertação de

mestrado denominada *Ação internacional no combate ao cibercrime e sua influência no ordenamento jurídico brasileiro*. Situação esta comum a todos os países, que não podem prescindir de um permanente plano de prevenção de alguns delitos cibernéticos, indicando como possível viés para minorar o problema, atraindo-se aportes necessários com o estabelecimento de parcerias com a iniciativa privada, com empresas de tecnologia “que detêm capacidade financeira, aparato tecnológico e humano para tanto.” Outra importante dificuldade que esse autor coloca em relevo é, exatamente, a ausência de informação, de conscientização da gravidade da situação. Neste aspecto adverte:

É fato, infelizmente, que o poder público no combate ao cibercrime não consegue reconhecer a potencialidade delitiva de novas tecnologias, até que seja tarde. A resposta dada pelo aparato policial e judicial está muito aquém do mínimo necessário para uma repressão adequada. Mesmo nos Estados Unidos da América a polícia se vê obrigada a realizar métodos de investigação desprovidos de respaldo legal suficiente. (SILVA, M., 34).

É atribuição do Comitê Gestor da Internet no Brasil (CGI), a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país, estabelecendo as diretrizes e estratégias relacionadas ao uso e desenvolvimento da internet no Brasil e regras para a execução do registro de Nomes de Domínio, alocação de endereço IP (*Internet Protocol*), bem como a administração pertinente ao Domínio de Primeiro Nível "br". Também, cabe ao CGI promover estudos, recomendar procedimentos e propor programas de pesquisa e desenvolvimento que permitam a manutenção do nível de qualidade técnica e inovação no uso da internet em âmbito nacional.

Com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à internet no Brasil, o Comitê Gestor da Internet no Brasil, através do Núcleo de Informação e Coordenação do Ponto BR, o NIC.br, entidade civil, sem fins lucrativos, desde dezembro de 2005, é responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à internet brasileira. Atua como um ponto central para notificações de incidentes de segurança, através do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br, atendendo à qualquer rede brasileira, conectada à internet com problemas de segurança.

É grande a preocupação com a segurança dos documentos gerados e em circulação por meio digital. A integridade e confiabilidade desses documentos dependem de técnicas e programas de computadores para dar credibilidade e autenticidade, mormente, aos documentos do comércio eletrônico, científicos e dos processos judiciais. São instrumentos e técnicas que visam à segurança dos atos e documentos no âmbito virtual, a assinatura digital³⁴, a certificação e autenticação, a criptografia e a esteganografia³⁵. (LIMA, 2011, p. 82).

O certificado digital ICP-Brasil³⁶ funciona como uma identidade virtual que permite a identificação segura e inequívoca do autor de uma mensagem ou transação feita em meios eletrônicos. Esse documento eletrônico é gerado e assinado por uma terceira parte confiável, ou seja, uma Autoridade Certificadora – AC, que, seguindo regras estabelecidas pelo Comitê Gestor da ICP-Brasil, associa uma entidade (pessoa, processo, servidor) a um par de chaves criptográficas. Os certificados contêm os dados de seu titular conforme detalhado na Política de Segurança de cada Autoridade Certificadora.

A questão da segurança na rede é de grande complexidade. De maneira geral, envolve entidades privadas prestadoras de serviços relacionadas à segurança de redes, como as provedoras de serviço e as empresas que disponibilizam, no mercado, os programas que detectam invasores como *firewall* pessoal, que é utilizado para proteger um computador contra o acesso não autorizado vindo da internet, e as ferramentas *antimalware*³⁷, que são programas capazes de detectar, anular ou remover os códigos maliciosos de um computador.

³⁴ Assinatura digital, segundo o Instituto Nacional da Tecnologia da Informação, é um mecanismo que identifica o remetente de determinada mensagem eletrônica. No âmbito da ICP-Brasil, a assinatura digital possui autenticidade, integridade, confiabilidade e o não-repúdio - seu autor não poderá, por forças tecnológicas e legais, negar que seja o responsável por seu conteúdo. A técnica permite não só verificar a autoria do documento, como estabelece também uma “imutabilidade lógica”. Qualquer alteração no documento, invalida a assinatura. A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Disponível em: <<http://www.iti.gov.br/>>.

³⁵ Esteganografia x Criptografia: Ao contrário do que pode parecer, esteganografia e criptografia são duas áreas com objetivos diferentes. Enquanto o segundo tem o propósito de impedir que as pessoas saibam o conteúdo de uma mensagem, o primeiro se baseia em evitar que as pessoas saibam que a mensagem existe. Ou seja, na criptografia, os receptores sabem da existência das mensagens, porém não conseguem, a princípio, lê-las; a esteganografia tenta fazer com que os receptores não percebam que há uma mensagem naquele meio [WAYNER, 2002]. Disponível em: <http://www.gta.ufrj.br/grad/09_1/versao-final/stegano/introducao.html>.

³⁶ Disponível em: <<http://www.iti.gov.br/noticias/96-perguntas-frequentes/1743-sobre-certificacao-digital>>.

³⁷ Disponível em: <<http://cartilha.cert.br/>>.

Por todos esses aspectos aqui abordados, verifica-se que, além do viés puramente tecnológico, a segurança digital depara-se com uma série de entraves multidimensionais, ligados à soberania estatal, interna e externa, ante ao caráter sem fronteiras da internet, por envolver a necessidade de cooperação internacional, por existir limitações técnicas, financeiras, legislativas e judiciárias, e, assim, tudo isso, exige um tratamento cooperativo que deve se traduzir em um tipo de governança política que, ainda, não está definida em uma política de prevenção e combate ao cibercrime.

As precauções com a segurança das redes que a Tecnologia da Informação propicia, através de técnicas da Segurança da Informação, como assegura Marcelo Mesquita Silva (2012, p. 37), constitui “a melhor maneira de prevenir os cibercrimes,” que pode ser alcançada com o “desenvolvimento e adoção de medidas de segurança, ao invés de deixá-los aos cuidados do direito penal, simplesmente,” mesmo sabendo que inexistente programa de segurança absolutamente impenetrável ou 100% seguro, haverá, sempre, uma margem de insegurança, mesmo que insignificante diante da cobertura que propicia.

5.3.2 Políticas de educação informacional e ética na internet

Com o escopo de se abordar o problema da ética nas relações cibernéticas, é preciso uma incursão no campo da Filosofia, mesmo que de forma superficial, mas suficiente para problematizar a questão da ética nas relações interpessoais na *web*, e ao mesmo tempo provocar uma reflexão crítica sobre a conduta ética e antiética na dimensão do ciberespaço.

Para a professora Marilena Chauí (2000), a reflexão organiza-se em torno de questionamentos. Assim, a atitude filosófica baseia-se em indagações fundamentais com características negativas e positivas, esclarecendo que:

A face negativa e a face positiva da atitude filosófica constituem o que chamamos de **atitude crítica** e **pensamento crítico**. A Filosofia começa dizendo não às crenças e aos preconceitos do senso comum e, portanto, começa dizendo que não sabemos o que imaginávamos saber; por isso, o patrono da Filosofia, o grego Sócrates, afirmava que a primeira e fundamental verdade filosófica é dizer: “Sei que nada sei”. Admiração e espanto significam: tomamos distância do nosso mundo costumeiro, através

de nosso pensamento, olhando-o como se nunca o tivéssemos visto antes, como se não tivéssemos tido família, amigos, professores, livros e outros meios de comunicação que nos tivessem dito o que o mundo é; como se estivéssemos acabando de nascer para o mundo e para nós mesmos e precisássemos perguntar o que é, por que é e como é o mundo, e precisássemos perguntar também o que somos, por que somos e como somos. (CHAUÍ, 2000).

Segundo Chauí (2000), a Filosofia se interessa por aquele instante em que a realidade natural (o mundo das coisas) e a histórica (o mundo dos homens) tornam-se estranhas, espantosas, incompreensíveis e enigmáticas, quando o senso comum já não sabe o que pensar e dizer e as ciências e as artes ainda não sabem o que pensar e dizer.

Foi através da Filosofia, que os gregos subsidiaram o ocidente europeu com as bases e os princípios fundamentais da chamada razão, racionalidade, ciência, ética, política, técnica, arte. (CHAUÍ, 2000).

A Ética como Ciência do *Ethos* começa na cultura grega antiga, partindo do pressuposto de que o homem é pequenino e insignificante perante os Deuses, mas isso não os impede de buscar e ser responsável por sua vida e felicidade. O homem é um animal político, conforme a filosofia de Aristóteles em suas obras *Política* e *Ética a Nicômano*. E, para Aristóteles, era na *polis* que o homem se realizava enquanto ser, onde encontrava o sentido de fazer parte da comunidade e, principalmente, o sentido da sua existência. Aquele que não fosse capaz de viver em sociedade era dotado de bestialidade ou divindade. Apenas na cidade, e somente nela, o homem seria completo, porque somente na *polis* poderia encontrar a virtude. (SILVA, A., 2013).

A ideia de virtude, na Grécia Antiga, tinha o sentido da excelência de cada ação, fazer bem feito, na justa medida, cada pequeno ato. Atualmente, a palavra virtude tem conceito atual, muito influenciado pelo cristianismo. Acreditavam os gregos que, a partir da vida em grupo, surgiam as interações e comunicações e o entendimento acerca do mundo e das coisas, indispensáveis à criação de conceitos comuns, partilhados por todos com objetivo e compreensão da mensagem que se deseja transmitir. (SILVA, A., 2013).

Para os gregos da Antiguidade, a pena do ostracismo servia para banir aqueles que eram nocivos à *polis* e justificava a necessidade do homem estar em comunidade. Assim, os homens existiam enquanto seres sociais, e deixar de fazer

parte da comunidade era tão temido pelos gregos que o filósofo Sócrates preferiu a morte ao exílio.

Desde Aristóteles, o homem busca a felicidade, e esta felicidade advinha das virtudes. O que era central na ética antiga era a comunidade, questionava-se o comportamento dos homens em relação aos outros, como se comportar para viver bem em relação ao outro. Por isso, o ético em Aristóteles é entendido a partir do *ethos* (do costume), da maneira concreta de viver vigente na sociedade. O *ethos* que funciona como elo entre as esferas jurídica e política. (SILVA, A., 2013).

Os filósofos estoicos foram os primeiros a formular uma teoria sobre a uniformização de tratamento universalista. O filósofo Thomas Hobbes (1588-1679), contrário à ética antiga de Aristóteles, apresenta em sua obra *O Leviatã* os principais aspectos desse momento da história.

Defensor do absolutismo estatal, Hobbes criou em *O Leviatã*³⁸ uma teoria que fundamenta a necessidade de um Estado soberano como forma de manter a paz civil. Nesta obra, *O Leviatã*, Hobbes elabora sua filosofia sobre a natureza humana, sobre a necessidade de governos e sociedade.

Para melhor elucidar sua linha de pensamento, realiza a construção hipotética de uma fase pré-estatal, constituindo-se esta em um momento do convívio humano onde não há autoridade e onde tudo é de todos. Foi a chamada fase do “estado natural”. Essa fase do “estado natural das coisas” se caracterizava na seara processual como um estágio primitivo, onde predominava a chamada “autotutela”. Neste período, o indivíduo era guiado pelos próprios instintos e realizava a sua vontade perante outro indivíduo, utilizando-se de sua própria força. Seguindo a linha de pensamento dos adeptos da doutrina do chamado “Direito Natural”, existem determinadas regras que são inerentes à condição humana e que decorrem da necessidade primordial de sobrevivência, sendo estas anteriores a qualquer regramento normativo. A origem de todo conhecimento está na sensação. (HOBBS, 1983).

De pensamento racionalista e materialista, Hobbes encontrava explicação para tudo na ideia de movimento. Compreendia o mundo psicológico, o mundo moral e o mundo político a partir das premissas instituídas pela física.

³⁸ Leviatã é um monstro bíblico citado no livro de Jó, 40-41, muito poderoso, sem medo de nada e com um coração de pedra. Disponível em: <http://www.filosofia.com.br/historia_show.php?id=77>. Acesso em: 19 abr. 2014.

Sobre a natureza humana, Hobbes afirma que o homem é um ser naturalmente egoísta e seu individualismo na busca incessante pela realização de seus anseios é que gera o movimento, o início de tudo. Para ele, do movimento, nasce a sensação: apetite ou desejo, aversão ou ódio, constituem o começo do esforço em direção a alguma coisa ou para longe de alguma coisa. O objeto do apetite ou desejo é o bem; o objeto da aversão ou do ódio é o mal. A vontade, o ato de querer, não é mais do que “o último apetite na deliberação”, que se encerra em um fazer ou não fazer. Segundo Hobbes, o movimento do homem segue sempre na direção do seu maior desejo, a felicidade, e esta se realiza no poder, como condição para alcançar a felicidade, manifestada na forma de riqueza, honra e ciência. Na fase do estado natural, sempre na busca pelo poder, havia uma guerra perpétua de “cada um contra cada um” e de “todos contra todos”. Todo homem é concorrente de outro homem. Na teoria de Hobbes, nas relações entre os homens estão intrínsecas a concorrência, a desconfiança recíproca, a avidez de glória ou de fama, para ele, o interesse e o medo são o princípio da sociedade. (HOBBS, 1992).

Portanto, no pensamento Hobbiano, a fase do “estado natural” se consubstancia em uma fase pré-estatal, onde o homem, individualista e introspectivo, é guiado pelos seus próprios interesses, subjugando o outro à sua vontade, utilizando-se para isso de todos os meios que lhe aprouverem, sendo, desta forma, o homem o próprio lobo do homem, e por isso era necessário um governo forte (absolutista) para apaziguar os conflitos humanos e que a guerra de todos contra todos só seria evitada através do contrato social

Aristóteles afirmava que o homem é, naturalmente, sociável. Hobbes ao contrário, entendia que a natureza não colocou no homem o instinto da sociabilidade. Com efeito, o homem só busca o social por necessidade e a sociedade política é consequência artificial de um pacto voluntário, em benefício do próprio interesse individual e egoísta do homem.

Com o Iluminismo, a razão é mais importante, o homem é o centro de tudo. Valoriza-se a disciplina, o autocontrole, um mundo mais racional, descartam-se as sensações que enganam sempre. “Penso, logo existo”, segundo Descartes, representa a lógica do pensamento temático, consciente. Contudo, houve um certo desencantamento do homem apenas como consequência da sua racionalidade. (SILVA, A., 2013).

A industrialização trouxe vários problemas, inclusive a violência e o aumento da criminalidade. Importantes filósofos teorizaram sobre a natureza humana, a ética no convívio social, a exemplo de Kant, filósofo do século XVIII que elabora a teorização entre direito natural e direito positivo, mas se recusa a aceitar a existência de uma força superior. Para Kant, nem Deus nem o cosmo conduzem a vida do homem, o próprio homem é o legislador do mundo. A ética e a moral fazem parte da própria racionalidade humana. O homem aspira à felicidade, o que é normal, mas tudo vem do próprio homem. A ética kantiana está centrada na noção de dever imperativo e categórico, avançando de uma ética local para uma ética de caráter universal. A ciência do Ethos sofreu grandes transformações na história da humanidade e, ao contrário da ética aristotélica, a ética moderna está centrada no indivíduo. (KANT, 2008).

A crise ética da contemporaneidade tem levado a questionamentos acerca da fluidez, a incerteza, a descrença nos valores, a crise ambiental, as disparidades entre países ricos e pobres e uma série de acontecimentos que têm apontado que não se deve insistir na ética individualista, mas se deve abrir a tendência da retomada dos valores da ética antiga, centrada no coletivo, na comunidade, com certas nuances modernas.

A ética da mundialidade apoia-se na responsabilidade humanitária para com o outro, para com o estrangeiro. Os avanços tecnológicos propiciam o enfrentamento do problema social decorrente do individualismo e da indiferença social. A questão do estrangeiro e das discriminações de raça e de gênero são repensadas. Surge o discurso da inclusão. Esses discursos político e social emergem com a crise da civilização moderna, já que as promessas da modernidade não foram concretizadas no que se refere a trazer o progresso, conforto e segurança aos excluídos, aos outros. Por isso, tão em voga os discursos e políticas de inclusão destinadas aos portadores de necessidades especiais, negros, índios, mulheres, homossexuais. (SILVA, A., 2013).

Vale lembrar que a ideia da ética comum a todos os povos surgiu com os gregos antigos. Os estoicos conceberam a teoria da ética universalista. O Apóstolo Paulo formou a teoria do cosmopolitismo e igualdade em Jesus Cristo. Cícero, senador romano, também teorizou sobre a ética universal, apoiada na ação sob um *logos*, universal. (SILVA, A., 2013).

Para um dos principais filósofos e sociólogos do século XX, o alemão Jürgen Habermas, a ética do discurso baseia-se na linguagem e seu poder argumentativo, com função eminentemente comunicativa, destinada às relações intersubjetivas, cuja fundamentação ética é capaz de situar os sujeitos na perspectiva de uma comunidade comunicativa mundial de variados grupos.

A ética do discurso é a tentativa de estruturar uma teoria da racionalidade amparada naquilo que Apel e Habermas chamam de “razão comunicativa”, a qual não é apenas uma denúncia contra a “razão instrumental”, mas uma proposta de uma ética do “viver bem”, da “felicidade” e da “solidariedade” entre indivíduos capazes de linguagem e ação. (ZANELLA, 2012, p. 131).

O núcleo da teoria habermasiana está no consenso como modelo ético para o entendimento, considerando que, apesar dos desejos e diferenças, deve-se aceitar como princípio as diferenças, as opiniões contrárias, exercitando a tolerância, para a convivência pública, de arena, abrindo-se para outras culturas. Já Derrida, filósofo argelino, que viveu na França, critica a teoria procedimental da tolerância de Habermas, para a convivência com outras culturas, substituindo o discurso da tolerância pela hospitalidade. Neste contexto apregoam-se as ideias dos filósofos Habermas e Derrida sobre a ética contemporânea. Habermas confia no progresso da ética e em face da civilização universal, que entende ser possível o consenso, apesar das diferenças. (SILVA, A., 2013).

Hodiernamente vive-se a crise de paradigma moderno da política e da cultura, busca-se, para além do nacionalismo e do cosmopolitismo, depois do fenômeno da globalização, “a reinvenção da morada do *ethos*” . (SILVA, A., 2013).

E sobre a importância da filosofia no auxílio dos grandes dilemas da humanidade, voltados a descortinar novos horizontes culturais e filosóficos, merecem destaques as observações do filósofo brasileiro Miguel Reale (2002, p. 8):

A Filosofia não existiria se todos os filósofos culminassem em conclusões uniformes, idênticas. A Filosofia é, ao contrário, uma atividade perene do espírito ditada pelo desejo de renovar-se sempre a universalidade de certos problemas, embora, é claro, as diversas situações de lugar e de tempo possam condicionar a formulação diversa de antigas perguntas: o que distingue, porém, a Filosofia é que as perguntas formuladas por Platão ou Aristóteles, Descartes ou Kant, não perdem a sua atualidade, visto possuírem um significado universal, que ultrapassa os horizontes dos ciclos históricos. A universalidade da Filosofia está de certa forma mais nos problemas do que nas soluções, o que não deve causar estranheza se lembrarmos, com Jorge Simmel, que a Filosofia mesma é, por assim dizer, o primeiro de seus problemas, revertendo o seu problematismo sobre a sua

própria essência. A pesquisa das razões últimas das coisas e dos primeiros princípios implica a possibilidade de soluções diversas e de teorias contrastantes, sem que isto signifique o desconhecimento de verdades universais que se imponham ao espírito com a força irrefragável da evidência.

Num olhar sobre a filosofia dos grandes pensadores, pode-se perceber que o homem sempre buscou o conhecimento, a felicidade e compreender suas angústias e frustrações diante dos conflitos que o cercam.

A sabedoria emanada da filosofia é um solo fértil para a formação cultural da geração tragada pelas novas tecnologias. Neste passo, é preciso levar essas questões aos usuários do ciberespaço, possíveis integrantes de uma cibercultura, com argumentos que convençam que, para além do significado da internet livre, há que se cultivar os altos valores da boa convivência, onde se exercitam com ética a solidariedade e o compartilhamento da vivência que eleva o espírito, o cuidado e a valorização do outro.

Ressalte-se, mais uma vez, que a explosão das tecnologias de informação multiplicou, em muitas vezes, as capacidades de comunicação, o que as torna um veículo de comunicação social alcançável pelas camadas mais desprovidas economicamente, de pouca escolaridade, além de ser acessível às pessoas portadoras de necessidades especiais, tornando-as, ainda, um bem socialmente democrático, inclusivo, um espaço plural e aberto ao estabelecimento de contatos entre pessoas e comunidades de perfil cultural diversificado.

É inegável que a internet, um veículo democrático de comunicação, com suas ferramentas operacionais de relativa simplicidade, oportuniza a acessibilidade não apenas àquelas pessoas mais especializadas, como cientistas, pesquisadores, jornalistas, professores, estudantes, etc., mas abre um mundo fantástico de possibilidades para todas as pessoas, em qualquer rincão do mundo, que tenham, em sua mão, um computador conectado à rede mundial de computadores.

Esta maravilha é uma conquista da humanidade que deve permanecer livre, disponível e sem as amarras ideológicas de falsos donos da verdade e do saber, ou em nome de uma crença maniqueísta. E, ao lado dos evidentes benefícios, a utilização da *World Wide Web* ("WWW"), pode trazer uma enormidade de problemas relacionados ao uso maléfico por internautas e organizações criminosas, o que não elimina ou inviabiliza sua utilização para os fins da felicidade dos homens e sustentabilidade do planeta onde temos nosso etos.

É irreversível e inexorável o atual estágio de desenvolvimento tecnológico, não se pode prescindir das novas tecnologias, porquanto possuem força impulsionadora da criatividade humana, e elevam a busca de novas descobertas voltadas ao bem-estar da humanidade, ao tempo em que permitem a fluidez de uma convivência cibernética, aproximando pessoas e comunidades virtuais.

É preciso e possível propalar nessa convivência virtual as mesmas bases da convivência real, que exige conduta respeitosa, cuidadosa, ética, honesta, como esteio sólido e confiável destinados à formação de vínculos, cujos elos possam passar do contato superficial e penetrar, na esfera da subjetividade de cada internauta, o sentimento de amizade, ajuda mútua e solidariedade social, fortalecendo os direitos humanos e respeitando a dignidade e as peculiaridades de cada cultura.

O livre fluxo de informações científicas, artísticas, culturais ou de puro lazer confere a internet um espaço plural, democrático, contemporaneamente e indispensável ao crescimento educacional, à democracia e às transformações culturais do mundo conectado, respeitando e fortalecendo o pluralismo e a diversidade, contribuindo, ainda, para o combate às desigualdades.

Do mesmo modo que, ao lado da espetacular velocidade das informações, cresceram as dificuldades de controlar as relações sociais, e, conseqüentemente, os fluxos ilícitos, é preciso e emergente intensificar a disseminação de uma cultura ética perante a *web*, acreditando na rapidez e no poder transformador das informações massivas, de caráter educacional ético, de linguagem simples que possa atingir um nível de conscientização transformador, calcados nas mensagens de acolhimento, de respeito à diversidade, tolerância nos choques de opiniões, hospitalidade, consenso, gentileza, cortesia, valores voltados à convivência pautada nos princípios universais de não lesar o outro, da alteridade com liberdade, que respeitam e observam o limite do outro.

O desenvolvimento de políticas socioeducativas e culturais destinadas aos internautas desviantes pode ser o caminho do bom aprendizado, da transformação e da socialização. Do mesmo modo que, através do convívio com uma cultura delinquente se produz associação e aprendizado de condutas criminosas, é perfeitamente possível reeducar o desviante de forma pedagógica, enfatizando-se os valores humanos, as questões éticas, da civilidade, da boa convivência em sociedade, valores que poderão ser perfeitamente internalizados, absorvidos e

aprendidos, o que poderá surtir efeitos mais eficazes e permanentes do que a prevenção baseada apenas na finalidade repressiva, do controle social, através do cárcere que não ressocializa.

Nesse contexto, é da alçada das agências estatais competentes a adoção de políticas públicas de prevenção, com desenvolvimento de programas educacionais de ética informacional, iniciadas desde o ensino fundamental e universalizada para todos os setores profissionais e internautas, em geral, fundamentadas nos elevados valores humanos, que possam servir como pilares na formação de novos paradigmas, de uma cibercultura plural, universalista, inclusiva, sociologicamente solidária e ética, tornando-se menos vulnerável à ciberdelinquência.

5.3.3 Política de solução de conflitos nas relações virtuais

Neste capítulo, abordaremos a jurisdição estatal e a dinâmica dos conflitos no ciberespaço, ponderando-se sobre as perspectivas da desjudicialização dos conflitos cibernéticos. Este estudo apresenta importante componente para a discussão de política de prevenção ao cibercrime.

Constitui grande desafio estabelecer uma política de prevenção da criminalidade no ciberespaço, considerando a grande complexidade das relações neste âmbito, que, além de ser um ambiente que funciona com alta tecnologia, desafia qualquer controle mais rígido, tendo em vista os pilares sobre os quais estão assentados os princípios da rede mundial de computadores, da universalidade, da liberdade de expressão, da privacidade, da diversidade e neutralidade da rede, bem como da “inimputabilidade da rede”.

No que diz respeito à “inimputabilidade da rede”, apregoa o Comitê Gestor da Internet no Brasil - CGIbr (www.cgi.br), que o

combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos. (COMITÊ GESTOR DA INTERNET NO BRASIL, 2012).

Na medida em que se universaliza o acesso à rede mundial de computadores, se intensificam as relações no ciberespaço, ao tempo em que, na mesma proporção,

crecem as condutas inescrupulosas, dando origem aos delitos e aos mais variados conflitos.

Embora exista na própria *web* intensa campanha por uma internet livre e ética, os ilícitos cibernéticos atingem indiscriminadamente a todos usuários, sejam entes públicos e privados ou o cidadão internauta, todos indistintamente protagonistas de inexorável vulnerabilidade, sujeitos aos mais variados e inesperados ataques de delinquentes cibernéticos, ou a diminutas infrações, os quais geram os diversos conflitos. Nesse diapasão, o controle social da nova criminalidade no âmbito do ciberespaço constitui verdadeiro desafio para a soberania dos Estados, considerando a ordem jurídica estabelecida internamente e a jurisdição internacional.

Segundo Ferreira (2010, p. 21), o fenômeno da globalização gerou grande interferência nas relações internacionais e no Direito Internacional Público, asseverando, também, a autora que essas interferências criaram a necessidade de “se redefinir conceitos até então enraizados, como o de soberania, jurisdição, competência, eficácia da lei no espaço, todos flexionados pelo surgimento de uma macrocriminalidade, que invade searas até então desconhecidas ou inimagináveis.”

O limite desta pesquisa está voltado para o problema específico da política criminal de prevenção da cibercriminalidade, ficando o enfoque sobre o controle repressivo arremetido para o capítulo que tratamos dos tipos penais de cibercrime.

Tradicionalmente, os conflitos são levados à Jurisdição, enquanto Poder e monopólio do Estado. O Poder Judiciário tem a primazia constitucional na solução dos conflitos gerados na sociedade. Contudo, neste limiar do novo século, surgem movimentos no sentido da desjudicialização de determinadas demandas, reservando a jurisdição estatal para as questões não solucionadas por vias alternativas de solução de conflitos e para as questões de grande relevância do direito discutido, de interesse do Estado ou que envolvam direitos difusos e coletivos.

O conflito é visto como fato natural da vida em sociedade que permeia, inexoravelmente, as relações humanas. Segundo Deutsch, citado por Azevedo (2013, p. 47), o conflito pode contribuir positivamente com as relações e, se abordados com técnicas adequadas, pode ser um importante meio de crescimento pessoal, profissional e organizacional, podendo também impulsionar relevantes alterações quanto à responsabilidade e à ética profissional.

O princípio da inafastabilidade da tutela jurisdicional ou, simplesmente, princípio da inafastabilidade, previsto no inc. XXXV do art. 5º da Constituição Federal, preceitua que a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça ao direito. A garantia constitucional do controle jurisdicional assegura a todos o direito de acesso à justiça e à universalização da tutela jurisdicional, porque nenhuma lei ou convenção pode impedir que qualquer conflito seja apreciado pelo Judiciário.

Impera esclarecer que, na prática, o acesso à Justiça é dificultado por várias razões de ordem política, social e jurídica, largamente descortinadas pelo movimento de acesso à justiça, apontando os vários obstáculos que dificultam ou impedem esse acesso à justiça, dentre os quais enumera-se a pobreza, a falta de informação, alto custo do processo, procedimentos morosos e inadequados, organização dos serviços judiciários e legislação ultrapassada, insuficiência de recursos financeiros para a capacitação de juízes e funcionários, além de aparelhamento e modernização dos serviços judiciários, dentre outros. (MARINONI, 1994, p. 67).

Nestas circunstâncias, a entrega da tutela jurisdicional pelo Estado, que proibiu a autotutela, está longe de cumprir a promessa constitucional de uma tutela jurisdicional adequada, tempestiva, a ser efetiva, capaz de solucionar os diversos conflitos de interesses postos em juízo, de forma mais reparadora ou preventiva, com vista à pacificação social. Portanto, já que o Estado se obrigou a prestar a tutela jurisdicional, deve entregá-la da forma mais adequada possível.

Tendo monopolizado a jurisdição, tornou-se um grande desafio para o Estado a busca de uma adequada tutela jurisdicional a todos os conflitos de interesses, sejam conflitos individuais ou coletivos, emergentes do ambiente social. A princípio, todos esses conflitos são jurisdicionalizáveis.

A Constituição Federal de 1988, a democratização das instituições, o surgimento de novos direitos individuais, difusos e coletivos e os chamados direitos de terceira geração, que atravessam a visão individualista, superando a separação entre o público e o privado, dos quais se cita, como exemplo, os direitos da família, dos adolescentes, dos jovens, o respeito aos idosos, entre outros, enquanto coletividade a merecer maior atenção e proteção, diretos ligados à etnia, à nação, à identidade, ao gênero e à própria humanidade, como o direito à paz, o de

autodeterminação dos povos e direito a um ambiente preservado, sustentável, ao desenvolvimento social e econômico, etc.

Além da excessiva judicialização dos mais variados conflitos, do simples ao mais complexo, a questão orçamentária do poder judiciário e o despreparo e ausência de políticas que levassem à estrutura funcional e administrativa a abarcar a excessiva quantidade, milhares e até milhões de processos anualmente ajuizados, ocasionaram o colapso do sistema jurisdicional, que já sofria de grande lentidão, não obstante as recentes e profundas atualizações das normas processuais.

Com a ampliação dos direitos, houve a crescente invasão do Direito na organização da vida social e política, levando a judicialização das mais diversificadas demandas, na medida em que foram positivados novos direitos fundamentais e sociais, gerando, em consequência, o fenômeno que os neoconstitucionalistas convencionaram denominar de ativismo judicial, com a efetivação de atividades próprias de políticas públicas diante da omissão estatal. Ademais, o fenômeno da nova hermenêutica constitucional, bem como a compreensão da contemporânea tendência da constitucionalização do Direito, repercutiu, especialmente, para a Jurisdição.

A Jurisdição, como manifestação do poder do Estado, que é uno, só se manifesta quando é provocada, vez que é função estatal inerte - *nemo index actore ou ne procedat index ex officio*. A ação processual é a contrapartida que o Estado ofereceu ao cidadão quando proibiu a autotutela.

Assim, na ocorrência do conflito de interesses, surge para aquele que sofreu lesão ou ameaça de lesão o direito de exigir do Estado a tutela jurisdicional, para pacificação e solução que o conflito requer, através do direito de ação, seja ela ação civil ou penal.

Os avanços tecnológicos impulsionaram a criação e implantação do processo judicial eletrônico, previsto na Lei n.º 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial, tendo o Brasil despontado como protagonista de um novo modelo de processo judicial, dispensando os autos físicos de papel, se desenvolvendo em ambiente eletrônico de forma totalmente virtual.

Constitui política da Justiça brasileira, especialmente do Conselho Nacional de Justiça, implantar essa nova modalidade de processo em todo território nacional, não obstante os avanços do processo judicial eletrônico, que já está em pleno funcionamento em tribunais do País e em franca implantação em todas as

comarcas, nos mais longínquos municípios, mas o problema da morosidade continua o mesmo de alguns anos atrás. Em trabalho monográfico, tivemos a oportunidade de escrever sobre a morosidade da Justiça e nessa oportunidade ressaltamos:

Várias são as causas da lentidão da justiça, algumas sociais, outras políticas e outras jurídicas. Os nossos dois sistemas processuais, civil e penal, são frutos do positivismo dogmático, com parte de seus institutos que não mais corresponde aos anseios da sociedade moderna, com termos e prazos ultrapassados, incompatíveis com o momento atual.

O tempo e o custo do processo devem ser sempre considerados. O processo que se arrasta ao longo do tempo, traduz uma justiça cara e inacessível para o hipossuficiente que não possui ao seu alcance instrumentos que façam valer seu direito de igualdade substancial, especialmente quando litigam com outra parte economicamente mais forte, mesmo que amparada pela assistência judiciária.

O mesmo deve ser dito da organização judiciária, carente de reestruturação, para a modernização e informatização dos serviços, além da melhor capacitação e valorização dos funcionários, e ampliação do número de juízes, sem falar na necessidade de se estruturar e organizar as Defensorias Públicas em todas as comarcas, além da diversificação e aumento do número de juizados especiais. (KUNRATH, 1995, p. 11).

Apesar dos esforços dos poderes constituídos, especialmente do Poder Judiciário, a despeito do processo eletrônico ser um grande avanço e contribuir sobremaneira para a tempestividade da resposta jurisdicional, a multiplicidade de demandas, sobretudo envolvendo fraudes eletrônicas nos sistemas bancários, financeiros e no comércio eletrônico de bens de consumo, abarrotada, especialmente, os Juizados Especiais Cíveis, visando principalmente a indenizações reparatórias. Ademais, as ocorrências de ataques cibernéticos e dos crimes comuns praticados através da internet, sobrecarregam a Justiça criminal.

Todos esses fatores culminam com uma excessiva judicialização de conflitos através do direito de ação, congestionando toda a estrutura da jurisdição estatal, o que deixa em evidência a necessidade e urgência de se buscar outras alternativas para soluções de diversas lides sociais.

Conquanto seja possível afirmar que a ampliação dos direitos, a universalização do acesso à Justiça, aliados ao fenômeno da alta conflituosidade da sociedade brasileira hodierna, conduziram a excessiva judicialização de demandas que, do mesmo modo, afigura-se, também, possível constatar que a ideia da solução judicializada é absolutamente aceita pelas instituições estatais e pela sociedade, o que leva à resistência a mudança desse paradigma.

A visão monista de que o Judiciário é o centro efetivo da harmonização e pacificação social limita a percepção de que outros campos sociais são igualmente capazes de encontrar solução para seus conflitos. Cindir este paradigma consiste, exatamente, em difundir uma nova concepção no sentido da implantação de programas voltados à produção de solução negociada de conflitos, que não provenha dos próprios órgãos de jurisdição.

5.3.3.1 Desjudicialização e a reserva da jurisdição

Em sentido contrário, no contexto da judicialização, surge como alternativa para solução dos conflitos excessivamente judicializados, com o mesmo escopo de pacificação social, o movimento da **desjudicialização**, como perspectiva viável e factível, mas que, por representar uma quebra de paradigma, encontra certa resistência, sobretudo, no campo jurídico.

A concepção monista da produção do direito se constitui zona de resistência a uma filosofia de ampliação dos meios de resolução de disputas fora da Justiça oficial. Na visão que reconhece o monopólio estatal sobre o direito da sociedade, não há lugar para um processo que não seja o judicial, independentemente da complexidade ou singeleza da questão. O direito processual contemporâneo é repositório dos conflitos decorrentes dessa tensão, e por mais que evolua, em pleno funcionamento o processo virtual em muitos tribunais e comarcas, não há estrutura física e funcional que faça triunfar a tão sonhada Justiça tempestiva, justa e efetiva.

O monopólio do Estado na criação de normas e da jurisdição tem se mostrado socialmente insuficiente para abarcar os meios de pacificação da crescente conflituosidade da hodierna sociedade brasileira, bastando uma breve retrospectiva acerca da jurisdição no Brasil para ser possível visualizar desde a adoção do modelo colonial português, até os dias atuais, as diversas crises pelas quais passam os modelos adotados.

Na estrutura judicial da Colônia, os portugueses consideravam a Administração da Justiça o atributo mais importante do governo que tinha como marco legal as Ordenações Portuguesas. As Ordenações Afonsinas (1500-1514), Manuelinas (1514-1603) e as Ordenações Filipinas (1603) eram compilações que

ditavam o direito oficial português, onde se previam as fontes subsidiárias, o direito romano, o direito canônico, em ordem sucessiva. A última, as Ordenações Filipinas, tiveram vigência no Brasil de 1603 até 1916, ao lado de leis locais esparsas, até o advento do Código Civil de 1916. O modelo colonial das Ordenações Portuguesas sofreu a crise de legitimidade, considerando que o arcabouço jurídico e jurisdicional era absolutamente dissociado do direito nativo indígena, cuja cultura e costumes em nada influenciaram a Administração da Justiça na Colônia e nos primeiros anos da República. (LOPES, 2002).

Na fase republicana, da Primeira República, o Poder Judiciário começou a dar seus primeiros passos no sentido de criação de um corpo normativo próprio, alicerçado no direito europeu, especialmente, no direito italiano. No entanto, o modelo adotado era incipiente e poucos membros da sociedade tinham acesso à Jurisdição obtendo, na Segunda República, alguns avanços com as legislações civil, processual civil e penal, mais adaptadas à realidade social brasileira. Todavia, ainda calcada no direito europeu, especialmente, no direito italiano e alemão.

Por último, inaugura-se o atual modelo alicerçado pela Constituição de 1988, com um forte arcabouço principiológico constitucional, de amplo leque de propósitos de universalização e ampliação do acesso à Justiça, porém permeado de dificuldades, o que se pode definir como crise de efetividade.

Aqui merece lembrar que, no decorrer do Século XX, na linha das tendências mundiais, o ordenamento jurídico brasileiro sofreu significativas mudanças com o declínio do Estado liberal individualista do Século XIX, passando a adotar novas perspectivas principiológicas, ingressando no chamado Estado de Direito, abarcando uma postura mais intervencionista, própria de um Estado Social, evoluindo para o atual Estado Democrático, suplantado na preservação da vontade popular, liberdade e igualdade, enfim nos ideais democráticos, sem maiores ingerências estatais, visando a oferecer maior proteção aos cidadãos (DALLARI, 2007, p. 145).

As promessas e legados da modernidade, do Estado Democrático de Direito, segundo Streck (2011), nunca se concretizaram no Brasil. O Direito, segundo este autor (ibid.), como um dos principais legados, “ — visto como transformação social, e não como obstáculo às mudanças sociais — ”, encontrou guarida na Constituição de 1988, apenas no sentido formal, porém longe de ser efetivado. Existe uma imensa dívida social a ser resgatada, ressaltando que o Estado Social-Providência, ainda

não ocorreu em terras brasileiras. De acordo com Lenio Streck, em sua obra *Hermenêutica Jurídica e(m) Crise: uma exploração hermenêutica da construção do Direito*, caminha-se na direção de novos paradigmas:

A modernidade “propôs uma dupla possibilidade para a humanidade. Uma delas, a realização da razão, seria o desenvolvimento universal para um sistema social que concretizasse o princípio da “igualdade formal”, através da crescente redução das desigualdades reais do mundo moderno. Tal não aconteceu. Ao contrário, *o que ocorreu foi a pós-modernidade aprofundar a irracionalidade, aumentar as diferenças sociais e consolidar relações cada vez mais alienadas*. Foi isso que os homens modernos fizeram da sua história. A razão foi ‘assaltada’ no sentido de ser despida de sua vocação humanizadora.” (STRECK, 2011, p. 299).

A ideia do monopólio da jurisdição decorreu dos valores do positivismo como garantia contra os abusos do Estado, do próprio Estado totalitário e, dentro desta lógica, nasceu a cultura jurídica brasileira baseada numa tradição monista, positivista, lógico-formal, que está em crise, pois há novos problemas e não existem novas soluções. (WOLKMER, 2002).

No Brasil, embora a jurisdição sempre tenha sido uma importante função estatal, desde as Capitanias Hereditárias, o Estado sempre teve dificuldade de universalizar o acesso à Justiça. Vale aqui destacar o estudo crítico desenvolvido no início da década de 70, pelo sociológico Boaventura de Souza Santos (1985), a respeito das relações de poder interno entre os cidadãos moradores de uma favela do Rio de Janeiro e as relações entre esses moradores e as instituições estatais, na obra intitulada *Notas sobre a história jurídico-social de Pasárgada*.

Santos (1985), no citado ensaio, empresta a esse lugar um nome fictício de Pasárgada. O referido sociólogo descreve seu objeto de estudo com estrutura social diversa da cidade onde está localizada, um território com diversas ocupações ilegais, onde vigora um direito não oficial, um direito próprio de Pasárgada em paralelo ao direito oficial brasileiro.

O estudo propôs-se a analisar a situação de pluralismo jurídico com vistas à elaboração de uma teoria sobre as relações entre Estado e Direito nas sociedades capitalistas, sob a contestação de que, no mesmo espaço geopolítico, vigoravam mais de uma ordem jurídica e a resolução de certos conflitos era submetido à sua própria normatividade, criada em decorrência da ausência estatal, da inacessibilidade de seus moradores para a solução de seus conflitos, como as questões de posse, construções de habitação (casas, barracos), sob um contexto

próprio decorrente das condições econômicas e da presença da delinquência e da violência invisíveis aos órgãos de controle social.

Ressalta Santos (1985) que a inacessibilidade aos juízes e tribunais, pelas classes mais baixas, evidencia a natureza classista do aparelho jurídico, típico das sociedades capitalistas. O aumento da violência, nessa época, decorreu de diversos fatores, dentre os quais a desconfiança na atuação da força policial em relação aos moradores, estereotipados como criminosos e malfeitores, habitantes daquele lugar, onde eram frequentes as buscas intimidadoras naquele território. Razão pela qual a polícia continua a desempenhar um papel mínimo na prevenção e resolução de conflitos, sendo vista como uma força hostil por parte da comunidade.

Os entrevistados consideravam-se "ilegais", não somente na ocupação do espaço onde construíram suas moradias (barracos), mas sobre todas as relações sociais, enquanto habitantes da favela (Pasárgada). A autodeclaração de ilegalidade, por parte dos habitantes, demonstra a ambiguidade da consciência popular acerca dos próprios direitos, numa demonstração clara que, de um lado, está o direito formal, reduzido a códigos e leis, e, de outro, um direito daqueles de condições inferiores.

A indisponibilidade dos mecanismos oficiais de controle e a ausência de mecanismos não oficiais, na época do processo de formação da comunidade, criaram uma situação de "privatização possessiva do direito", caracterizada pela produção individual na aplicação das normas que regem a conduta social. No momento em que havia divergências entre esses centros, os conflitos tomavam proporções maiores, atingindo todas as relações sociais entre as partes conflitantes, criando-se uma situação onde a violência determinava a superação do conflito.

Conclui o autor que a inacessibilidade dos mecanismos de defesa oficiais de controle social poderia ser evitada se, na própria comunidade, desenvolvesse mecanismos internos, capazes de solucionar conflitos frequentes entre os moradores. Ilustrada a questão do pluralismo do direito no exemplo de Pasárgada, anos após esse ensaio de Santos (1985), observam-se que as contínuas transformações sociais não se coadunam mais com a concepção monista das fontes do direito.

Sob o prisma do pluralismo jurídico, em antagonismo ao monismo jurídico, propugna-se o problema da insuficiência da lei (estatal), bem como a superação dos limites da autoridade estatal, em uma sociedade plural, contendo variados centros

de poder e de conflitos. Assim, sem deslegitimar o Poder Judiciário, ou limitar seu poder jurisdicional, diante das contínuas transformações sociais, que não comportam mais um único órgão a tutelar seus direitos, é preciso voltar-se para outras formas aliadas de resolução de litígios. A realidade social abarca outros instrumentos, além do processo judicial, como instrumento de defesa social.

Observe-se que essas alternativas não suprimem nem desprestigiam as decisões judiciais, sobretudo as decisões que não podem ser delegadas em matérias de grande relevância do direito discutido, como nos casos das ações constitucionais ou grave violação dos direitos à liberdade e à vida, merecendo nestes aspectos a reserva da jurisdição. O constitucionalista português Canotilho (2003) refere-se aos princípios da reserva de juiz e da reserva de tribunal, na atuação da jurisdição, asseverando que:

Relativamente a algumas situações é legítima a intervenção de outros poderes (designadamente administrativos) desde que seja assegurado depois o direito de acesso aos tribunais. Na reserva de juiz, o tribunal intervém logo no início; na reserva de tribunal o apelo aos juízes ocorre, a maior parte das vezes, sob a forma de recurso. Dito por outras palavras: na reserva de juiz verifica-se o monopólio total da função jurisdicional quanto à decisão de certas questões; na reserva de tribunal, o exercício da função jurisdicional é parcial, posto que no mais das vezes não se exige a intervenção inicial do juiz. (Canotilho, 2003, p. 665).

A Constituição da República Portuguesa prevê, no artigo 209º, 2, na parte que trata da organização dos tribunais, a permissão de criação de tribunais arbitrais e julgados de paz, competindo à lei determinar os casos e as formas em que esses tribunais não jurisdicionais podem ser constituídos.

O caráter jurisdicional na aplicação do direito, no caso concreto, deve ser opção do legislador na perspectiva da pertinência e adequação constitucional que irá delimitar o núcleo pétreo da reserva absoluta da jurisdição, ao passo que também pode diferir residualmente a solução de litígios a outros órgãos estatais ou não estatais, ressaltando-se, sempre, o princípio do controle jurisdicional.

A própria Constituição de 1988 adota o princípio do pluralismo em suas relações, baseada na construção de uma sociedade livre, justa, solidária, na igualdade, na prevalência dos direitos humanos, nos propósitos da erradicação da pobreza e da solução pacífica dos conflitos e defesa da paz. O desenvolvimento de políticas de crescimento da estrutura judicial pode trazer algum alento, a médio ou

longo prazo, entretanto, provavelmente, não irá solucionar o problema da morosidade.

A propalada crise do Judiciário perpassa, como já revelado, pelo fenômeno da judicialização dos conflitos. A intervenção judiciária mínima apresenta-se com real possibilidade de racionalizar a jurisdição, deixando para sua atuação, residualmente, os conflitos não resolvidos nas instâncias alternativas, os conflitos mais complexos e/ou socialmente relevantes e impactantes.

Processualistas do movimento instrumentalista, como Cândido Dinamarco e Ada Pellegrini Grinover, enfatizam os esforços dos processualistas comprometidos em encontrar soluções para a “crise da Justiça” que se posicionam em duas vertentes:

A vertente jurisdicional, com a tentativa de descomplicação do próprio processo, tornando-o mais ágil, mais rápido, mais direto, mais acessível, com relação à qual se fala em deformalização do processo. E a vertente extrajudicial, buscando-se por ela a deformalização das controvérsias, pelos equivalentes jurisdicionais, como vias alternativas ao processo. É nesta segunda perspectiva que se insere a revisitação da conciliação (autocomposição) e da arbitragem (heterocomposição). (CINTRA; GRINOVER; DINAMARCO, 1992, p. 175).

Abordando a problemática da reforma judiciária, em trabalho monográfico, Cesar Augusto dos Santos (2011), sintetiza com clareza que a Desjudicialização é o caminho alternativo, mas coadjuvante para amenizar o problema da superjudicialização das últimas duas décadas:

No decorrer do século XX, apresenta-se o fenômeno da judicialização consistente na canalização de todas as mazelas sociais que deságuam no Poder Judiciário, fortalecendo o ativismo judicial. Todavia, o acampamento de novos direitos, aliado aos novos moldes de procedimento judiciais, abriu as portas para novas formas de tutela decorrentes da vida político-social. Se, de certo modo, a judicialização trouxe melhoria incalculável à cidadania, por outro lado, exacerbou milhares de demandas a serem dirimidas jurisdicionalmente, tendo por consequência a malfadada morosidade e a ineficiência do atual sistema. Contextualizar a desjudicialização acaba por redescobrir o caminho para a busca da efetivação da justiça, realçando a temática do acesso à justiça, sob a ótica de novo século em harmonia com todas as novas modalidades de solução não jurisdicionais de conflito, tratados como meios alternativos de pacificação judicial. (SANTOS, C. 2011, p. 11).

Contudo, mesmo com os problemas de acesso e da demora da resposta da prestação jurisdicional, a sociedade brasileira desconhece ou simplesmente não confia em outros instrumentos de solução de conflitos que não provenham de uma

sentença judicial ou que não decorram da força coercitiva das leis. Ou ainda, que seja originado fora da estrutura institucionalizada dos tribunais oficialmente concebidos e destinados para este fim.

Essa postura da sociedade decorre da tradição cultural e do próprio campo jurídico, que constitui importante fator de resistência à ideia da desjudicialização. No item seguinte trataremos dessa problemática.

5.3.3.1.1 O campo jurídico contra a desjudicialização

As possíveis soluções dos conflitos são enfocadas, normalmente, a partir do estudo meramente técnico-dogmático do direito, ou seja, segundo a interpretação e a aplicação das normas jurídicas, operando-se a subsunção do caso concreto à norma jurídica, através da jurisdição.

Num primeiro plano, deve ser salientado o papel da jurisdição como função estatal, monopolizadora da dicção do direito, na ocorrência de demandas postas sob sua apreciação, constituindo direito fundamental o acesso à jurisdição, já que se proibiu a autotutela. Com efeito, outros mecanismos de pacificação de conflitos, sem a presença da Jurisdição estatal, não têm merecido maior aceitação por algumas razões, sobretudo, em virtude de não se adaptarem à lógica do campo jurídico. Assim, indaga-se: o que vem a ser campo jurídico?

A noção de campo jurídico será enfocada segundo a sociologia de Pierre Bourdieu, em sua obra *O Poder Simbólico*, especificamente, no capítulo VIII, dedicado ao tema *A força do direito: elementos para uma sociologia do campo jurídico*.

Para Bourdieu (2005), os discursos são carregados de poder social e causam efeitos reais sobre o mundo. Ele concebe a sociologia como a ciência do oculto, na medida em que busca desvelar o que está por trás do discurso ou de práticas. Cabe à sociologia desvendar e trazer à tona os verdadeiros sentidos e lógica que estão por trás das estruturas e relações sociais produzidas e exercidas num determinado campo social.

O campo jurídico, segundo Bourdieu (2005), constitui o lugar onde há concorrência pelo monopólio do direito de dizer o Direito, pelos agentes investidos de competência. Tais agentes possuem a capacidade reconhecida de interpretar um *corpus* de textos que consagra a visão legítima, justa, do mundo social.

O discurso jurídico é produzido a partir de um *habitus* linguístico do campo jurídico onde esses agentes se defrontam com a tendência de ditarem certos e determinados discursos estilizados e caracterizados, que lhes conferem uma competência técnica e uma capacidade social, ao mesmo tempo, para utilização em determinadas situações (BOURDIEU, 2005, p. 212).

É, pois, um campo que, pelo menos em período de equilíbrio, tende a funcionar como aparelho na medida em que a coesão dos *habitus* espontaneamente orquestrados dos intérpretes é aumentada pela disciplina de um corpo hierarquizado o qual põe em prática procedimentos codificados de resolução de conflitos entre os profissionais da resolução regulada dos conflitos". (BOURDIEU, 2005, p. 214).

A noção de campo, para Bourdieu (2005), surgiu com base na obra de Max Weber sobre o funcionamento do campo religioso, na qual aborda alguns conceitos e terminologias da ciência econômica, como mercado, capital, concorrência, monopólio, levando-o à percepção de que seria possível enfocar outros estudos para outros espaços sociais. E o campo jurídico seria um subcampo de uma espécie de campo social delimitado à atuação dos operadores do direito, ou profissionais que desenvolvem suas atividades.

Para o sociólogo francês, o surgimento de um campo social decorre de necessidades sociais, como resultado de um processo histórico e paulatino de formação e de busca de autonomização em relação às pressões externas do contexto, e que se desenvolve a partir do aparecimento de um grupo de agentes incumbidos e dedicados ao exercício de uma atividade profissional específica, a fim de atender ao surgimento de uma demanda social. (BOURDIEU, 2005).

Sob o enfoque de elementos da sociologia de Bourdieu, o Direito possui força que incide sobre o campo jurídico, fazendo com que a sociedade o aceite e o entenda como algo natural à sociedade. Porém, no que concerne aos profissionais e à divisão do trabalho jurídico dos operadores do direito (bacharéis, magistrados, advogados, promotores de justiça, defensores, procuradores, servidores da justiça, etc.), o campo jurídico representa seu mercado de trabalho, que deve ser preservado.

Do ângulo dos profissionais do direito, seus clientes, a sociedade e todo o aparato que servem àqueles que militam na esfera jurídica, há uma concepção de que estão investidos num poder expresso através de elementos da sociologia que, segundo Bourdieu (2005), podem ser identificados na linguagem, no *habitus*.

Esses simbolismos podem ser expressos na legitimação, na técnica e distribuição de competências, socialmente aceitas, destinadas à dialética jurídica voltada para a aplicação das normas jurídicas, conforme hermenêutica interna do próprio ordenamento jurídico. Para o sociólogo, o poder simbólico do qual o campo jurídico tende a preservar, pode levar a injustiças e violências, diante de dominação e hegemonia destes atores, da própria lógica de funcionamento das estruturas e relações sociais engendradas no campo jurídico. (BOURDIEU, 2005).

Noutras palavras, do exercício do poder simbólico decorre uma violência simbólica, ao passo que essa violência consiste na arbitrariedade e pessoalidade veladas e dissimuladas nas práticas dos agentes sociais do campo jurídico, desconhecida pelos sujeitos que estão submetidos a ela, ou seja, os jurisdicionados.

O campo jurídico, diante de seu simbolismo e poder, é, sem dúvida, um empecilho a uma mudança ou quebra de paradigma, enraizado num país de cultura do civil *law*, cuja concepção do campo jurídico sobreleva os interesses dos profissionais que atuam nesta área, sem qualquer disposição a mudanças.

Nesta abordagem, focada na visão sociológica de Bourdieu (2005), tem-se a pretensão de provocar a reflexão acerca da correlação entre o encastelamento da jurisdição e do campo jurídico na sociedade brasileira que opõe resistência a acolher, conceber e a implantar novas alternativas de solução de conflitos sociais, que não a Jurisdição estatal.

Permite-se asseverar que é equivocada a concepção de que todas as controvérsias devem ser dirimidas pelo Estado-juiz. Outros atores sociais, especialmente aqueles mais próximos das divergências sociais, são igualmente capazes de solucionar conflitos. O pensamento científico em crise decorreu do avanço e da pluralidade de condições teóricas e sociais, que a própria ciência proporcionou. O direito estatal alberga a necessidade do controle social, e se firma sobre as vertentes regulatórias restritivas das leis, do mercado e do próprio Estado.

No campo jurídico, o Estado Democrático de Direito trouxe com o novo constitucionalismo a quebra paradigmática do positivismo jurídico. O direito, como

ciência prática, não pode ser visto apenas como um corpo de normas em sua pureza jurídica do qual se abstrai o sentido metafísico dos valores axiológicos, sobretudo da moral e da ética. O resgate do mundo prático – facticidade – até então negado pelo positivismo, como pregavam os filósofos Kelsen e Hart. (STRECK, 2011, p. 376).

Em outra vertente, vale destacar a análise sociológica do sistema judiciário de Boaventura de Souza Santos (2007) em seu livro *Por uma Revolução Democrática da Justiça*, onde ressalta que se deve indagar se “poderá o direito ser emancipatório?”, enfocando suas observações sobre o continente latino-americano e, em particular, o Brasil, afirmando que, com o crescimento das desigualdades sociais e com a consciência social da sua injustiça, para as sociedades contemporâneas, são cada vez mais desiguais, assumindo novas facetas e dimensões.

Santos (2007) partiu da observação de que a revolução democrática do direito e da justiça só se faz, verdadeiramente, no âmbito de uma revolução mais ampla, que inclua a democratização do Estado e da sociedade, chamando a atenção para o fato de o direito, para ser exercido democraticamente, tem de se assentar numa cultura democrática, tanto mais preciosa quanto mais difícil são as condições em que ela se constrói, observando que tais condições são muito difíceis, ante a distância que separa os direitos das práticas sociais que, impunemente, os violam. (SANTOS, 2007, p 8).

Em sua análise extensiva, crítica e criativa dos principais vetores de refundação democrática do papel do direito e da justiça, tendo como ponto de partida as transformações sofridas pelos tribunais nas últimas décadas,

[...] a revolução democrática da justiça assenta na valorização da diversidade jurídica do mundo como mola propulsora do pensamento jurídico crítico. No âmbito do quadro teórico do que venho denominando sociologia das ausências e das emergências, sobressai um elemento subjetivo que balizou a elaboração deste livro: a consciência cosmopolita da existência de diferentes imaginários e práticas do direito no mundo e o inconformismo em face do desperdício da experiência da luta por direitos mais justos, mais acessíveis e mais inteligíveis.” (SANTOS, 2007, p. 8).

Com efeito, opondo-se ao senso comum dos operadores jurídicos, o autor em destaque apresenta posição epistemológica sobre o direito, partindo da visão da oposição existente entre regulação e emancipação, na busca de direitos mais justos,

através de uma “sociologia das ausências” em confronto com uma “sociologia das emergências”. (SANTOS, 2007, p. 9).

O ativismo dos movimentos sociais passa a exigir um processo de construção de um pensamento jurídico alternativo e crítico destinado a acudir as demandas populares, com as quais a dogmática jurídica não está acostumada, e que está a exigir uma visão ampla em defesa de seus direitos, bem como novos mecanismos de resolução de conflitos de interesses coletivos.

Outro aspecto a ser discutido consiste na falta de interlocução dos juízes para com profissionais de outros campos do conhecimento, como auxiliares de sua função pacificadora. As varas judiciais não estão acostumadas às decisões provenientes de equipes interdisciplinares. As sentenças são prolatadas segundo a técnica jurídica, sem a preocupação de resolução da lide sociológica, mas, apenas, aquela porção do conflito representado pela lide processual.

Nesta linha, observa Santos (2007) que, sob o enfoque sociólogo, merece reflexão a desconstrução do paradigma da resolução do conflito através da sentença judicial, questionando-se acerca da crença de que só o magistrado, por ser magistrado, tem competência para resolver litígios e de que, pela mesma razão, tem competência para resolver todos os litígios. Se a lei é o único fator na resolução dos litígios e o magistrado o seu intérprete fidedigno, uma vez que a lei é geral e universal, a competência do magistrado também deve ser geral e universal. A ideia de que é necessária uma competência genérica para resolver os litígios está ainda hoje muito enraizada. (SANTOS, 2007, p. 56).

Evidente que os atores do campo jurídico reagem a qualquer pensamento que desestabiliza ou leva a desconstruir o funcionamento pretensamente autônomo do sistema jurídico e judicial, acostumado à noção de neutralidade do direito e sua autonomia da política e moral.

Na perspectiva dessa problemática, do senso comum teórico, segundo Santos (2007, p. 57), a sociedade distancia-se da

cultura normativista técnico-burocrática. Nesta dimensão, o papel e a formação do magistrado assume importância, eis que, o magistrado em geral conhece bem o direito e a sua relação com os autos, mas não conhece a relação dos autos com a realidade. Não sabe espremer os processos até que eles destilem a sociedade, as violações de direitos humanos, as pessoas a sofrerem, as vidas injustiçadas. Como interpreta mal a realidade, o magistrado é presa fácil de ideias dominantes. Aliás, segundo a cultura dominante, o magistrado não deve ter sequer ideias próprias, deve é aplicar a lei.

Pontua, ainda, Boaventura Souza Santos (2007) que outros mitos, ou preconceitos, disseminados na nossa cultura judicial, levam a preferência por tudo o que é institucional, burocraticamente formatado, apontando que são os seguintes os sintomas mais evidentes:

Uma gestão burocrática dos processos, privilegiando-se a circulação à decisão – o chamado andamento aparente dos processos; a preferência por decisões processuais, em detrimento de decisões substantivas; a aversão a medidas alternativas, por exemplo, penas alternativas, por não estarem formatadas burocraticamente. (SANTOS, 2007, p. 56).

Em síntese, em sua lúcida e profunda avaliação sobre as bases para a revolução democrática do Judiciário, Boaventura de Souza Santos (2007) elenca importantes fatores para o desenvolvimento de uma consciência crítica do cidadão, seja ele profissional do campo jurídico ou não, como as questões estruturantes da justiça, da formação dos seus operadores nas faculdades de direito à formação do magistrado, à atuação dos tribunais.

Quanto à compreensão do direito, adverte que é preciso estar atento para a exploração de seus simbolismos, sem deixar de perceber as dimensões da participação comunitária e da solidariedade, numa aprendizagem recíproca em que a mobilização do direito atua a serviço da transformação social e a mobilização social transforma os pressupostos de atuação da prática jurídica.

Por todos esses fatores, é preciso reconhecer que a excessiva conflituosidade e a complexidade das relações sociais estão a exigir, do campo jurídico, a busca de mudança de paradigmas, que provoque uma ruptura do acomodado pensamento dogmático, em direção ao novo modelo de sociedade pós-moderna, rapidamente habituada às respostas instantâneas, oferecidas pela Internet, com tendências a virtualização e globalização.

5.3.3.1.2 Vias sociais de solução de litígios

Antes de fazermos algumas incursões acerca das vias sociais de soluções de litígios, é importante pôr em relevo o trabalho que o Conselho Nacional de Justiça vem desenvolvendo, nos últimos anos, no sentido de estabelecer políticas públicas

destinadas ao tratamento adequado dos conflitos no âmbito do próprio Judiciário, incrementando tanto meios autocompositivos, quanto heterocompositivos, estes com a implantação de metas a serem alcançadas no enfrentamento da morosidade em todas as esferas judiciais nacionais, com apresentação de resultados numericamente positivos.

A Resolução n.º 125 do Conselho Nacional de Justiça (CNJ)³⁹ traça as bases da política pública nacional destinada à adequada resolução dos conflitos, cujo principal objetivo é disseminar a cultura da pacificação social, sobretudo planejando amplos programas de autocomposição, a exemplo da Semana Nacional de Conciliação, com índices satisfatórios de acordos em processos judiciais em tramitação.

Merece destaque a experiência do Tribunal de Justiça da Bahia, que, desde 2003, implantou o projeto Balcão de Justiça e Cidadania, em constante aperfeiçoamento e expansão, diante do êxito do trabalho desenvolvido na solução pré-processual de litígios, com atendimento da população de baixa renda e com reais dificuldades de acesso à Justiça tradicional. O projeto é fundado na mediação e tem alcançado ótimo desempenho durante essa década de funcionamento.

A seguir, o resumo das atividades do Balcão de Justiça e Cidadania (Fig. 4), envolvendo as questões na área de interesse de pensão de alimentos, divórcio consensual, dissolução de união estável, reconhecimento espontâneo de paternidade e questões cíveis referidas no art. 3º da Lei n.º 9.099/95 (Juizados Especiais).

³⁹ A Resolução nº 125, de 29 de novembro de 2010, expedida pelo Conselho Nacional de Justiça — CNJ dispõe sobre a Política Judiciária Nacional de tratamento adequado dos conflitos de interesses no âmbito do Poder Judiciário e prevê a possibilidade de se organizar outros mecanismos de solução de conflitos, em especial os consensuais, como a mediação e a conciliação.

Figura 4 – Resumo das atividades do Balcão de Justiça e Cidadania

ITEM	ANO						
	2007	2008	2009	2010	2011	2012	Σ
Orientação Jurídica	10.690	20.659	29.341	34.738	38.006	49.997	172.741
Casos para Mediação	9.799	17.184	26.163	33.467	36.826	44.077	157.717
Total de Atendimento	20.489	37.843	55.504	68.205	74.832	85.074	321.458
Acordos de Família	2.843	5.321	9.182	13.193	14.960	16.618	59.274
Acordos Cíveis	875	1.877	1.254	2.073	2.198	2.139	9.541
Total de Acordos	3.718	7.198	10.436	15.266	17.158	18.757	68.815
Sessões Realizadas	5.857	13.105	21.082	27.764	30.097	31.482	123.530

Fonte: Tribunal de Justiça da Bahia. Disponível em: <<http://www5.tjba.jus.br>>.

Na área criminal, a implantação do Núcleo de Justiça Restaurativa, criado pela Resolução n.º 8, de 28 de julho de 2010, do Tribunal de Justiça da Bahia, constitui outro instrumento de solução de conflitos concebido para utilização de métodos e práticas restaurativas nas ocorrências e nos processos em tramitação no Juizado Especial Criminal de Salvador, possuindo funções específicas de planejar, apoiar, executar e avaliar a aplicação de vias alternativas na solução de conflitos inseridos na área de atuação jurisdicional.

Segundo afirma a Juíza Joanice Maria Guimarães de Jesus, que dirige e elaborou a Cartilha⁴⁰ do Núcleo de Justiça Restaurativa do Núcleo de Justiça Restaurativa na Bahia, a principal ferramenta de atividade está assentada no consenso e, para alcançá-lo, vítima, infrator, terceiros afetados pela infração e membros da comunidade refletem, transformam e constroem soluções para os conflitos causados pelo crime. Faz parte da atividade do Núcleo de Justiça Restaurativa a realização de curso de capacitação para mediação penal e prevenção da violência e promoção da paz social, possibilitando a conciliação às vítimas e, aos agressores, de resolverem os transtornos decorrentes dos conflitos sociais.

A iniciativa bem sucedida do Tribunal de Justiça da Bahia, no que tange aos mecanismos alternativos de solução de conflitos, teve as seus pilares, suas ideias incorporadas e ampliadas pela Resolução n.º 125/2010 do CNJ, que agora abre as

⁴⁰ BAHIA. Tribunal de Justiça da Bahia. **Cartilha do Núcleo de Justiça Restaurativa**. Disponível em: <<http://www5.tjba.jus.br/conciliacao/images/stories/jrcartilha.pdf>>.

portas do Poder Judiciário de todo país para a concepção de política pública visando a implantar tais meios alternativos

[...] de tratamento adequado dos problemas jurídicos e dos conflitos de interesses, que ocorrem em larga e crescente escala na sociedade, de forma a organizar, em âmbito nacional, não somente os serviços prestados nos processos judiciais, como também os que possam sê-lo mediante outros mecanismos de solução de conflitos, em especial dos consensuais, como a mediação e a conciliação. (Resolução 125/2010 do CNJ).

Para uma revolução democrática do judiciário, Boaventura Souza Santos (2007) procura desmistificar uma gama de discursos jurídicos com críticas consistentes, ao tempo em que aponta caminhos possíveis de serem trilhados, no sentido de se repensar e superar o modelo jurídico tradicional, sinalizando para os meios alternativos de resolução de litígios, concebidos como práticas afirmativas, porém pouco divulgadas, a exemplo da justiça itinerante, da justiça restaurativa e dos juizados especiais, de mediação, da justiça comunitária, conciliação pré-processual judicial e extrajudicial.

Dentro do pensamento de Santos (2007, p. 31), é interessante registrar o desempenho judicial de rotina, ou de massa, sob a concepção do movimento de acesso à justiça encetado por Cappelletti e Garth (1988), da década de 1960, a respeito de estudos sociojurídicos voltados para o tema do acesso à justiça.

Os citados juristas italianos, em seus estudos, afirmam que, em diferentes países, a introdução de reformas processuais ou na estrutura do sistema de justiça, com o fim de universalizar o acesso à justiça, tem como a primeira onda a defesa e promoção de mecanismos de apoio judiciário aos cidadãos carentes. Nesta dinâmica, o apoio judiciário deixa de ser entendido como filantropia e passa a ser incluído como medida de combate à pobreza nos programas estatais. (SANTOS, 2007).

A segunda onda introduz mudanças de apoio, voltadas para a reivindicação e defesa dos interesses coletivos e difusos em juízo, de grupos sociais mais vulneráveis. (SANTOS, 2007, p 32).

Durante a terceira onda, que estamos vivenciando, o movimento de acesso à justiça procura expandir a concepção clássica de resolução judicial de litígios, desenvolvendo um conceito amplo de justiça, em que os tribunais fazem parte de um conjunto integrado de meios de resolução de conflitos, o que inclui o que se

convencionou chamar de ADR (resolução alternativa de litígios), dentre os quais as defensorias públicas, a capacitação jurídica de líderes comunitários e a advocacia popular, os programas governamentais e não governamentais destinados à preparação de integrantes da comunidade como mediadores na solução dos conflitos locais. Tudo isso, com o escopo de introduzir uma revolução democrática da justiça. (SANTOS, 2007, p. 31-36).

A terceira fase corresponde a importantes iniciativas governamentais, as quais buscam a mediação como meio de solução de conflitos, como o programa extraordinário “Justiça Comunitária”, concebido pela juíza Gláucia Falsarella Foley, do Tribunal de Justiça do Distrito Federal. Esse programa introduz e orienta a experiência de justiça comunitária no Brasil, incentivando tribunais de justiça estaduais em capacitar os membros das localidades mais pobres a prestar orientação jurídica e dar solução a problemas que não poderiam ser solucionados devidamente no judiciário por não se adequarem às exigências formais/probatórias do juízo ou porque não obteriam uma pronta resposta na justiça oficial. (SANTOS, 2007, p. 41).

Após se referir ao programa Justiça Comunitária, Santos (2007, p. 42) acentua:

O exemplo do programa justiça comunitária convida-nos a pensar na importância do poder judiciário como instituição de fomento à solução alternativa de litígios no Brasil. Um estudo recente sobre sistemas alternativos de resolução de conflitos no Brasil demonstrou que, das 67 iniciativas em curso no ano de 2004, 33 eram programas criados por instituições públicas, 32 desenvolvidos por organizações não governamentais e 2 criados por universidades. No caso dos programas públicos, o poder judiciário destaca-se como um dos principais impulsionadores da resolução alternativa de conflitos. Nos programas públicos, predominam, assim, os instituídos pelo judiciário estadual (17 programas, 51%), sendo 10 criados por tribunais de justiça e os restantes criados em varas e juizados. Nos programas não governamentais, predominam as organizações de abrangência nacional, de pequena e média estrutura, com alto grau de profissionalização (a maioria trabalha com técnicos remunerados) e direção composta por voluntários. A maior parte existe há mais de 10 anos e possui igual experiência na resolução alternativa de conflitos. No âmbito das iniciativas não governamentais de resolução de conflitos dirigidas para a capacitação de líderes comunitários e criação de escritórios populares de mediação, cito a atividade da organização não governamental Jus Populi, na Bahia. (SANTOS, 2007, p. 42).

Outro programa que vem dando bons resultados, segundo Santos (2007, p. 43), são as assessorias jurídicas populares, chamadas “advocacia popular”, que encerram ações de advogados populares por toda a América Latina, implementadas

a partir da abertura política e de redemocratização do Brasil, a partir da década de 1980.

Esses programas possuem importante aspecto para o universo dos juristas quanto à questão de um novo paradigma de uma advocacia, constatando Santos que “este processo de evolução da advocacia popular testemunha ainda a passagem de um modelo de defesa de base individualista para um modelo baseado na politização e coletivização do direito”, voltado para os movimentos de luta pela moradia urbana e rural, dos trabalhadores, desempregados, dos indígenas, aposentados, pensionistas da previdência social, dentre outros. (SANTOS, 2007, p. 43).

Ressalve-se que a ampliação dos meios de solução de litígios não quer dizer eliminação ou atrofia do Poder Judiciário, mas apenas otimização dos seus órgãos como último refúgio para solução de conflitos porque especialmente qualificados para a função jurisdicional. Mormente não se apregoa aqui a relativização do princípio constitucional da inafastabilidade da tutela jurisdicional.

Numa abordagem a respeito da constitucionalidade dos meios alternativos de resolução de conflitos, relativamente à arbitragem, Cândido Dinamarco (2002, p. 191) ressalta que:

É tão grande a convergência teleológica entre estes e a jurisdição estatal, que já se chegou a sustentar, sem qualquer heresia sistemática, a natureza jurisdicional dos processos arbitrais. Na medida de sua legitimidade social e política, que certos órgãos alternativos cumprem também a missão que em sede jurisdicional o Estado por longo tempo monopolizou. (Dinamarco, 2002, p. 191).

São várias as atividades que levam à pacificação social sem desviar a garantia constitucional da universalidade da jurisdição do Poder Judiciário.

Mudanças vêm ocorrendo com a edição de leis que desjudicializaram alguns tipos de demandas. São algumas iniciativas pontuais que possibilitam às partes satisfazerem seus interesses com maior celeridade, a exemplo da Lei n.º 11.441, 4 de janeiro de 2007, que retirou do Código de Processo Civil, os institutos de inventários e partilhas, com algumas exceções, bem como a separação consensual, transferindo os mesmos para os Serviços Notariais, dando mostras do acerto da iniciativa legislativa. Esta experiência deve ser ampliada para outras causas de natureza patrimonial ou não, mas com potencial de acerto e autocomposição entre contendores.

Conquanto a ideia da desjudicialização de conflitos encontre receptividade em órgãos estatais, a exemplo do CNJ, o grande desafio está na mudança de paradigma do campo jurídico, suas desconfiças, dúvidas e incertezas que fazem parte da aprendizagem, da consciência crítica e da transformação cultural.

Neste cenário, a prudência recomenda que não se suprima o controle jurisdicional, mas se criem mecanismos e instrumentos alternativos, concomitantemente à jurisdição com o escopo de ampliar as práticas, no contexto e participação social, nas situações corriqueiras de desavenças, desacordos, disputas, lides e conflitos.

São infinitas as possibilidades de solução de controvérsias por outros meios, como a mediação, juízes de paz, câmeras de conciliação, contenciosos administrativos em todos os níveis de governo, agências reguladoras, PROCONs, associações, sindicatos, conselhos tutelares, comissões condominiais, etc., partindo-se da necessidade do corpo social que irá detectar e exigir dos atores sociais as alternativas para a condução de um resultado satisfatório diverso de um comando judicial.

A difusão da cultura de pacificação de conflitos, através de métodos e instrumentos não jurisdicionais, pode acarretar uma maior participação e cooperação dos atores sociais, caracterizando uma espécie de solidariedade social, com o sentimento de pertencimento e empoderamento do grupo de indivíduos, para a realização de escolhas daquele grupo social que, só na sociedade, pode-se atingir. Os resultados dos conflitos apaziguados apresenta-se como elo de corresponsabilidade, partilhada por todos os atores envolvidos, os contendores e os agentes de pacificação social como membros da comunidade.

Segundo Santos (2007), o pensamento jurídico crítico parte da constatação de que não há exclusividade para a produção estatal do direito, circunstância que ocasiona uma grande perda de experiência e da prática jurídica. Contrapondo-se a esse paradigma, propugna esse autor a existência de uma pluralidade de ordens jurídicas, no interior do mesmo espaço geopolítico.

A problemática da superação de uma visão monista de produção do direito e do monopólio estatal da jurisdição afigura-se um novo paradigma, de viés emancipatório, que se abre a partir de uma racionalidade pragmática, na qual se encontram desde aspectos estético-expressivos relacionados às artes até a própria razão prático-moral situada na justificação do direito e nas teorias da justiça.

A percepção de que o Estado não tem desempenhado a contento sua função jurisdicional e, conseqüentemente, seu escopo de pacificação, viabilizam-se as bases necessárias para que se justifique a iniciativa de resolução extrajudicial de litígios, mediante decisões provenientes de outros poderes, autoridades públicas e órgãos delegados da Justiça, sem que tais soluções violem o princípio do controle jurisdicional, com resultados axiologicamente éticos, moralmente e socialmente aceitos, e, por último, sem afronta ao sistema jurídico e judicial.

De um ponto de vista sociológico, as sociedades são jurídica e judicialmente plurais, circulam nelas vários sistemas jurídicos e judiciais, e o sistema jurídico estatal nem sempre é, sequer, o mais importante na gestão normativa do cotidiano da grande maioria dos cidadãos. (SANTOS, 2007, p. 77).

Pontua-se, ademais, que o debate e a análise crítica dos paradigmas que levam à excessiva judicialização podem estar na nossa cultura social individualista, (cada um cuida de si), sem o despertar para o coletivo, para o campo social onde habitamos. A socialização da pacificação dos conflitos, que surgem como fato social, pode gerar um efeito mais amplo e enraizado na base social onde nasceu e se solucionou o conflito, possivelmente gerando o reequilíbrio e justiça social.

Para concluir este capítulo, merece enfatizar que a desjudicialização constitui um processo civilizatório para a sociedade contemporânea, acostumada com a rapidez e a flexibilização do próprio Direito que acompanha o progresso tecnológico, do qual não abre mão.

A Justiça estatal já admite os mecanismos que facultam às partes comporem seus litígios fora da esfera dos comandos judiciais, seja na esfera administrativa ou por entidades privadas, que podem desempenhar importante papel coadjuvante da jurisdição estatal, ampliando as vias de pacificação social e, por via transversa, contribuir para a superação da eterna crise da Justiça.

A verdadeira cultura da paz poderá ser disseminada por nós, operadores do direito, se abrirmos os olhos para as possibilidades da socialização de conhecimentos, aceitação da multidisciplinaridade, com o rompimento da crença de que só o Judiciário tem poder e competência para resolver os conflitos. Enfim, a desjudicialização é, pois, um dos caminhos para pacificação social, constituindo uma diretriz para a escolha de política pública criminal de prevenção de conflitos cibernéticos e, em última análise, de prevenção da cibercriminalidade.

Nesta linha de raciocínio, a política criminal de prevenção da ciberdelinquência irá se materializar através das diversas fontes de pacificação social, utilizando-se dos métodos alternativos de solução de conflitos, como a arbitragem, negociação e mediação, convencional ou *on-line* por ODR, de modo que a satisfação dos direitos e interesses das partes envolvidas evitará a judicialização de demanda civil ou criminal.

Assim, por exemplo, num conflito em que se discute o uso indevido de um *software*, a atuação de um arbitro ou mediador extrajudicial, com uma solução negociada que atenda aos interessados, poderá afastar uma ação de reparação civil, bem como uma ação penal por infração ao tipo penal previsto no artigo da lei.

5.3.3.1.3 Vias alternativas de solução de conflitos cibernéticos

Tudo que ocorre na internet toma uma dimensão macro e os conflitos, também. O grande desafio é exatamente questionar como resolver tais conflitos, considerando que a jurisdição estatal vem se debatendo com a problemática da superjudicialização de demandas e a busca incessante da entrega da prestação jurisdicional efetiva em tempo razoável.

Como resolver os conflitos advindos do comércio eletrônico, dos abusos decorrentes das redes sociais, as invasões de privacidade ou qualquer violação aos direitos fundamentais? Quais os caminhos a trilhar, considerando que a internet não está sob o controle de qualquer autoridade ou empresa? O que fazer com a ubiquidade da rede e a efemeridade de suas tecnologias? Grande parcela desses conflitos deverá ficar na margem da litigiosidade contida?

Como salientado, o monopólio do Estado na criação de normas jurídicas e da jurisdição tem se mostrado socialmente insuficiente para abarcar a crescente e desenfreada conflituosidade da sociedade contemporânea, sobretudo diante da nova realidade imposta pela intensificação das relações no ciberespaço e da expansão dos conflitos.

Numa breve retrospectiva, cumpre lembrar que o movimento de acesso à justiça liderado pelos juristas italianos Cappelletti e Garth (1988) demonstrou a elevada importância do direito ao acesso à justiça que, em muitas legislações de Direito Comparado, passou a ter *status* de direito fundamental da pessoa humana:

De fato, o direito ao acesso efetivo tem sido progressivamente reconhecido como dado de importância capital entre os novos direitos individuais e sociais uma vez que a titularidade de direitos é destituída de sentido, na ausência de mecanismos para sua efetiva reivindicação. O acesso à justiça pode, portanto, ser encarado como requisito fundamental — o mais básico dos direitos humanos — de um sistema jurídico moderno e igualitário que pretende garantir, e não apenas proclamar os direitos de todos. (CAPPELLETTI; GARTH, 1988, p. 110).

A Constituição Federal de 1988, também, erigiu o direito ao acesso à justiça ao patamar dos direitos fundamentais. Dentro da concepção de acesso à justiça, enquadra-se a universalização da tutela jurisdicional, isto porque todos os conflitos, sejam individuais ou coletivos, difusos ou homogêneos, podem ser invariavelmente submetidos à apreciação do Poder Judiciário, o que consubstancia o princípio da inafastabilidade da tutela jurisdicional.

O processualista Cândido Rangel Dinamarco, precursor, no Brasil, do movimento de acesso à justiça, aqui também chamado de instrumentalista, doutrina a dimensão desse movimento:

Aguarda-se a caminhada para um sistema em que se reduzam a um mínimo inevitável os conflitos não-jurisdicinalizáveis (a universalização da tutela jurisdicional) e em que o processo seja capaz de outorgar a quem tem razão toda a tutela jurisdicional a que tem direito. (Dinamarco, 1993, p. 21).

Passados vinte anos, após a constatação de que o Poder Judiciário não consegue abarcar todos os conflitos surge novo movimento no sentido de se conscientizar a sociedade de que o acesso à justiça não se confunde com o acesso ao Poder Judiciário. Neste diapasão,

[...] o acesso à Justiça não se confunde com o acesso ao Judiciário, tendo em vista que não visa apenas levar as demandas dos necessitados àquele Poder, mas realmente incluir os jurisdicionados que estão à margem do sistema” para que possam ter seus conflitos resolvidos (por heterocomposição) ou recebam auxílio para que resolvam suas próprias disputas (pela autocomposição. (AZEVEDO, 2013, p. 29).

A Resolução N.º 125/10 do CNJ, ao estabelecer política pública de tratamento adequado dos conflitos, passou a incentivar a atividade de prevenção de demandas com as chamadas atividades pré-processuais de conciliação e mediação, reconhecendo, contudo, que:

Atualmente, a administração da justiça volta-se a melhor resolver disputas afastando-se muitas vezes de fórmulas exclusivamente positivadas e incorporando métodos interdisciplinares a fim de atender não apenas aqueles interesses juridicamente tutelados mas também outros que possam auxiliar na função de pacificação social. (AZEVEDO, *ibid.*, p 31).

Após várias reformas e etapas evolutivas, o processo judicial, que supervalorizava o procedimento ordinário, passou a admitir “tutelas diferenciadas”, em razão da necessidade de adequação do procedimento ao direito material a ser tutelado, bem como tutelas preventivas. (SILVA, O., 1991, p. 98).

Contudo, apesar de estar em constante aprimoramento, o processo judicial continua moroso e caro, fatores preponderantes que impulsionam a busca por alternativas de meios de resolução de conflitos de forma rápida e com um custo reduzido. A respeito do conjunto destas ideias, assevera Hobaika (2004):

O processo eletrônico é uma importante realidade que se materializa e tende a auxiliar e muito o funcionamento do Poder Judiciário, em todas as suas instâncias. Não apenas pela consulta aos andamentos e o acesso ao teor das decisões, mas principalmente a informatização dos atos processuais pode otimizar o já desgastado e arcaico sistema de papel. Entretanto, apesar de ser uma tendência bem-vinda para a desburocratização, o processo eletrônico não é uma garantia efetiva de solução contra a morosidade e o acúmulo de litígios que sobrecarregam a Justiça.

A relevância desta abordagem surge, então, da necessidade do emprego de meios legais e eficazes para a solução dos conflitos que envolvam aspectos informáticos, levando-se em consideração suas peculiaridades técnicas e a rapidez (com eficiência) no deslinde das demandas.

[...] já é possível a realização de soluções de controvérsias por mediação e arbitragem, em tempo real (*online*), representando isso uma verdadeira revolução chamada de *E-resolution* ou *Online Dispute Resolution* (ODR), como é mais conhecida.

Em alguns países, adota-se a prática de métodos de solução de conflitos através de organismos que utilizam métodos alternativos tradicionais (arbitragem e

mediação), por meio do sistema "ODR" ou *Online Dispute Resolution*, ou *E-resolution*, utilizado para dirimir disputas vinculadas ou não ao comércio eletrônico, em tempo real (*on-line*). (HOBAlKA, 2004).

Argumenta esse autor que, no Direito Comparado, países da União Europeia, como Alemanha, Espanha e Itália, possuem legislação autorizando a resolução de conflitos originados de transações de comércio eletrônico através de métodos alternativos como a mediação e arbitragem, em linha, conhecidos como *E-resolution* ou *Online Dispute Resolution (ODR)*. Tanto que a Diretiva 2000/31/EC, em comércio eletrônico, prevê, como prioridade, políticas que incentivem a resolução de conflitos no contexto da sociedade de informação, dos países integrantes da União Europeia, através de entidades que operam na própria internet e que utilizam mecanismos de soluções extrajudiciais. (HOBAlKA, 2004).

Esses métodos alternativos são comumente usados nas questões envolvendo disputas advindas de ocorrências em linha sobre propriedades, marcas, mensagens indesejáveis (*spam*), infração a direitos autorais, apropriação ilícita de segredos comerciais, difamação, fraude, práticas enganosas de negócio, remoção de sítios da *web*, enfim conflitos contratuais, a maioria de proteção do consumidor em comércio eletrônico, relativos atividades *on-line*.

A utilização de tais serviços fica a critério do usuário da internet sem, no entanto, abrir mão do direito ao acesso à jurisdição, para os casos que tais métodos não lograrem êxito, ou não haja a confiança na funcionalidade e ética do serviço.

Essas organizações dispõem de um banco de dados a respeito dos diversos conflitos ou são especializados em um tipo específico de disputa, como seguros, cartões de créditos, *software*, ou em certos conflitos que não exigem uma grande quantidade de interação face a face.

Essas entidades contam com um quadro de mediadores e árbitros profissionais, muitos dos quais são juízes aposentados, advogados experientes, especialistas do setor e as principais autoridades em seus respectivos campos. O interessado pode pesquisar no próprio sítio da entidade a localização geográfica, as áreas de atuação, direito, tecnologia, por exemplo, tipo de experiência, ou o número de casos tratados. Incentivar e reconhecer a funcionalidade e eficácia dos novos procedimentos de resolução em linha *on-line* é uma tendência mundial, até porque vários órgãos e institutos oferecem esses serviços, gratuitamente ou a preços

acessíveis, na rede mundial de computadores. Marcelo Hobaika (2004) chama a atenção para a necessidade desses métodos de solução de conflito em linha:⁴¹

No Brasil, ao contrário dos Estados Unidos e da Europa, as formas não adversárias de solução de conflitos ainda estão em processo de consolidação, inclusive em relação às disputas *offline*. A expectativa, contudo, é que as instituições nacionais promovam também os métodos por meio eletrônico, principalmente em relação às disputas que tratem do *e-commerce*.

Este caminho vai de encontro à nova ordem mundial e o Brasil deve estar preparado para se inserir nesta ótica, sob pena de exclusão. Evidentemente, qualquer importação de ideias deve ser precedida da promoção de debates e discussões a fim de adaptar as novas situações e possibilidades à realidade nacional.

Segundo Atheniense (2003), o número de entidades que tem finalidade de oferecer os meios alternativos de solução de conflitos pela internet, também conhecida no Direito norte-americano por ADR (*Alternative Dispute Resolutions*), tem crescido, de forma que

esses foros compreendem diversas técnicas para dirimir disputas de interesse como a arbitragem, a mediação e a negociação. Em alguns casos concretos, essas soluções têm se mostrado mais eficientes, principalmente, pela flexibilidade concedida às partes para a argumentação técnico-jurídica de suas defesas, bem como pela maior afinidade da compreensão do objeto da lide por parte de árbitros reconhecidamente *experts* nas questões envolvendo inovações tecnológicas. Essas organizações têm-se estruturado e oferecido seus serviços pela internet para solucionar litígios típicos ou não do mundo eletrônico. (ATHENIENSE, 2003).

⁴¹ Marcelo Bechara de Souza Hobaika (2004) afirma que são praticadas “formas variadas de realização de métodos ODR, [...]. Atualmente, destacam-se quatro tipos de sistemas de ODR, a saber: 1) Sistema automatizado online de reivindicações financeiras, com a utilização de perícia para a solução; 2) Arbitragem *online*. [...] 3) Serviços *online* de *Ombudsman* para reclamações de consumidores e 4) Mediação *online*. Existem duas formas. A automatizada e a assistida. Na primeira as partes submetem a um computador uma proposta [...]. Alguns métodos de ODR, entretanto, são também aplicáveis aos conflitos tradicionais (conflitos *offline*). O termo ODR ou resolução eletrônica de disputa, entretanto, não se refere ao tipo de conflito, mas ao meio pelo qual o procedimento é executado. Além do mais, em alguns casos, nem todas as formas de resolução de disputa e nem todas etapas dos procedimentos são executados inteiramente *online*. A solução para conflitos envolvendo nomes de domínio através do já tratado UDRP é um exemplo de *e-resolution*, mas de longe não é o único.”

Com efeito, para Atheniense (2003, p. 11), em termos de ciberespaço, a observância do princípio de que a jurisdição pressupõe a existência de um território onde será exercida, deve ser repensada diante das múltiplas relações que os indivíduos instauram através da internet, independentemente dos aspectos geográficos.

Ainda, segundo Alexandre Atheniense, especialistas ingleses e norte-americanos estudiosos do tema *Law of the Cyberspace*, enfatizam que a internet poderia ou deveria ser autorregulamentada, sob o argumento de que a legislação aplicável à solução dos conflitos estaria vinculada a uma instituição específica de uma determinada nação e isso seria menos efetivo “e apropriado do que se buscar construir centros de arbitragem ou mediação para apreciar os problemas oriundos do federalismo eletrônico.” Observa este autor que

nessa perspectiva, autores como o inglês Cliff Dilloway e o prof. norte-americano David Post vislumbram a perspectiva que a internet deveria, ao menos potencialmente possuir sua própria jurisdição sem ser atrelada a padrões de territórios geográficos ou a qualquer outro meio físico e virtualmente sem soberania de países. Tratando-se de internet, o conceito tradicional de soberania, que preceitua que o Estado deverá exercer sua autoridade plena e governo próprio, dentro do território nacional e em suas relações com outros Estados deverá ser reavaliado. Isso porque uma das características principais da grande rede é o fato de o indivíduo instaurar múltiplas relações por meio eletrônico, sem que o Estado possa efetivamente controlá-lo. (ATHENIENSE, 2003, p. 77).

Consoante à argumentação dos articulistas suprarreferidos, a solução de controvérsias pelo método ADR (*Alternative Dispute Resolution*) por intermédio da negociação, conciliação, mediação e arbitragem, em linha, são possivelmente métodos mais adequados a solução de conflitos decorrentes das atividades no ciberespaço, especialmente quando os interesses em disputas não afetam os direitos das vítimas de crimes e ilícitos graves, tanto no sentido da repulsa da ordem jurídica, ética e justa, quanto do âmbito individual, quando a vítima não deposita a confiança e, portanto, não internaliza o sentimento da solução ética e justa que se espera de todo julgamento ou solução negociada de um conflito.

A resolução de disputas *on-line* permite uma combinação baseada na *web* de tecnologias multimídias e processos de negócios, eliminando as limitações de tempo, custo e distância. Os interessados estabelecem comunicação entre si, em qualquer localização. Os agentes que promovem essa aproximação, mediadores,

árbitros e juízes virtuais, promovem a aproximação dos interessados, que podem contar com a comodidade de não ter que se deslocar de seu ambiente habitual, contar com a transparência e a segurança digital com instrumentos cada vez mais inovadores

Essa tendência é corolário da evolução tecnológica, que está em constante aperfeiçoamento, permite encurtar distâncias e realizar diversas atividades em tempo real. Nesse âmbito, os conflitos devem ser resolvidos segundo a mesma dinâmica e anseios desta sociedade informatizada, acostumada à rapidez, imediatidade, baixo custo e eficiência.

Essa evolução, a que podemos chamar de forma genérica de espécie de “Ciberjustiça”, apresenta grande potencial de funcionalidade e inovação, seguindo a evolução das ferramentas, programas e aplicativos diuturnamente lançados na grande rede mundial de computadores — a internet, a invenção mais instigante da atualidade.

Com a visão crítica de que a Política Criminal tem a missão de propor caminhos que conduzem à quebra de resistência de soluções extrajudiciais para a redução da criminalidade, não se pode olvidar, como ressaltam Forti e Beristain Ipiña *apud* Reale Junior (2009, p. 70), que a Política Criminal “rege-se pelo senso da possibilidade, ou em vista do possível e do desejável em face a criminalidade”, o que converge para a intervenção do Estado com a adoção de medidas preventivas em conjunto com as mais variadas lideranças das comunidades e entidades interessadas numa internet, livre, segura e democrática.

A disseminação de métodos alternativos de resolução de conflitos em seu nascedouro produz o extraordinário efeito de redução significativa da criminalidade e, por via indireta, resulta na diminuição e seletividade dos conflitos que irão para o Poder Judiciário.

A elaboração de Política Criminal de prevenção à cibercriminalidade, com a demonstração de os métodos alternativos como mediação, arbitragem, negociação, inclusive *on-line*, deve ficar a cargo de propostas legislativas ou de medidas executivas de programas de governo do Ministério da Justiça e da Cidadania, podendo inclusive ficar inserido no âmbito do Pronasci.

6 CONCLUSÕES

O estudo teve como objetivo a discussão crítica acerca da compreensão do fenômeno da cibercriminalidade, sob o enfoque interdisciplinar, confrontando-se não apenas os aspectos puramente penais, mas com reflexões e abordagens de cunho sociológico, ligadas a criminologia, políticas públicas e segurança pública, com escopo da produção de conhecimento que contribua no campo da Política Criminal para prevenção de práticas ilícitas no ciberespaço.

Questionou-se se é possível a prevenção primária e quais os desafios para o estabelecimento de uma política criminal voltada à redução da cibercriminalidade, diante da complexidade da atuação de condutas desviantes no ciberespaço.

Para tanto, adotou-se uma metodologia qualitativa, através de investigação de fontes documentais concernentes ao tema.

Na contemporaneidade, o desenvolvimento da multiplicidade das relações no ciberespaço propiciou o surgimento de um novo gênero de criminalidade, impulsionado pela sensação de anonimato e liberdade que a internet e a realidade virtual proporcionam aos usuários, especialmente aos mais jovens. Atrás de um computador, é possível criar e assumir muitas faces, falsas identidades, mascarando o verdadeiro caráter, podendo qualquer pessoa, com conhecimento médio de informática, passar-se por outra, com o propósito deliberado de praticar ilícitos, nesse agitado e veloz mundo cibernético.

A grande incidência de ataques aos usuários da Internet para prática de ilícitos e crimes informáticos implica no importante fenômeno da criminalidade cibernética, que é crescente e globalizado, tendo despertado a preocupação da comunidade internacional, conforme retrata a Convenção sobre o Cibercrime adotada pelo Conselho da Europa, em Budapeste, em 2001.

A presente pesquisa intitulada *A expansão da criminalidade no ciberespaço: desafios de uma política criminal de prevenção ao cibercrime* tem a pretensão de contribuir para a discussão da problemática do crescimento vertiginoso da criminalidade informática e subsidiar as discussões acerca do papel e postura do Estado Brasileiro diante do fenômeno do crescimento dos ilícitos no ciberespaço, enfatizando a necessidade e desafios para criação e implantação de uma política

criminal específica, destinada à redução dos ilícitos decorrentes da universalização e intensificação do uso da Internet.

Nesse contexto, a pesquisa esteia-se nas seguintes eixos:

- a) A universalização do uso e acesso à internet como novo direito da pessoa humana;
- b) A intensificação das relações no ciberespaço e o surgimento de uma cibercultura;
- c) A grande incidência de ilícitos nas relações virtuais e surgimento da cibercriminalidade, fenômeno em crescimento e globalizado;
- d) O papel do Estado, enquanto responsável pela Segurança Pública, que desafia a definição e implantação de Políticas Criminais destinadas à prevenção, redução d ao cibercrime e ilícitos cibernéticos.

Como resultado da pesquisa, revelou-se que, sob o enfoque do controle social, pode-se afirmar que o Estado brasileiro, apesar das novas leis que preveem as mais recorrentes condutas delitivas no ciberespaço, não dispõe de meios suficientes para coibir a prática de crimes informáticos, por diversos fatores, como ausência de criminalização de alguns ataques cibernéticos considerados importantes, por carência da estrutura tecnológica da polícia judiciária para realizar investigações ou, ainda, pela morosidade da Justiça.

Assim, na perspectiva da política de controle, não basta uma legislação que incrimine certas condutas ilícitas, enquanto persiste uma série de entraves à persecução penal.

Nessa dimensão política, em razão da natureza transacional da *web*, a elaboração de legislação interna conectada ao direito penal comunitário e convenções internacionais, com as finalidades da prevenção e persecução do crime tecnológico, afigura-se de suma importância, como ponto de partida para o adequado tratamento e enfrentamento da criminalidade eletrônica.

A pesquisa revelou, principalmente, que, na emergência da sociedade da informação, a importância de debater e conhecer o fenômeno da criminalidade cibernética em ascensão, que surge como problema de Segurança Pública e de Política Criminal, considerando que, diante das perplexidades existentes do novo fenômeno as agências estatais responsáveis pela formulação de políticas de controle e prevenção permanecem com certa indiferença, sem priorizar medidas e ações destinadas à redução dos delitos informáticos.

Das reflexões acerca do problema, chega-se à ilação de que, na busca de respostas político-criminais ao fenômeno da cibercriminalidade, analisando-as sob prisma mais amplo, no âmbito das relações sociais, considerando a tendência de transformação da estrutura social, do nascer de uma cultura virtualizada, a prevenção, em oposição à perversidade seletiva do sistema penal, apresenta-se como a melhor política criminal de enfrentamento da expansão dos ilícitos praticados no ciberespaço.

A pesquisa revelou, também, que, em termos de Política Criminal e de Política de Segurança Pública, o problema do crescimento da criminalidade cibernética deve ser focado sob a interferência de paradigmas culturais impostos pela virtualização da sociedade contemporânea, concomitantemente ao fenômeno da globalização e seus efeitos nas relações humanas ditadas pela urgência, na sociedade pós-moderna, rapidamente habituada às respostas instantâneas oferecidas pela internet, confrontando esses paradigmas de uma sociedade cada vez mais digital, aos paradoxos do controle social baseado apenas na repressão, que não tem alcançado os objetivos da redução da criminalidade, de modo geral.

No que diz respeito aos ilícitos através da internet, ressalte-se que, após profundas reflexões, visualiza-se a **prevenção** como o principal paradigma, para o enfrentamento do preocupante problema da cibercriminalidade, enquanto eixo de política criminal e de política de segurança pública.

Nesse aspecto, afloram-se e justificam-se as discussões, concepções e implantações de políticas públicas de prevenção primária, dirigidas à segurança digital, investindo-se nos programas de desenvolvimento de tecnologias de proteção digital do fluxo de informações e conexões no ciberespaço, bem como na concepção e implantação de políticas públicas de inclusão digital, de educação e ética informacional, destinadas à atual e futuras gerações de usuários da Internet.

Em outra dimensão, a pesquisa resultou no fortalecimento do entendimento de que é de fundamental importância escolher e adotar a prevenção como a linha da Política Criminal, em face do fenômeno em ascensão da ciberdelinquência, através da utilização de métodos alternativos de solução de litígios, preferencialmente antes e até durante os atos de persecução criminal.

Nesta perspectiva, propugna-se, sob a concepção de política criminal de prevenção ao cibercrime, a disseminação de métodos alternativos de resolução de conflitos, em seu nascedouro, o que seguramente produzirá o extraordinário efeito

de redução significativa da criminalidade e, por via indireta, resultará na diminuição e seletividade dos conflitos, que, por não terem sido solucionados por autocomposição, serão submetidos à apreciação do Poder Judiciário.

Neste viés, a pesquisa propõe a elaboração de Política Criminal de prevenção dos ilícitos ocorrentes no ciberespaço, com a criação e implantação de programas que utilizem os métodos alternativos de solução de conflitos como a mediação, a arbitragem, a negociação, inclusive *on-line*, com métodos ODR (*Online Dispute Resolution*), a cargo da iniciativa privada ou órgãos públicos, concebidas e originadas de propostas legislativas de incentivo ou de medidas executivas de programas de governo, em especial do Ministério da Justiça e da Cidadania, podendo, inclusive, ficar inserido no âmbito do Pronasci e do Poder Judiciário, neste através do Conselho Nacional de Justiça.

Outro resultado relevante fundamenta-se no escopo da pesquisa contribuir para o desenvolvimento de uma atitude reflexiva e crítica sobre os atuais quadros epistemológicos na área das políticas públicas de segurança, subsidiando a discussão de novos campos de pesquisa, a respeito das questões da segurança digital em face da soberania Brasileira, o direito de acesso à informação, Internet e da segurança e privacidade das conexões.

Portanto, a necessidade premente de política criminal específica, destinada a municiar as agências estatais legislativas, executivas e judiciárias para compreenderem com uma visão científica, pluralista e atualizada a lidar eficazmente com o fenômeno da ciberdelinquência e redução dos ilícitos decorrentes das relações no âmbito da Internet.

Por fim, os fundamentos discutidos no decorrer do trabalho convergem para a inarredável conclusão de que o Estado brasileiro não pode prescindir da adoção, em caráter prioritário, de políticas públicas, destinadas à prevenção da criminalidade no ciberespaço.

REFERÊNCIAS

ANDRADE, Vera Regina Pereira de. Do paradigma etiológico ao paradigma da reação social: mudança e permanência de paradigmas criminológicos na ciência e no senso comum. **Seqüência**, Florianópolis, v. 16, n. 30, pp. 24-36, jun. 1995. Disponível em: <<http://periodicos.ufsc.br/index.php/sequencia/article/view/15819>>. Acesso em: 18 mar. 2013.

ARAS, Vladimir. Crimes de informática: uma nova criminalidade. **Jus Navigandi**, Teresina, ano 5, n. 51, out. 2001. Disponível em: <<http://jus.com.br/artigos/2250/crimes-de-informatica>>. Acesso em: 2 jun. 2014.

ARISTÓTELES. Ética a Nicômaco. Tradução Leonel Vallandro e Gerd Bornheim da versão inglesa de W. D. Ross. In: **Os Pensadores**. São Paulo: Nova Cultural, 1973. v.4.

ATHENIENSE, Alexandre. A jurisdição no ciberespaço. **Revista Cej – Centro de Estudos Judiciários**, Brasília, n. 20, p. 74-81, jan./mar. 2003. Disponível em: <<http://www2.cjf.jus.br/>>. Acesso em: 5 mar. 2014.

AZEVEDO, André Gomma (org). **Manual de mediação judicial**. Brasília/DF: Ministério da Justiça e Programa das Nações Unidas para o Desenvolvimento – PNUD, 2013.

BAHIA. Tribunal de Justiça da Bahia. **Cartilha do Núcleo de Justiça Restaurativa**. Elaboração Joanice Maria Guimarães de Jesus, Maria Aparecida Lopes Nogueira e Andréa Tourinho Peixoto de Miranda. Salvador, 2011. Disponível em: <<http://www5.tjba.jus.br/conciliacao/images/stories/jrcartilha.pdf>>. Acesso em: 2 jun. 2014.

BARATTA, Alessandro. **Criminologia crítica e crítica do direito penal**. 2 ed. Rio de Janeiro: Freitas Bastos, 1999.

BAUMAN, Zygmunt. **Comunidade: a busca por segurança no mundo atual**. Tradução Plínio Dentzien. Rio de Janeiro: Zahar, 2003.

BECCARIA, Cesare. **Dos delitos e das penas**. Tradução Torrieri Guimarães. 6. ed. São Paulo: Martin Claret, 2000.

BOBBIO, Norberto. **O positivismo jurídico: lições de filosofia do direito**. São Paulo: Ícone, 1995.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 22. ed. São Paulo: Malheiros, 2007.

BOURDIEU, Pierre. **O poder simbólico**. Tradução Fernando Tomaz. 8 ed. Rio de Janeiro: Bertrand Brasil, 2005.

BRASIL. **Congresso Nacional. Câmara dos Deputados. Diário da Câmara dos Deputados**, Discurso do Deputado Eduardo Azeredo. Brasília, 17 julho 2013, Sessão 214.3.54. Disponível em: <<http://www.camara.gov.br/internet/sitaqweb/TextoHTML.asp?etapa=3&nuSessao=214.3.54.O&nuQuarto=93&nuOrador=2&nuInsercao=0&>>. Acesso em: set. 2013.

_____. **Constituição da Republica Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 20 maio 2014.

_____. Lei n.º 11.530, de 24 de outubro de 2007. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2007/Lei/L11530.htm>. Acesso em: 20 maio 2014.

_____. Lei n.º 12.735, de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 20 maio 2014.

_____. Lei n.º 12.737, de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 20 maio 2014.

_____. Ministério da Justiça. **Marco civil da Internet**: seus direitos e deveres em discussão. Disponível em: <<http://culturadigital.br/marcocivil/>>. Acesso em: 23 abr. 2014.

_____. Projeto de Lei n.º 2.793, de 2011. Disponível em: <<http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>>. Acesso em: 20 maio 2014.

CABETTE, Eduardo L. S. O novo crime de Invasão de Dispositivo Informático. **Consultor Jurídico**, São Paulo, 4 fev. 2013. Disponível em: <<http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>>. Acesso em: 20 maio 2014.

CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da Constituição**. 7. ed. Coimbra: Almedina, 2003.

CAPPELLETTI, Mauro; GARTH, Bryant. **Acesso à justiça**. Tradução de Ellen Gracie Northfleet. Porto Alegre: Fabris, 1988.

CHAUÍ, Marilena. **Convite à Filosofia**. São Paulo: Ática, 2000.

CINTRA, Antônio C. de Araújo; GRINOVER, Ada Pellegrini; DINAMARCO, Cândido Rangel. **Teoria geral do processo**. 9. ed. rev. e atual. São Paulo: Malheiros, 1992.

COMITÊ GESTOR DA INTERNET NO BRASIL. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de segurança para internet**. 2. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012.

CONVENÇÃO DE BUDAPESTE SOBRE O CIBERCRIME DE NOVEMBRO DE 2001, em vigor em 01 de julho de 2004. Disponível em: <<http://conventions.coe.int>>. Status as of: 18/3/2013.

CORRÊA, Cybthia Harumy Watanabe. Comunidades Virtuais gerando identidades na sociedade em rede. **Universiabrasil.net**, 2004. Disponível em: <www.uff.br/mestcii/cyntia1.htm+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 2 set. 2013.

COSTA, Arthur Trindade M. É possível uma Política Criminal? A discricionariedade no Sistema de Justiça Criminal do DF. **Soc. estado**, Brasília, v. 26, n. 1, abr. 2011. Disponível em <<http://www.scielo.br/ =iso>>. Acesso em: 27 mar. 2013.

COSTA, Ivone Freire. **Política e sociedade: gestão de segurança pública, violência e controle social**. Salvador: Edufba, 2005.

COSTA, Marco Aurélio Rodrigues da. Crimes de Informática. **Jus Navigandi**, Teresina, ano 2, n. 12, 5 maio 1997. Disponível em: <<http://jus.com.br/artigos/1826>>. Acesso em: 2 jun. 2014.

CRESPO, Marcelo Xavier de Freitas. **O cibercrime**. São Paulo: Saraiva, 2011.

_____. Noções introdutórias aos delitos informáticos. In: **Âmbito Jurídico**, Rio Grande, XII, n. 67, ago 2009. Disponível em: <<http://www.ambito-juridico.com.br/site/index.php?>>. Acesso em: jul. 2014.

CRUZ, Danielle da Rocha. **Criminalidade informática: tipificação penal das condutas ilícitas realizadas com cartão de credito**. Rio de Janeiro: Forense, 2006.

DALLARI, Dalmo de Abreu. **O Poder dos Juízes**. São Paulo: Saraiva 1996.

DELMANTO, Celso et al. **Código Penal Comentado**. 6 ed. atual. e amp. Rio de Janeiro: Renovar, 2002.

_____. **Código Penal Comentado**. 8 ed. rev. e ampl. São Paulo: Saraiva, 2010.

DERRIDA, Jacques. **Cosmopolitas de todos os países, mais um esforço!** Tradução Fernanda Bernardo. Coimbra: Minerva, 2001.

DIAS, Vera Elisa Marques. **A problemática da investigação do cibercrime**. Universidade de Lisboa, Lisboa, 2010. Disponível em: <http://www.verbojuridico.com/doutrina/2011/veradias_investigacaocibercrime.pdf>. Acesso em: 30 mar. 2014.

DIAS, Wladimir Rodrigues. Nota Sobre Direito e Conhecimento em Boaventura de Sousa Santos. **Jus Navigandi**, Teresina, ano 18, n. 3699, 17 ago. 2013 . Disponível em: <<http://jus.com.br/artigos/25146>>. Acesso em: 7 set. 2013.

DINAMARCO, Cândido Rangel. **A instrumentalidade do processo**. 3. ed. São Paulo: Malheiros, 1993.

FARIA, José Eduardo. **Sociologia jurídica direito e conjuntura**. 2. ed. São Paulo: Saraiva, 2010.

FERRAJOLI, Luigi. **Direito e Razão: teoria do garantismo penal**. Tradutores Ana Paula Zomer et al. São Paulo: Revista dos Tribunais, 2002.

FERREIRA, Érica Lourenço de Lima. **Internet: macrocriminalidade e jurisdição internacional**. 1. ed. (ano 2007), 1ª reimpr. Curitiba: Juruá, 2010.

_____. **Jurisdição metaterritorial para a cibernética**. 2005. Disponível em: <<http://sisnet.aduaneiras.com.br/lex/doutrinas/arquivos/meta.pdf>>. Acesso em: 4 mar 2014.

FILOCRE, Lincoln D'Aquino. **Direito de segurança pública: limites jurídicos para políticas de segurança pública**. Coimbra: Almedina, 2008.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Tradução Raquel Ramallete. Petrópolis: Vozes, 1987.

FUNDAÇÃO GETÚLIO VARGAS. Centro de Tecnologia e Sociedade da Escola de Direito do Rio de Janeiro. **Relatório de políticas de Internet: Brasil 2011**. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: <<http://www.cgi.br/media/docs/publicacoes/1/relatorio-politicas-internet-pt.pdf>>. Acesso em: 30 mar. 2014.

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. **Crimes na internet e inquérito policial eletrônico**. São Paulo: EDIPRO, 2012.

GARSON, Samy. **A adequação da ideia de monopólio de jurisdição com os meios alternativos de resolução de litígios: desjudicialização da execução**. Disponível em: <<http://www.sgaa.adv.br/publicacoes.php>>. Acesso em: 6 ago. 2013.

GOMES, Luiz Flávio; CERVINI, Raúl. **Crime organizado: enfoques criminológico, jurídico (Lei 9.034/95) e política criminal**. 2. ed. São Paulo: Revista dos Tribunais, 1997.

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. **Revista de Direito Mackenzie**, São Paulo, v. 1, p. 35-39, 2000.

HOBBAKA, Marcelo Bechara de Souza. O uso da arbitragem como solução para os conflitos da tecnologia da informação e os métodos odr (online dispute resolution) como alternativas não adversariais para resolução de controvérsias por meio eletrônico. **Instituto Brasileiro de Direito da Informática**, Recife, 3 fev. 2004. Disponível em: <<http://www.ibdi.org.br/site/artigos.php?id=102>>. Acesso em: 23 maio 2014.

HOBBS, Thomas. **Leviatã ou matéria, forma e poder de um estado eclesiástico e civil**. Tradução João Paulo Monteiro e Maria Beatriz Nizza da Silva. São Paulo: Abril Cultural, 1983. Disponível em: <<http://projeto-phronesis.files.wordpress.com/2009/04/os-pensadores-thomas-hobbes.pdf>>. Acesso em: 25 set. 2013.

HOBBS, Thomas. **Do Cidadão**. Tradução, apresentação e notas de Renato Janine Ribeiro. São Paulo: Martins Fontes, 1992. Disponível em: <<http://charlezzine.com.br/wp-content/uploads/Do-Cidad%C3%A3o-Hobbes.pdf>> Acesso em: 25 set. 2013.

IANNI, Octavio. **Globalização: novo paradigma das ciências sociais**. **Estudos Avançados**, v. 8, n. 21, São Paulo, maio/ago 1994. Disponível em: <<http://dx.doi.org/10.1590/S0103-40141994000200009>> Acesso em: 23 maio 2013.
IANNI, Octavio. O Declínio do Brasil-Nação. **Revista Estudos Avançados**, v. 14 (40): 51-58, set/dez. 2000. Disponível em: <http://resistir.info/brasil/ianni_declinio.htm>. Acesso em: 10 mar. 2014.

JAIME, Silena. Breves reflexões sobre a política criminal. **Jus Navigandi**, Teresina, ano 11, n. 1155, 30 ago. 2006. Disponível em: <<http://jus.com.br/revista/texto/8860>>. Acesso em: 27 mar. 2013.

KAHN, Tulio. Intimidação, incapacitação ou prevenção? Qual o melhor meio para reduzir a criminalidade. **Revista Brasileira de Ciências Criminais**, v. 30. Conjuntura Criminal, ano 2, n. 9, out. 1999.

_____. Prefácio. In: **Das Políticas de Segurança Pública às Políticas Públicas de Segurança**. Coletânea, organização conjunta do ILANUD (Instituto Latino-Americano das Nações Unidas para Prevenção da Criminalidade e Tratamento do Delinquente) e pelo Gabinete de Segurança Institucional da Presidência da República. São Paulo: ILANUD, 2002. Disponível em: <<http://www.ilanud.org.br>>. Acesso em: 5 mar 2013.

KANT, Immanuel. A paz perpétua: um projecto filosófico. In: KANT, Immanuel. **A paz perpétua e outros opúsculos**. Tradução Artur Morão. Lisboa: Edições 70, 1995. p. 21-37.

_____. **A religião nos limites da simples razão**. Tradução Artur Morão. Covilhã: Universidade da Beira Interior, 2008 [1793]. (Col. Textos Clássicos de Filosofia). Disponível em: <<http://marxists.architexturez.net/portugues/kant/1793/mes/limites.pdf>>. Acesso em: 23 set. 2014.

KELSEN, Hans. **Teoria geral do direito e do estado**. Tradução Luís Carlos Borges. 3. ed. São Paulo: Martins Fontes, 1998.

KUNRATH, Josefa Cristina Tomaz Martins. **A técnica da sumarização e a busca de tutelas diferenciadas**. 1995. Trabalho de conclusão de curso (Pós-graduação *lato sensu* em Direito Processual Civil) — Universidade Estadual de Santa Cruz, Ilhéus-BA, 1995.

LEMO, André. **As estruturas antropológicas do ciberespaço**. Salvador: texto produzido para os seminários do grupo Cyberpesquisa/Facom-UFBA, 1996, p.1 Disponível em: <<http://www.facom.ufba.br/ciberpesquisa>>. Acesso em: 6 set. 2013.

_____. **Cibercultura**: entrevista [2003]. Disponível em: <<http://informatica.terra.com.br>> Acesso em: 6 set. 2013.

LÉVY, Pierre. **Cibercultura**. Tradução Carlos Irineu da Costa. São Paulo: Editora 34, 1999. Disponível em: <http://www.moodle.ufba.br/file.php/8897/levy_cibercultura.pdf>. Acesso em: 2 mar. 2013.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. 2. ed. São Paulo: Atlas, 2011.

LOPES, José Reinaldo de Lima. **O Direito na História**: lições introdutórias. 2. ed. São Paulo: Max Limond, 2002.

LUCENA, Mariana Barrêto Nóbrega de. O desvio social na rede mundial de computadores: aspectos sociológicos e psicológicos dos indivíduos pertencentes às subculturas criminais da internet. **Jus Navigandi**, Teresina, ano 17, n. 3128, 24 jan. 2012. Disponível em: <<http://jus.com.br/revista/texto/20921>>. Acesso em: 23 mar. 2013.

MACHADO, Luís Antonio; SILVA, Jardel Luís. Crimes digitais: o aumento da complexidade das relações sociais e os novos espaços de intervenção estatal. **Revista do curso de ciências contábeis**, n. 3, Taquara, RS, 2013. Disponível em: <<https://seer.faccat.br/index.php/contabeis/article/download/76/70>>. Acesso em: 20 jun. 2014.

MARINONI, Luis Guilherme. **Efetividade do processo e tutela de urgência**. Porto Alegre: Sérgio Fabris Editor, 1994.

MIRABETE, Julio Fabbrini. **Manual do Direito Penal**. 22. Ed. São Paulo: Atlas, 2005.

_____; FABBRINI, Renato N. **Manual de Direito Penal**. 28. ed. São Paulo: Atlas, 2011. (v. II)

MONTEIRO NETO, João Araújo. **Aspectos constitucionais e legais do crime eletrônico**. 2008. M775a. 191 f. Disponível em: <www.dominiopublico.gov.br>. Acesso em: 15 mar. 2013.

MOREIRA, Rômulo de Andrade. A nova lei sobre a tipificação de delitos informáticos: até que enfim um diploma legal necessário. **Jus Navigandi**, Teresina, ano 17, n. 3443, 4 dez. 2012. Disponível em: <<http://jus.com.br/artigos/23163>>. Acesso em: 18 abr. 2014.

NOGUEIRA, Sandro D'Amato. **Crimes de informática**. 2. ed. São Paulo: BH Editora, 2009.

ORAÇÃO Hacker. Disponível em <<http://forum.imasters.com.br/topic/349848-orao-hacker/>> Acesso em 20 jun 2014.

PEREIRA, Flávio Cardoso. Breves apontamentos sobre a política criminal e o pensamento roxiniano. 2007. Disponível em: <<http://www.lexml.gov.br/urn/urn:lex:br:rede.virtual.bibliotecas:artigo.revista:200>>. Acesso em: 30 jun. 2014.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. ed. São Paulo: Saraiva, 2010.

_____.; HAIKAL, Victor Auilo. A nova lei dos direitos digitais. **Gazeta do Povo**, Curitiba, 12 abr. 2013. Disponível em: <<http://www.gazetadopovo.com.br/vidapublica/justica-direito/artigos/conteudo.phtml?id=1362035&tit=A-nova-lei-de-crimes-digitais>>. Acesso em: 30 jun. 2014.

PINHEIRO, Wecsley dos Santos. Reflexões sobre o campo jurídico a partir da sociologia de Pierre Bourdieu. **Âmbito Jurídico**, Rio Grande, XV, n. 100, maio 2012. Disponível em: <http://www.ambito-juridico.com.br/site/index.php/?n_link=revista_artigos_leitura&artigo_id=11638&revista_caderno=24>. Acesso em: set. 2013.

REALE, Miguel. **Filosofia do Direito**. 20. ed. São Paulo: Saraiva, 2002.

REALE JUNIOR, Miguel. **Instituições de Direito Penal**. 3. ed. Rio de Janeiro: Forense, 2009.

SANTOS, Boaventura de Sousa. **Para uma revolução democrática da justiça**. São Paulo: Cortez, 2007.

_____. **O Discurso e o poder**: ensaio sobre a sociologia da retórica jurídica. Porto Alegre: Fabris. 1988. p. 14.

_____. Notas sobre a história jurídico-social de Pasárgada. In: **Sociologia do Direito**. Rio de Janeiro: Tempo Brasileiro, 1985.

SANTOS, César Augusto dos. Breve abordagem sobre o tema da desjudicialização em busca de alternativas ao descongestionamento do poder judiciário. **De jure – Revista jurídica do Ministério Público do Estado de Minas Gerais**, Belo Horizonte, v. 10, n. 17, p. 259-281, jul./dez. 2011. Disponível em: <<http://acervo.mp.mg.gov.br/ojs/index.php/dejure/article/view/110/19>>. Acesso em: 4 jun. 2014.

SHECAIRA, Sérgio Salomão. **Criminologia**. São Paulo: Revista dos Tribunais, 2004.

_____. **Criminologia**. 3. ed. São Paulo: Revista dos Tribunais, 2011.

SILVA, Antonio Sá. A retórica jurídica e a formação dos juristas: a observação de Aristóteles sobre os argumentos de Ulisses no Filoctetes de Sófocles. **Revista do Programa de Pós-Graduação em Direito da Universidade Federal da Bahia**, ISSN 1516-6058, v. 1, p. 315-322, Salvador, 2008.

_____. Notas das aulas das disciplinas Ética e Responsabilidade Social e Sociologia da Solidariedade, ambas do Mestrado em Segurança Pública da UFBA. Grupo de Discussão no Mestrado em Segurança Pública na EMAB/UFBA. 18 maio 2013. Disponível em: <<http://antoniosa.com.br/topico/16/Grupo+de+Discuss%3Eo+n+o+Mestrado+em+Seguran%27a+P%27ublica+na+EMABUFBA>>.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 33. ed. São Paulo: Malheiros, 2010.

SILVA, Marcelo Mesquita. **Ação internacional no combate ao cibercrime e sua influência no ordenamento jurídico brasileiro**. 2012. 107 f. Dissertação (Mestrado) — Programa de Pós-Graduação *Stricto Sensu* de Mestrado em Direito Internacional Econômico, Universidade Católica de Brasília, Brasília-DF, 2012. Disponível em: <http://www.bdttd.ucb.br/tede/tde_busca/arquivo.php?codArquivo=1691>. Acesso em: 4 jul. 2014.

SILVA, Ovídio Baptista. **Curso de processo civil**. Porto Alegre: Fabris, 1991.

STRECK, Lenio Luiz. **Hermenêutica Jurídica e(m) crise: uma exploração hermenêutica da construção do direito**. 10. ed. rev. atual. e ampl. Porto Alegre: Livraria do Advogado, 2011.

VIANNA, Túlio Lima. **Fundamentos de direito penal informático**. Rio de Janeiro: Forense, 2003.

_____. Hackers: um estudo criminológico da subcultura cyberpunk. In: CERQUEIRA, Tarcísio Queiroz; IRIARTE, Erick, PINTO, Márcio Morena (Coords.). **Informática e Internet: aspectos legais internacionais**. Rio de Janeiro: Esplanada, 2001. p.173-190.

ZAFFARONI. Eugênio Raúl. **Em busca das penas perdidas: a perda de legitimidade do sistema penal**. Tradução Vania Romano Pedrosa, Almir Lopez da Conceição. Rio de Janeiro: Revan, 1991.

ZANELLA, Diego Carlos. A ética comunicativo-discursiva de Jürgen Habermas. **Revista on line de Filosofia Thaumazein**, Ano V, Número 10, Santa Maria, dez. 2012, pp. 131-149.

WOLKMER, Antonio Carlos. **Pluralismo jurídico: fundamentos de uma nova cultura no direito**. 3. ed. São Paulo: Alfa Omega, 2001.