UNIVERSIDADE FEDERAL DA PARAÍBA
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS – CENTRO DE EDUCAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM GESTÃO NAS ORGANIZAÇÕES APRENDENTES

POLIANA POLICARPO DE MAGALHÃES AGUIAR

GESTÃO JURÍDICO-ESTRATÉGICA DO CIBERCRIME NO CONTEXTO DA CIBERDEMOCRACIA

JOÃO PESSOA
2015

POLIANA POLICARPO DE MAGALHÃES AGUIAR

GESTÃO JURÍDICO-ESTRATÉGICA DO CIBERCRIME NO CONTEXTO DA CIBERDEMOCRACIA

Dissertação apresentada ao Mestrado Profissional em Gestão nas Organizações Aprendentes da Universidade Federal da Paraíba (MPGOA/UFPB), linha de pesquisa Gestão de Projetos Educativos e Tecnologias Emergentes, como requisito parcial para obtenção do título de Mestre.

Orientadora: Profa. Dra. Edna Gusmão de Góes Brennand.

JOÃO PESSOA

2015

A282g Aguiar, Poliana Policarpo de Magalhães.
Gestão jurídico-estratégica do cibercrime no contexto da ciberdemocracia / Poliana Policarpo de Magalhães Aguiar. – João Pessoa, 2015.
262p. : il. color.

Dissertação (Mestrado Profissional em Gestão nas Organizações Aprendentes) - Universidade Federal da Paraíba.
Orientadora: Profª. Drª. Edna Gusmão de Góes Brennand.

1. Ciberdemocracia. 2. Cibercrime. 3. Gestão jurídico-estratégica. I. Título.

UFPB/BC CDU: 34:004(043)

POLIANA POLICARPO DE MAGALHÃES AGUIAR

GESTÃO JURÍDICO-ESTRATÉGICA DO CIBERCRIME NO CONTEXTO DA CIBERDEMOCRACIA

Dissertação apresentada ao Mestrado Profissional em Gestão nas Organizações Aprendentes da Universidade Federal da Paraíba (MPGOA/UFPB), linha de pesquisa Gestão de Projetos Educativos e Tecnologias Emergentes, como requisito parcial para obtenção do título de Mestre.

Aprovada em: 30 / de novembro /2015.

BANCA EXAMINADORA

Profa. Dr.ª Edna Gusmão de Góes Brennand
Orientadora (MPGOA/UFPB)

Prof. Dr. Gustavo Rabay Guerra
Membro externo (CCJ/UFPB)

Prof. Dr. Marcílio Franca Filho
Membro interno (MPGOA/UFPB)

AGRADECIMENTOS

Desde a máquina que elimina as distâncias interestelares, até a miúda semente que se desfaz para que o broto rompa o chão; desde o pequeno fio d'água de uma nascente entre os seixos até o engenhoso cérebro eletrônico dos megacomputadores, em cujos cernes habita o silêncio do ciberespaço, aflorando-se, aqui e alhures, na tela plana e solitária de um monitor; ao derredor de tudo isso, há uma demão de amigos, um adjutório providencial.

Com este trabalho não poderia ser diferente. Por ser assim, quero dirigir meu primeiro agradecimento à Fonte Substantiva do Tudo: Deus! A Ele dedico da primeira à ultima linha desta dissertação.

Aos meus familiares rendo agradecimentos pelo jogo lúdico e profético de que tudo terminaria bem. Assim o disseram e assim foi. Minha mãe, a quem minguei as visitas, por pura falta de tempo. Ao meu esposo, Luís Carlos, por compreender minhas ausências, motivadas pelas viagens à Paraíba. À minha para sempre pequena Larissa, cujas faces reclamavam um roçar de afeto e cujos olhos ficaram, muitas vezes, órfãos da minha cumplicidade, por estar eu, quase sempre, entre os muros dos livros que me cercavam.

À Estimada Professora, Dra. Edna que, a despeito de tantos afazeres, não me deixou na orfandade, foi sempre prestimosa em me orientar, ouvir-me, apontar-me o melhor caminho.

Aos companheiros de viagem Iuri, Flávio e Norimá, pela amizade verdadeira e por muitas vezes acordar as manhãs de uma janela de avião, madrugada adentro, num universo de risos e suores.

A todos os colegas e amigos do MPGOA, pela mútua colaboração e pelos ombros assaz disponíveis. Aos colaboradores incansáveis, Miro, Tassyara, Tony e Márcio, pela presteza e atenção constantes.

Enfim, a todos aqueles que estiveram, ainda que anonimamente, mesmo a certa distância, torcendo para que este trabalho chegasse ao estuário da aprovação.

A corroborar o que foi dito, eis Antoine de Sant-Exupéry: "Aqueles que passam por nós não vão sós nem nos deixam sós. Deixam um pouco de si, levam um pouco de nós"

RESUMO

No contexto da sociedade contemporânea globalizada e tecnológica, novas possibilidades de comunicação e acesso ao conhecimento surgem de forma autônoma, por meio das conexões e saberes compartilhados, construindo identidades, especialmente nos campos político e cultural caracterizando a denominada Ciberdemocracia. No entanto, a interconexão de computadores e sistemas, aliada à dependência informática de inúmeros setores, deixa internautas expostos e vulneráveis a ataques virtuais, possibilitando o surgimento dos chamados Cibercrimes. A pesquisa tem como objetivo precípuo investigar as formas de Gestão Jurídico-estratégica do Cibercrime no contexto da Ciberdemocracia, a partir da análise do fenômeno da mundialização, da vasta transformação sociocultural, política e tecnológica e dos problemas jurídicos advindos da massificação intensa do uso da Internet, surgindo, assim, as práticas ilícitas no cenário virtual. Trata-se de uma pesquisa com procedimento metodológico sob uma análise bibliográfica de caráter exploratório e descritivo. Nessa órbita, o estudo ancora-se em referências que tratam, de modo crítico, dos institutos da Ciberdemocracia (como nova forma do agir humano, das interconexões e da construção de saberes, culminando com os movimentos de rua) e dos Cibercrimes (suas tipologias, formas de execução, as faces do anonimato, legislação e processo investigatório).Conclui-se que para alcançar êxito no processo investigativo e na punição dos infratores dos Cibercrimes é preciso criar dispositivos legais que desburocratizem o processo, a obtenção das provas, a aquisição e preservação dos dados, já que, a celeridade na investigação de tais crimes é fundamental para descobrir sua autoria. Diante do exposto, nota-se que as tecnologias e os princípios da sociedade de informação, a democracia da Internet e os crimes cibernéticos são assuntos efervescentes e complexos, tanto para a administração estatal, quanto para a seara jurídica, pois ainda estão sendo redesenhados e estudados. Portanto, depreende-se da análise que as diretrizes de uma gestão jurídico-estratégica eficaz perpassam pela criação de uma força tarefa integrada entre policiais, membros do Ministério Público e magistrados, além de um investimento significativo do governo para a prevenção e defesa cibernéticas, bem como a assinatura de acordos de cooperação internacional no combate à ciberdelinquência. A matéria abordada, por ser de profundo alcance sociojurídico, pode influenciar num futuro, pouco distante, os doutrinadores, legisladores e organismos nacionais e internacionais, para que se busque de maneira específica e decisiva a melhor forma de gestão estratégica na prevenção e combate aos Cibercrimes, mas salvaguardando o ideário novo de democracia cultivado no ciberespaço. Dessa forma, a investigação em curso apresenta uma natureza profícua, podendo contribuir para a busca da segurança na rede, da garantia dos direitos fundamentais e do equilíbrio ético e jurídico na era digital.

Palavras-Chaves: Ciberdemocracia. Cibercrime. Gestão Jurídico-estratégica.

ABSTRACT

Inside the context of a globalized and technological modern society, new possibilities for communication and access to knowledge rises autonomously, through connections and shared knowledge, constructing identity, especially in the political and cultural fields characterizing the cyber democracy. However, the interconnection of computers and systems, combined with computer dependency of numerous sectors, will let the netizens exposed and vulnerable to cyber attacks, enabling the emergence of so-called Cybercrime. The research has as main objective to investigate the forms of legal and strategic Cybercrime management in the context of cyber democracy from the analysis of the phenomenon. The vast social-cultural transformation, political, technological and legal problems arise from intensive mass use of the Internet, emerging thus illicit practices in the virtual scene. It is a survey of methodological procedure under a bibliographical analysis of exploratory and descriptive form. In this orbit, the study is anchored in references dealing, critically, with the institutes of cyber democracy (as a new form of human action, interconnection and the construction of knowledge, culminating in the street movements) and Cybercrime (their types, forms of implementation, the faces of anonymity, legislation and investigative process). It concludes that to achieve success in the investigative process and punishment of violators of Cybercrime is necessary to create legal provisions with less burocratic processes, the taking of evidence, the acquisition and preservation of data, since the speed in the investigation of such crimes is crucial to solve them. Given the above, we note that the technologies and principles of the information society, the Internet democracy and cyber crimes are effervescent and complex issues, both for the state administration, as to the legal harvest, because they are still being redesigned and studied. Therefore, it appears from the analysis that the guidelines of a legal management effective strategy permeate the creation of an integrated task force of police, prosecutors and judges, as well as a significant government investment to prevent and cyber defense, and the signing of international cooperation agreements to combat cyber crimes. The matter is adressed to be of far-reaching in social jurisdiction, and how it can influence in the future, the scholars, legislators and national and international organizations, in order to seek specific and decisive manner. The best way to do a strategic management in preventing and combating cyber crime is safeguarding the new ideas of democracy cultivated in cyberspace. Thus, ongoing research presents a useful nature, contributing to the pursuit of network security, the guarantee of fundamental rights and the ethical and legal balance in the digital age.

Key Words: Cyber democracy. Cyber crime. Legal and strategic management.

LISTA DE ILUSTRAÇÕES

Figura 1 – Movimento “Vem Pra Rua”- Em junho de 2013. 66
Figura 2 – Movimento ocorrido em 15 de março de 2015 69
Figura 3 – Denúncias de crimes na Internet 111
Figura 4 – O perfil da vítima de *sexting* 112
Figura 5 – Site de aluguel de escravo 117
Figura 6 – Site de aluguel de *Hacker* 117
Figura 7 – Site de venda de passaporte falso 118
Figura 8 – Site de venda de livros raros 118
Figura 9 – Site de guia para canibalismo 119
Figura 10 – Acesso de banda larga móvel no mundo 175
Figura 11 – Acesso de banda larga fixa no mundo 175
Figura 12 – Sete estágios das ameaças avançadas na Internet 175

Gráfico 1 – Incidentes no período de 1999 até 2014 177

Quadro 1 – Ataques comuns 89

LISTA DE TABELAS

Tabela 1– Acesso por celular e *tablet*.....174
Tabela 2 – Formas de acesso e suas variações 174
Tabela 3 – Uso do computador para navegar na Internet.....174
Tabela 4 – Total de ataques ocorridos no ano de 2014 178

LISTA DE SIGLAS

ANATEL	Agência Nacional de Telecomunicações
APF	Administração Pública Federal
ARPANET	*Advanced Research Projects Agency Network*
CD Ciber	Centro de Defesa Cibernética do Exército
CERN	Centro de Estudos de Energia Nuclear
CERT	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança
CGI	Comitê Gestor da Internet
CGSI	Comitê Gestor de Segurança da Informação
CIA	*Central Intelligence Agency* (lit. "Agência Central de Inteligência")
CMM	Câmara Municipal de Manaus
CNCP	Conselho Nacional de Combate à Pirataria e Delitos contra a Propriedade
CND	Central Nacional de Denúncias de Crimes Cibernéticos
CNPJ	Cadastro Nacional de Pessoa Jurídica
ComDCiber	Comando de Defesa Cibernética
CONIN	Conselho Nacional de Informática
CP	Código Penal
CPI	Comissão Parlamentar de Inquérito
DDoS	*Distributed Denial of Service*
DNS	*Domain Name System*
DOD	Departamento de Defesa dos Estados Unidos
ECA	Estatuto da Criança e do Adolescente
EGTIC	Estratégia Geral de Tecnologia da Informação e Comunicações
EMBRATEL	Empresa Brasileira de Telecomunicações

ENaDCiber	Escola Nacional de Defesa Cibernética
EUA	Estados Unidos da América
FBI	*Federal Bureau of Investigation*
FEBRABAN	Federação Brasileira de Bancos
FISA	*Foreign Intelligence Surveillance Act*
FTP	*File Transfer Protocol*
G-8	Grupo dos 8 (Estados Unidos, Japão, Alemanha, Canadá, França, Itália, Reino Unido e Rússia)
GCHQ	*Govermente Comunications Headquarters*
GTI	Grupo de Trabalho Interministerial
HTML	*Hiper Text Marked Language*
HTTP	*Hyper Text Transfer Protocol*
IAB	*Internet Architecture Board*
ICANN	*Internet Corporation for Assigned Names and Numbers*
ICCB	*Internet Configuration Control Board*
IETF	*Internet Engineering Task Force*
ILTF	*Internet Law Task Force*
IRTF	*Internet Research Task Force*
ISOC	*Internet Society*
MBL	Movimento Brasil Livre
MCT	Ministério da Ciência e Tecnologia
MLB	Movimento Limpa Brasil
NASA	*National Aeronautics and Space Administration*
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OECD	*Organization for Economic Cooperation and Development*

ONU	Organização das Nações Unidas.
P2P	*Peer-to-peer*
PEC	Projeto de Emenda Constitucional
RNP	Rede Nacional de Pesquisa
SEI	Secretaria Especial de Informática
SIC	Segurança da Informação e Comunicações
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
STJ	Supremo Tribunal de Justiça
TCP	*Transmission Control Protocol*
TCP/IP	*Transmission Control Protocol*/*Internet Protocol*
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
TIP	*Terminal Interface Processor*
UIT	União Internacional de Telecomunicações
URL	*Universal Resource Location*
WWW	*World Wide Web*

SUMARIO

1 CONSIDERAÇÕES INICIAIS 14
2 PARÂMETROS METODOLÓGICOS 19
2.1 PROBLEMÁTICA 19
2.2 JUSTIFICATIVA 22
2.3 OBJETIVOS 23
2.3.1 Objetivo Geral 24
2.3.2 Objetivos Específicos 24
2.4 TIPO DE PESQUISA 24
2.5 FONTES DA INVESTIGAÇÃO 25
2.6 AMOSTRAGEM 26
2.7 ESTRATÉGIAS DE ANÁLISE 27
2.8 DOCUMENTOS UTILIZADOS 28
2.9 ESTUDOS CORRELATOS 29
3 DA CIBERCULTURA AO CIBERCRIME: reestruturando novos espaços sociais na rede 31
3.1 O CONCEITO DE CIBERCULTURA 31
3.2 CIBERESPAÇO E SOCIEDADE EM REDE 36
3.3 AS TECNOLOGIAS NA SOCIEDADE ATUAL 37
3.4 A INTERNET 38
3.4.1 O acesso à Internet no mundo 40
3.4.2 As gerações da Web 41
3.4.3 A Internet e as Interconexões Sociais 43
3.5 A CIBERDEMOCRACIA 47
3.5.1 Democracia e Formação do Espaço Público 48
3.5.2 Ciberdemocracia e Espaço Público Virtual 51
3.5.3 Democracia e racionalidade comunicativa: contribuições para se pensar a Ciberdemocracia 52
3.5.4 Ciberdemocracia: ativismo político-social e vivências na rede 56
3.5.5 Cidadania, Mobilização Social e Construção de Identidades no Ciberespaço 60
3.5.6 Os movimentos de rua no Brasil 64
3.5.6.1 Os Black Blocs e a construção de identidades no ciberespaço 70
3.6 A RELAÇÃO ENTRE CIBERDEMOCRACIA E CIBERCRIME 74
4 TIPOLOGIAS DO CIBERCRIME E TRATAMENTO JURÍDICO-NORMATIVO 79
4.1 O CRIME 79
4.2 OS CIBERCRIMES 80
4.3 CLASSIFICAÇÃO DOS CIBERCRIMES 84
4.4 OS AGENTES DA CIBERDELINQUÊNCIA 86
4.5 CIBERCRIMES COMUNS NO UNIVERSO DIGITAL 90
4.5.1 A espionagem 90
4.5.2 Pirataria 94

4.5.3 Pornografia Infantil e Pedofilia *on-line* 96
4.5.4 Crimes de ódio virtuais 98
4.5.5 O *bullying*, as ofensas à honra e a apologia ao suicídio.. 99
4.5.6 O Cyberterrorismo 105
4.5.7 Fraudes eletrônicas 106
4.6 OUTRAS CONDUTAS ILÍCITAS TÍPICAS NO CIBERESPAÇO 108
4.6.1 Denúncias dos cibercrimes 110
4.7 A DEEP WEB: o submundo do cibercrime 112
4.7.1 O acesso 113
4.7.2 A moeda eletrônica e alguns Cibercrimes cometidos na Deep Web 114
4.7.3 O lado bom da Deep Web 119
4.7.4 Riscos do acesso à Deep Web 120
4.8 A PERMISSIVIDADE NA REDE 120
4.9 LEIS BRASILEIRAS E PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO 127
4.9.1 Lei Carolina Dieckmann e Lei Azeredo 130
4.9.2 Uma análise do processo de inclusão do Marco Civil da Internet na agenda governamental à luz da teoria de múltiplos fluxos de John Kingdon 131
4.9.3 O Marco Civil da Internet 138
4.9.4 A Convenção de Budapeste 143
5 O CASO SNOWDEN: a necessidade de criação de diretrizes para fortalecer a Cibersegurança brasileira 147
5.1 O CASO SNOWDEN: Prolegômenos 147
5.1.1 The True Hooha: um jovem da Carolina do Sul 150
5.1.2 Os jornalistas aliados de Snowden 152
5.1.3 O teor das reportagens e os principais arquivos revelados 156
5.1.4 Os precursores de Snowden: Assange, Ellsberg e Manning 159
5.1.5 Repercussões do caso no Brasil e no mundo 161
5.2 CIBERSEGURANÇA 166
5.2.1 Ciberespionagem e Cibersegurança 167
5.2.2 Novas Diretrizes em Cibersegurança no Brasil 169
6 DA GESTÃO JURÍDICO-ESTRATÉGICA NO COMBATE AOS CIBERCRIMES 173
6.1 A AMPLIAÇÃO DAS INTERCONEXÕES E O CRESCIMENTO DOS CIBERATAQUES 173
6.1.1 Ciberataques importantes no mundo 179
6.1.2 Cibercriminalidade, Globalização e Soberania 182
6.1.3 Cibercrime, Jurisdição, Competência e Transnacionalidade 185
6.2 DA GESTÃO JURÍDICO-ESTRATÉGICA NO PROCESSO INVESTIGATÓRIO 191
6.2.1 Gestão Jurídica 192
6.2.2 O processo de Investigação Criminal no Cibercrimes 194
6.2.2.1 Órgãos que combatem a cibercriminalidade: Polícia Federal, Judiciário e Ministério Público 195

6.2.3 Táticas e desafios na investigação preliminar dos Cibercrimes 199
6.2.4 Diretrizes estratégicas do processo investigatório 205
6.2.5 Gestão jurídico-estratégica no enfrentamento dos Cibercrimes: desafios e perspectivas 215
7 CONSIDERAÇÕES FINAIS 222
REFERÊNCIAS 229
GLOSSÁRIO 244
APÊNDICE A –Tabela de Amostragem nº 1 253
APÊNDICE B – Tabela de Amostragem nº2 254
APÊNDICE C – Tabela de Amostragem nº3 255
APÊNDICE D – Tabela de Amostragem nº4 256
APÊNDICE E – Tabela de Amostragem nº 5 257
APÊNDICE F – Tabela de Amostragem nº 6 258
APÊNDICE G – Tabela de Amostragem nº 7 259
APÊNDICE H – Tabela de Ameaças 260

1 CONSIDERAÇÕES INICIAIS

> *"O ciberespaço impõe uma interface entre o profano e o sagrado; Uma fronteira entre a existência banal do dia a dia, e o espaço eletrônico de circulação do saber."*
>
> (André Lemos)

No contexto da sociedade contemporânea globalizada e tecnológica, novos caminhos e desafios são colocados à vida em sociedade. Essas novas e diferentes possibilidades de comunicação e acesso ao conhecimento, de forma autônoma e através de conexões e saberes compartilhados, possibilitam inúmeros trajetos, não só para a difusão de conhecimento e informação, mas, principalmente, para a construção de identidades.

Essa sociedade não mais se prende ao contexto local, mas tem a perspectiva de novas conexões globais. Esses novos espaços ou ciberespaços, através das configurações em rede, promovem uma relação diferenciada entre emissores e receptores, numa ambiência global, caracterizada pela dinamicidade das relações sociais.

A "Aldeia Global", já desenhada por McLuhan em meados do século passado, transformou-se em uma imensa rede com vastas conexões formando um complexo sistema de informação, descentralização e ausência de limites territoriais e físicos.

Dessa maneira, não há mais como prescindir da Internet, visto que se constitui um ambiente multifacetado, com características específicas, abertura e convergência de várias mídias; também funciona como atrativo para os usuários, que passam a utilizar esse novo meio de comunicação como fonte de expressão de opiniões, gerando debates construindo, neste espaço, afeições e relações sociais.

Nesse sentido, podemos definir esses ciberespaços como um mundo virtual desterritorializante, ou seja, espaços que, mesmo não sendo palpáveis, existem de outra forma, noutra realidade, já que possuem caráter de intangibilidade. Neste sentido, os espaços físicos, rompendo padrões convencionais, foram substituídos pelos espaços etéreos, proporcionando a desmaterialização das relações sociais, ou seja, o que antes era concreto e palpável transforma-se em dimensão imaterial na forma de impulsos eletrônicos, trazendo o mundo virtual como uma nova modalidade de ser.

Toda essa diversidade funcional permeia o cotidiano da humanidade. Todos esses mecanismos tecnológicos são utilizados para diversos fins: sejam eles econômicos, sociais e/ou políticos. Deixar de reconhecer que, na era digital, as relações são moldadas e

estabelecidas a partir da liberdade de acesso à informação e conhecimento, disponíveis nos espaços virtuais compartilhados, seria o mesmo que negar o Estado Democrático de Direito e, com ele, a Democracia.

A interatividade da Internet proporciona o delineamento de uma nova forma de exercício da cidadania a que chamamos de Ciberdemocracia, que possibilita a livre veiculação de conteúdos e o livre manuseio e acesso aos mesmos. Esse acesso fez com que os cidadãos deixassem de ser meros receptores de informações, para se transformarem em produtores de conteúdo. O usuário passou a interagir-se com o mundo e a Internet tornou-se um espaço democrático para troca de informações, criando um território público virtual, onde vários assuntos de importância coletiva podem ser debatidos.

Entretanto, a liberdade virtual e o acesso ilimitado aos ciberespaços, principalmente na esfera privada, fazem surgir um novo modelo cultural, ou Cibercultura, que não se limita a demarcações territoriais, nem se prende a questões temporais, é pluricultural e permite que o conhecimento humano ganhe uma relevância nunca antes vista, tornando-se valoroso, surpreendente e, conforme seja adequadamente utilizado, pode se revelar como um dos maiores bens em favor da humanidade.

Essa sociedade em rede vincula-se a uma nova perspectiva de Estado, o Estado de Vigilância, e assume tipificações e novos modelos sociais, fazendo com que a sociedade da informação viva mudanças conceituais buscando, na Democracia digital, ou Ciberdemocracia, a liberdade necessária para o agir e relacionar-se. Essa liberdade, entretanto, nos moldes do conceito jurídico de liberdade, não é absoluta; porquanto, para que haja uma segurança digital, ou cibersegurança, é necessária uma constante vigilância, seja através de entes públicos ou privados.

Mesmo que a Internet facilite, agilize e amplie a interação entre as pessoas e seja, também, uma grande fonte de informações e conhecimentos entre diferentes usuários e países, ela também pode ser utilizada como meio ou espaço para a prática de condutas ilícitas, dentre elas, os Cibercrimes.

Com base nas questões pontuadas, esta pesquisa tem como objeto de análise um fenômeno tecnológico, cujo tecido constitutivo situa-se na esfera da intangibilidade, no universo da virtualidade e não guarda qualquer semelhança com o palpável, diferente daquilo em que, até pouco tempo atrás, os meios de armazenamento dos saberes e história humanos se constituíam.

A presente dissertação trata da cibernética e de seus nichos e desdobramentos exploratórios no campo social. Os conceitos e exploração contemplados neste trabalho

buscam responder a uma série de indagações a respeito das vantagens, dos avanços conseguidos e do surgimento de subprodutos não desejáveis desta conquista tecnológica. No decorrer deste estudo, observar-se-á que o radical "ciber" irá se unir a outros, formando neologismos, motivos de análises mais aprofundadas nesta pesquisa, tais como: ciberespaço, Ciberdemocracia, cibersegurança, Cibercrime, ciberdelinquência, *cyberbullying*, etc.

A importância do tema em questão – o estudo de grande parte das conhecidas variáveis de "ciber" no campo social – surge do entendimento de que se trata de um fenômeno que permeia o mundo pós-moderno e está presente, mais que nunca, nas relações humanas e nas ligações destas com os cérebros eletrônicos - os computadores - cuja invenção veio transformar e incrementar o universo tecnológico do século XX.

A proposta deste trabalho é fazer uma pesquisa acurada de fenômenos modernos advindos do uso democrático da cibernética e as suas consequências no campo social.

Este estudo é composto de seis capítulos, cuja arquitetura busca traçar um histórico coerente dos elementos constitutivos da pesquisa, analisando-os sob uma ótica crítica, trazendo questionamentos e conclusões lançados por estudiosos do assunto, dentre os quais se destacam Pierre Lévy, Dominique Cardon, Castells, dentre outros.

Após as considerações iniciais, segue o segundo capítulo que trata dos Parâmetros Metodológicos, configurando o problema, as justificativas, os objetivos e o viés exploratório desta pesquisa. As fontes da investigação, aqui centradas nos documentos analisados, a amostragem, a estratégia da análise, sua abordagem didática, bem como seus estudos correlatos também estão delineados neste capítulo.

O terceiro capítulo traz a compreensão do que significa a Cibercultura e o ciberespaço, demonstrando como a rede se reestrutura na configuração de novos espaços sociais. Para tanto, serão exploradas as categorias que fundamentam a construção da cibernética, da Cibercultura e do ciberespaço, bem como do desenvolvimento da Internet, de seus usos e gerações, assim como as interconexões sociais formadas pelo advento da sociedade em rede. Analisaremos o uso dos ciberespaços com seus aspectos positivos e negativos, buscando compreender como esses novos locais de comunicação e fluxo de informação podem influenciar e interferir na (des)construção da Cibercultura, que, facilitada pela convergência digital, poderá construir as bases da Ciberdemocracia. Analisaremos a construção da Ciberdemocracia e do ciberespaço como estrutura pública virtual, verdadeira ágora, onde se torna possível o seu exercício. O ativismo político construído através das redes é compreendido como verdadeira manifestação da Ciberdemocracia, e o uso da linguagem e da comunicação como os amálgamas que possibilitam a existência de sociedades virtuais. Por

fim, debruçar-nos-emos sobre a relação entre a Ciberdemocracia e o Cibercrime e o paradoxo que nos é posto pela liberdade no ciberespaço, destacando-se esta como condição *sine qua non* para a sobrevivência da Ciberdemocracia, mas, também, como um limite para a transparência e segurança dos usuários da grande rede.

No quarto capítulo, abordaremos as questões relacionadas ao Cibercrime, suas tipologias e seu arcabouço normativo-jurídico. Essa abordagem tem como objetivo principal desvendar os mecanismos de execução dos Cibercrimes, bem como a atuação dos agentes da delinquência no ciberespaço, que nos possibilitará entender a personalidade e os padrões comportamentais do fenômeno criminal virtualizado. Nessa linha de entendimento, serão descritos alguns tipos de Cibercrimes, suas especificidades, causas e consequências para a sociedade da informação e para a Ciberdemocracia, examinando algumas espécies, como: a espionagem, a pirataria, a pornografia infantil e pedofilia, crimes de ódio virtual, *bullying*, ofensas à honra e a apologia ao suicídio, ciberterrorismo e fraudes eletrônicas, dentre outros. Após definirmos cada um desses crimes e apresentarmos suas características, meios de prática e formas de combate, faremos um apanhado geral das legislações vigentes sobre o tema, tais como a Lei Carolina Dieckmann, o Marco Civil da Internet e a Convenção de Budapeste. Essa compreensão do arcabouço jurídico normativo e suas carências servirão para abordarmos a permissividade e a dificuldade de punir os agentes criminosos. Aliado a isso, também, serão identificadas que a ausência de legislações específicas sobre tais delitos e a falta de cooperação entre nações revelam-se como sendo grandes obstáculos na luta contra a cibercriminalidade. Analisaremos algumas teorias que tratam da regulamentação da Internet, como as Teorias Anárquicas, a Teoria de Autorregulação, Privada e a Teoria da Regulação Governamental. Para concluirmos o quarto capítulo, trataremos da *Deep Web*, ou Internet profunda, local considerado perigoso e obscuro no ciberespaço que permite ao usuário trafegar de modo anônimo e sigiloso, o que muitas vezes dificulta a identificação dos criminosos, facilitando e/ou permitindo a prática de transações ilícitas no ciberespaço.

O quinto capítulo tratará do caso Snowden e de como este influenciou o governo brasileiro a criar novos órgãos e a traçar um mapa estratégico de cibersegurança no país. Será realizada uma investigação sobre o teor das reportagens e os principais arquivos divulgados na imprensa mundial sobre o caso. Como resultado, enfatizará que a utilização das tecnologias de coleta de dados, para fins de segurança e defesa das nações, é, sim, relevante, desde que haja fundamento jurídico, sensatez e equilíbrio, a fim de não afrontar os direitos mais básicos da personalidade.

Por fim, o sexto capítulo discorrerá sobre as diretrizes de uma gestão jurídico-estratégica no combate ao Cibercrime. A investigação é essencial para a discussão de temas relevantes no terreno da soberania estatal, como Jurisdição e Competência, bem como o passo a passo da investigação preliminar no processo de crimes cibernéticos, mostrando como uma sólida gestão jurídico-estratégica pode interferir e ajudar no combate a estes crimes.

2 PARÂMETROS METODOLÓGICOS

A edificação do conhecimento científico origina-se das indagações, das dúvidas, de uma inquietação perante a realidade, o que no âmbito metodológico denomina-se problema de pesquisa.

> No processo de construção do problema e do próprio conhecimento científico, esta inquietação será o "motor" que conduzirá o pesquisador no seu levantamento de dados, na busca por uma "resposta" - a hipótese - que deverá estar embasada em um marco teórico, em um quadro de leitura que permita ao leitor relacionar este tripé – problema/hipótese/marco teórico - de forma coerente e sistematizada (XIMENES, 2015).

Interpondo-se na conexão do tripé mencionado, encontra-se a metodologia, ferramenta indispensável para dar logicidade científica à pesquisa.

Com o objetivo de alcançar uma melhor desenvoltura da investigação em tela, é necessário percorrer alguns caminhos metodológicos, tais quais: as razões que motivaram o presente estudo, os objetivos pretendidos, a forma de abordagem do problema, os métodos e técnicas utilizados, o tipo de pesquisa, as estratégias de análises dos resultados alcançados e os estudos correlatos empregados.

Abriremos este tópico com a exposição dos motivos que deram origem ao problema.

2.1 PROBLEMÁTICA

A velocidade da informação e as mudanças tecnológicas ocorrem em tal progressão geométrica, que tudo se torna obsoleto numa rapidez estonteante. O conhecimento, óbvio, não é exceção.

Da era industrial em que a Inglaterra se desfez dos teares e do processo de manufatura para implantar sua maquinaria na tecelagem, até o primeiro computador eletromecânico foram quase dois séculos. Daí até os computadores terem a capacidade de armazenar dados de uma cidade, por exemplo, já demandou menos tempo. Hoje, computadores de mesa arquivam dados de um país e, a cada mês, invadem o mercado, mais potentes e mais compactos. Em conjunto com celulares, *smartphones*, *palmtops*, já chegam às lojas com novos protótipos sendo fabricados sob a égide de novas tecnologias e pesquisas em desenvolvimento.

No cenário hodierno, caracterizado por um mundo globalizado e altamente tecnológico, surgem novas trajetórias, modos e distintas formas de aprendizagem em função

das inovações ocorridas na construção, compartilhamento e difusão do conhecimento. Tais transformações possibilitaram não somente uma nova maneira de acesso à informação, mas, também, modificações profundas nos costumes, hábitos e nas culturas de vários povos, que ultrapassaram os limites locais e romperam as barreiras transnacionais.

Nesse raciocínio, Pierre Lévy faz um paralelo entre o crescimento do **ciberespaço** (a rede com novas formas de comunicação oriundas da interconexão de computadores) e o advento da **Cibercultura (**como surgimento de novos valores e práticas provocados pelos avanços tecnológicos, bem como o aparecimento da Internet) (LÉVY, 1999). Para o autor, as novas ambiências virtuais, ou ciberespaços, através das configurações em rede, promovem contatos e relações diferenciadas entre emissores e receptores que podem trilhar diferentes caminhos possíveis, construindo suas próprias trajetórias.

O Ciberespaço, quebrando padrões convencionais de circunscrição proporcionou a desmaterialização das relações sociais. Esse mundo virtual está sustentado em quatro pilares primordiais, a saber: o tempo real, a desterritorialidade, a imaterialidade e a interatividade. Os referidos pilares permitem a simultaneidade das relações sociais e o acesso imediato a qualquer ponto do globo, trazendo à baila uma nova percepção do tempo, do espaço e, principalmente, das interações sociais. A simbologia que esse novo mundo digital apresenta é marcada por uma nova sociabilidade, diferenciada pelo participante e por novas relações entre vários seres humanos em todos os continentes (WIKIEDUCAÇÃO, [2012]).

A fluidez de ir e vir nesse espaço virtual, da confluência de relações na globosfera, favorece a construção da Ciberdemocracia (LIMA, 2012)[1].

Nos últimos tempos, acontecimentos sociais marcantes estiveram sob os holofotes da mídia no Brasil e no mundo. Um deles ocorreu ao longo do mês de junho de 2013 com força e expressão populares nunca antes vistas, um movimento social arquitetado nas redes sociais, com ímpeto disseminador e agregativo, a ponto de tomar de surpresa lideranças políticas, civis e militares, bem como envolver a sociedade como um todo. As ruas foram tomadas por amplos protestos, tendo, no seu espectro, jovens, adultos e idosos. O estopim inicial do movimento seria a redução das tarifas de transporte público e, em alguns casos, sua gratuidade. Dessa primeira motivação, o movimento se agigantou em tamanho e objetivo, variando para outras demandas mais complexas e amplas nas reivindicações, tais como: mau uso do dinheiro público, gastos do governo para financiar a Copa do Mundo, em detrimento de ações, cuja implementação situava-se num nível imediato de prioridade. Dentre as mais

[1] http://www.sbu.unicamp.br/seer/ojs/index.php/rbci/article/viewFile/518/pdf_24

discutidas e citadas, estiveram em destaque a saúde e toda a sua infraestrutura hospitalar, a educação e a segurança, através de temáticas presentes em cartazes, discursos e outros meios de expressão explorados nas passeatas. Outro tema bastante abordado foi a corrupção e suas consequências na corrosão do erário público.

O movimento foi-se notabilizando e tomando grandes proporções em diversas capitais. Esta mobilização popular tornou-se uma das maiores da história do país, desde a inquietação das "Diretas Já" em 1985. Em algumas cidades, a pressão popular foi tamanha que obrigou governantes a reduzirem os preços de passagens e a reverem algumas decisões políticas, dentre elas, a eliminação do 14° e 15° salários para Deputados, bem como a derrubada da Proposta de Emenda Constitucional - PEC 37.

Embora a força do movimento tenha-se esvaído, restringindo-se, sobretudo, ao mês de junho, foi um notável exercício de cidadania, tanto que veio a se emergir em 2015, com um cronograma mais bem definido de eventos. Assim, em 15 de março deste ano, um movimento intitulado de "Vem pra Rua" tomou todo o país com protestos e reivindicações. A Polícia Militar estimou que mais de dois milhões de pessoas participaram das passeatas que, vale a pena ressaltar, se concretizaram dentro de um clima de ordem e conscientização, diferentes das de 2013, quando atos de vandalismo depredaram patrimônios públicos e privados.

Estas manifestações foram propositadamente exploradas para evidenciar o papel das diversas redes sociais, facultadas pelo fenômeno da Ciberdemocracia. Neste sentido, a Ciberdemocracia tem se mostrado o caminho mais acessível e poderoso para se discutir temas de fundamental importância para as sociedades.

Paralelamente a este fenômeno, não podemos ignorar que, como espaço de troca de realidades e sentidos complexos, o ciberespaço pode tornar-se um meio para a prática de condutas lesivas e ilícitas, praticáveis e praticadas, na Internet.

A interconexão de computadores e sistemas, aliada à dependência da informática por todos os setores, deixa muitos internautas expostos e vulneráveis a ataques virtuais, pois, a cada dia, aumenta a dependência da sociedade da informação aos sistemas informativos, o que possibilita que o Cibercrime se torne frequente, habitual, internacional e perigoso.

Ainda no mês de junho de 2013, outro acontecimento de destaque movimentou, por muito tempo, o cenário midiático brasileiro e mundial: um ex-funcionário terceirizado da CIA expôs ao mundo a conduta americana na rede, comprovando práticas ilegais e antiéticas dos Estados Unidos. A repercussão foi tão imediata e de tal monta, que nações atingidas, dentre elas o Brasil, requereram do país norte-americano explicações para a conduta considerada de espionagem, levantando questões fundamentais sobre o conceito de democracia e de crime

nas redes. Estaria o ciberespaço a facultar atitudes contrárias à privacidade e até à soberania das nações?

Edward Snowden, em reportagem ao jornal britânico The Guardian, deu detalhes da operacionalidade das agências de informação ianques e seu super programa de monitoramento e espionagem, o PRISMA. Confirmou o que muitos já suspeitavam: os norte-americanos buscam vigiar, controlar e espionar os mais diversos cidadãos ao redor do mundo.

É perfeitamente perceptível que, nas pegadas deixadas pelo uso democrático das redes de dados e de outros territórios virtuais, um substrato indesejável vem formar uma intercessão incômoda com a referida Ciberdemocracia através do Cibercrime.

Dessa forma, pode-se constatar que a Internet alterou, drástica e definitivamente, a vida de muitos navegantes. A sociedade, de modo geral, tornou-se dependente dela, o que potencializou e efetivou a globalização (culminando na "aldeia global"), possibilitou a ampliação de espaços democráticos de atuação, mas também constituiu-se em espaço e meio ampliados e complexos para a prática de condutas ilícitas.

Resta, diante de tudo que foi explanado, uma inquietação que se poderia traduzir no seguinte questionamento: Como identificar as formas de Gestão Jurídico-estratégica do Cibercrime no atual contexto da Ciberdemocracia?

2.2 JUSTIFICATIVA

A revolução ocorrida com o aprimoramento das tecnologias da informação e comunicação, acompanhada do fenômeno da globalização, permitiu uma ampla interação entre os seres humanos. A evolução tecnológica e informacional vinculada à grande rede de computadores em escala mundial popularizou o acesso à informação, facilitou a inclusão digital e contribuiu, de certa forma, para a promoção da diversidade cultural, delineando uma nova forma de exercício da democracia.

Entretanto, esta vasta transformação sociocultural, política e tecnológica, também desencadeou problemas jurídicos advindos da massificação intensa do uso da Internet, surgindo, assim, os Cibercrimes e as práticas ilícitas no cenário virtual. Nesse sentido, desenvolver um estudo crítico sobre a Ciberdemocracia (como nova forma do agir humano e da construção de saberes) aliado a uma pesquisa analítica sobre os Cibercrimes (suas espécies, forma de execução e gestão estratégica de prevenção) é de significativa importância para o meio acadêmico, notadamente, nas searas sociojurídicas. O presente estudo trata de uma reflexão acerca das bases que sustentam a Ciberdemocracia e da necessidade ou não do

controle dos Cibercrimes no cerne virtual por meio dos marcos regulatórios instituídos em escala nacional e global, com o objetivo de normatizar o ciberespaço, indo de encontro às premissas libertárias da Internet, especialmente, a que defende a publicação livre e a não regulação.

Contudo, não desmerecendo as pesquisas existentes sobre o assunto, verifica- se que há uma escassez de estudos voltados à análise conjunta dos dois fenômenos: Ciberdemocracia e Cibercrimes, notadamente nos tempos atuais em que se confundem liberdade de pensamento e de expressão com mensagens de ódio, ofensas à honra e à imagem das pessoas, chegando ao extremo do Ciberterrorismo.

Sendo assim, justifica-se a pesquisa em foco, pela relevância da temática no atual contexto da Sociedade de Informação e Comunicação. Quanto ao aspecto científico, o tema proposto constitui centro de muitas discussões e críticas tanto no âmbito nacional quanto internacional. É uma matéria que desperta curiosidade e indagações em muitos juristas, sociólogos, antropólogos, cientistas políticos e filósofos, sendo, portanto um estudo interdisciplinar, alcançando uma abordagem ampla, sob diferentes enfoques.

A pesquisa aborda o tema com originalidade e atualidade, uma vez que se utiliza da combinação e adequação das mais diversas doutrinas de natureza filosófica, social, política e histórica em conjunção com outras advindas dos vários ramos do Direito, especialmente do Direito Penal e do Direito Digital.

Espera-se que as questões abordadas ao longo da pesquisa, por se inserirem em uma seara fértil de análises sociais, jurídicas e políticas, possam contribuir com alternativas que busquem uma melhor forma de gestão estratégica na prevenção e combate aos Cibercrimes, salvaguardando o ideário novo de democracia cultivado no ciberespaço. Tal mister científico poderia contribuir dirimindo as dúvidas e injustiças, conferindo maior segurança aos direitos dos usuários das tecnologias de informação e comunicação no Brasil e em outras partes do globo. Dessa forma, a investigação em curso apresenta uma natureza profícua e busca contribuir para encontrar meios que facultem a segurança na rede, garantia dos direitos fundamentais e equilíbrio ético e jurídico na era digital.

2.3 OBJETIVOS

Nesta seção, apresentam-se os objetivos que visam responder o problema de pesquisa.

2.3.1 Objetivo Geral

- Investigar as formas de gestão jurídico-estratégica do Cibercrime no contexto da Ciberdemocracia.

2.3.2 Objetivos Específicos

- Mapear as categorias teórico-conceituais para se pensar a respeito da Ciberdemocracia e o Cibercrime;
- Estabelecer as principais tipologias do Cibercrime e suas legislações;
- Verificar a partir do "caso Snowden", a necessidade da criação de diretrizes governamentais para se fortalecer a cibersegurança.
- Identificar formas de gestão jurídico-estratégica na prevenção dos Cibercrimes.

2.4 TIPO DE PESQUISA

Na elaboração de uma pesquisa, é indispensável procurar conhecer quais os recursos necessários à construção do embasamento teórico, uma vez que este é fundamental para o bom desenvolvimento da investigação. Assim, há tipos diferenciados de pesquisa na busca ou obtenção de dados.

Para Oliveira (2002, p. 62) "a pesquisa tem por objetivo estabelecer uma série de compreensões a fim de construir respostas para as indagações e questões levantadas nos diversos ramos do conhecimento humano".

Na presente dissertação, a pesquisa é de natureza exploratória que, aliada a uma reflexão crítica, permitirá um melhor entendimento e uma abordagem inovadora sobre o tema.

A pesquisa exploratória é aquela que permite ao investigador sondar, ventilar ideias e aprofundar-se sobre determinado conteúdo. O estudo exploratório surge como uma ferramenta estratégica para desvendar um assunto que foi pouco estudado ou, ainda, é pouco explorado, permitindo ao pesquisador, conforme enfatiza Gil (2010, p.27), uma maior familiaridade com o objeto pesquisado.

Ela também necessita, à semelhança de outros tipos de pesquisa, de uma fonte bibliográfica e de algum conhecimento anterior, ainda que exíguo. Nas pesquisas, de modo geral, costumam-se estudar, de forma exploratória, obras, observar entrevistas com pessoas

em situações parecidas, ou analisar exemplificações semelhantes para alcançar uma melhor compreensão do problema. A exploração de um determinado tema pode resultar no aprofundamento de mais conhecimentos ou no surgimento de abordagens inovadoras (ANDRADE, 2002). Desse modo, resumidamente, conforme os ensinamentos de Raupp e Beuren (2003, p.80), "[...] explorar um assunto significa reunir mais conhecimento e incorporar características inéditas, bem como buscar novas dimensões até então não conhecidas."

Destarte, uma pesquisa de cunho exploratório deve ensejar alguns fins específicos como: o acúmulo de informações sobre algum tema investigado; a facilitação da delimitação temática; a orientação na elaboração dos objetivos e hipóteses; e o auxílio para a inovação do enfoque sobre o tema explorado. Quando a pesquisa se enquadrar num dos casos acima, será considerada exploratória.

A pesquisa exploratória visa oferecer diretrizes para a elaboração de trabalhos acadêmicos, cumprindo esclarecer que, para não desvalorizar as pesquisas desta natureza, o pesquisador deve examinar a temática de modo diferenciado, apresentando uma nova abordagem ou tratamento, evitando, assim, a mera repetição ou transcrição do tema, conforme realizado por outros autores ou estudiosos.

2.5 FONTES DA INVESTIGAÇÃO

As fontes de investigação da presente pesquisa são as bases de dados sobre Ciberdemocracia e Cibercrime no Brasil, em língua portuguesa, em espanhol e em inglês. A fonte utilizada é, em grande parte, bibliográfica e documental, preferencialmente, de caráter multi e interdisciplinar (já que ainda é bastante difícil encontrar fontes transdisciplinares). Foram incluídas, num primeiro momento, referências no âmbito da Cibercultura e da Ciberdemocracia, como Pierre Levy, André Lemos e Manuel Castells, em paralelo com as contribuições teóricas de Habermas para o desenvolvimento de uma nova cultura democrática.

Numa segunda seção, foram utilizadas fontes doutrinárias na área do Direito Digital da autora Patrícia Peck Pinheiro, dos crimes cibernéticos, ameaças e procedimentos de investigação dos autores Emerson Wendt e Higor Vinícius Nogueira Jorge. Outrossim, também foram estudados livros que tratavam da segurança na rede e dos crimes virtuais e suas vítimas de autoria de Luciano Gonçalves Carvalho e Moisés de Oliveira Cassanti. Foram estudadas obras estrangeiras, como as de autoria do argentino Diogo F. Migliorisi (Crímenes

em La Web- Los delitos Del sieglo XXI- Argentina) e da autora inglesa Misha Glenny (Dark Market-Cyber Cops and you), dentre outras.

Foram utilizadas também as legislações e jurisprudências nacionais e de outros países sobre o assunto, a exemplo dos EUA, Portugal, Espanha, França, Alemanha, dentre outros.

2.6 AMOSTRAGEM

Para a concretização do estudo, foi importante estabelecer uma amostra dos principais artigos, teses e dissertações sobre o assunto. A busca foi feita em 4 sites acadêmicos distintos: Google Acadêmico, Biblioteca Digital da USP, Biblioteca Digital da Unicamp e Scielo. Restringiu-se a pesquisa aos anos de 2012 a 2015, em razão de relevantes mudanças e acontecimentos em nível nacional e internacional sobre o tema nesse triênio.

Foram utilizadas as seguintes categorias para busca: Ciberdemocracia, Cibercrime, crimes virtuais, democracia na Internet, crimes no ciberespaço e crimes na Internet. Todas elas foram pesquisadas em aspas, para que os resultados fossem mais precisos em relação ao assunto.

Alguns critérios foram utilizados para a seleção dos artigos mais relevantes, tais como a similaridade do tema e a qualidade acadêmica da pesquisa. Foram pesquisadas também as mencionadas categorias nos idiomas inglês e espanhol. Os resultados são a seguir apresentados.

O site que mais apresentou resultados foi o Google Acadêmico. Ao digitar, ali, a categoria "Ciberdemocracia" para pesquisa, foram encontrados 587 resultados em português. Alguns dos mais relevantes estão descritos na tabela de amostragem nº 1, constantes do Apêndice A.

Digitando a categoria "Cibercrime", no mesmo site, foram obtidos 134 resultados em português. Alguns dos mais relevantes constam da tabela de amostragem nº 2, conforme Apêndice B.

Lançando no instrumento de busca as categorias "Crimes no Ciberespaço", foram encontrados 10 resultados em português, sendo relevante a tabela de amostragem nº 3, conforme Apêndice C.

Utilizando as categorias "Crimes na Internet" no site em tela, encontraram-se 105 resultados, em língua portuguesa. Os mais relevantes foram os dispostos na tabela de amostragem nº 4, conforme Apêndice D.

Com as categorias “Democracia na Internet” ainda no site em questão, foram encontrados 20 resultados em língua portuguesa, sendo os mais importantes descritos na tabela de amostragem nº5, conforme Apêndice E.

Utilizando a categoria “Cybercrime” no Google Acadêmico, foram conseguidos 11.500 resultados, do período de 2012 a 2015, sendo relevantes alguns textos em língua inglesa, como os que integram a tabela de amostragem nº 6, conforme Apêndice F.

Ao digitar a categoria “Ciberdelincuencia” no Google Acadêmico, foram registrados 266 resultados, do período de 2012 a 2015, sendo relevantes em língua espanhola os distribuídos na tabela de a tabela de amostragem nº 7, conforme Apêndice G.

2.7 ESTRATÉGIAS DE ANÁLISE

A análise de dados foi realizada através da comparação dos materiais utilizados para a pesquisa, tais como livros, artigos, dissertações, teses e legislações, identificando-se os pontos convergentes e divergentes entre os posicionamentos adotados pelos autores pesquisados com o objetivo de responder ao problema proposto por esta investigação.

A fim de sistematizar os dados obtidos no corpo da investigação em comento procedeu-se à análise crítica dos fundamentos teóricos e conceituais abordados pela dissertação, notadamente as categorias relacionadas em cada capítulo do presente trabalho.

Na parte destinada ao conhecimento das categorias de análise centrais, Ciberdemocracia e Cibercrime, buscou-se compreender a evolução histórico-conceitual de democracia e as contribuições de Habermas na crítica ao modelo representativo liberal e na construção de um novo saber utópico democrático.

Analisaram-se ainda as bases centrais da Ciberdemocracia, o ativismo político nas redes, os movimentos de rua, ou seja, a Ciberdemocracia no contexto brasileiro, chegando a relacioná-la ao Cibercrime em meio a algumas indagações e incertezas na atualidade.

No alcance do estudo específico dos Cibercrimes, foram investigados os agentes, modos de execução e as espécies delituosas mais comuns, para, de modo sistêmico, identificar os mecanismos que cercam a ciberdelinquência.

No trabalho, foi essencial analisar os conceitos e técnicas desenvolvidos para compreender a importância da Ciberdemocracia nesse novo contexto da sociedade de Informação.

Em decorrência da inovação da análise do tema no mundo jurídico e científico-político, mostrou-se necessário fazer a contextualização da discussão desde a formação do

ciberespaço e do surgimento da democracia virtual, abordando as principais questões que envolvem tal temática, passando pelos principais crimes cibernéticos, bem como por uma análise minuciosa da legislação em vigor.

Foi traçada uma investigação aprofundada acerca do Marco Civil, buscando compreender, à luz da teoria de Kingdon, a razão de o referido compêndio legal ter figurado como prioridade na agenda política do governo, após as denúncias de espionagem norte-americana em 2013.

Analisou-se também a principal legislação internacional aplicada ao tema (Convenção de Budapeste), tomando como objeto de estudo o "caso Snowden" e sua repercussão no mundo, especialmente no Brasil, com a criação de aparatos estratégicos para fortalecer a segurança nacional. Foi descrita, por fim, a estratégia jurídica dos agentes brasileiros no combate ao Cibercrime, bem como as formas de prevenção e controle na atualidade.

Ao final, buscou-se responder quais são as formas de gestão jurídico-estratégica no combate ao Cibercrime, no atual contexto ciberdemocrático.

2.8 DOCUMENTOS UTILIZADOS

Para a efetivação deste trabalho, foi utilizada, de forma suplementar, a técnica de pesquisa documental. Assim como a pesquisa bibliográfica, a documental revela-se como um instrumento de apoio a toda e qualquer pesquisa. A distinção entre elas reside na natureza das fontes. A bibliográfica vale-se das contribuições de inúmeros autores, já a documental refere-se a materiais que ainda não foram analisados ou que passaram por uma reelaboração. "Nestes casos, os conteúdos dos textos ainda não tiveram qualquer tratamento analítico, são ainda matéria-prima, a partir da qual o pesquisador vai desenvolver sua investigação e análise" (SEVERINO, 2007, p. 123). A pesquisa documental apresenta a vantagem de que os documentos constituem uma fonte rica e estável de dados e sobrevivem ao longo do tempo.

Os documentos referidos podem ser oriundos de órgãos públicos ou de instituições privadas, tais como: Câmara, Senado, Tribunais, associações científicas, sindicatos, partidos políticos e etc (LAKATOS; MARCONI, 2010).

Foram realizadas, na construção da pesquisa em referência, a análise dos seguintes documentos de natureza jurídica:

a) Documentos nacionais:

- Constituição da República Federativa do Brasil;
- Código Civil;

- Código de Defesa do Consumidor;
- Código Penal;
- Código de Processo Penal;
- Estatuto da Criança e Adolescente;
- Lei "Carolina Dickman" de 12.737/2012 que se transformou num marco para a história das legislações acerca do *cyberbullying*. A lei tipifica condutas no ambiente virtual que são classificadas como delitos informáticos principalmente referentes à invasão de computadores ou aparelhos digitais, dados de comunicações privadas e informações sigilosas, bem como estabelece punições específicas;
- **Marco Civil da Internet**-A Lei 12.965, de 23 de abril de 2014, sancionada pela presidente Dilma Rousseff, "estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil" (BRASIL, 2014, art. 1). Revela-se como sendo uma espécie de Constituição digital. O Marco regulatório tramitou por dois anos na Câmara dos Deputados. Foi apresentado, inicialmente, não como um texto de lei, mas como uma indagação à sociedade, a respeito do que se desejaria no tocante à regulação da Internet.

b) Documentos Internacionais

- **Convenção de Budapeste**-Também intitulada"Convenção sobre o Cibercrime", foi firmada pelo Conselho Europeu, em 23 de novembro de 2001, celebrada em Budapeste – Hungria. Teve 43 Estados signatários, estando aberta a assinatura para todos os países do Mundo. A Convenção de Budapeste tem como objetivo facilitar, por meio da cooperação internacional, a prevenção e punição dos "infratores virtuais".

2.9 ESTUDOS CORRELATOS

Com o objetivo de realizar uma pesquisa interdisciplinar nas áreas de Ciência Política e Direito, foram selecionados e lidos artigos sobre Cibercrime e Ciberdemocracia, produzidos no período que corresponde aos anos de 2012 a 2015 e que estejam disponibilizados na rede, conforme se enuncia a seguir.

No Google Acadêmico, utilizando a categoria Cibercrime, foram encontrados 138 resultados em língua portuguesa, tratando os mais relevantes sobre temas como: crimes virtuais, ameaças e procedimentos de investigação, pedofilia, ausência de privacidade, preconceito, discriminação e pornografia. (MELO NETO, 2012; LUZ; CASTRO, 2013; SANTOS, 2015; CAROCA; BEZERRA; BEZERRA, 2013; PORDEUS, 2014; SANTOS, 2013; FORTES; BOFF, 2014; NASCIMENTO; SILVA, 2014).

No mesmo site, utilizando a categoria Ciberdemocracia, foram encontrados mais de 500 resultados em português, tratando dos mais relevantes sobre temas como: ágora virtual, blogosfera, marco civil e redes sociais. (OLIVEIRA; RODEGHERI, 2012; LIMA, 2012; CABALLERO, 2013; GROSSELLI, 2012; BARRETO, 2012; OLIVEIRA, 2012; SILVA, 2014; RODEGHERI; SANTOS; OLIVEIRA, 2012).

Foram encontrados também estudos correlatos em língua espanhola, a respeito da“Ciberdelincuencia” e em língua inglesa, sobre o “Cybercrime”, respectivamente, a exemplo de Sesé, 2014; Alvarez e Egaña, 2012; Baker e Lewis, 2014; Soudijn e Zegers, 2012.

3 DA CIBERCULTURA AO CIBERCRIME: reestruturando novos espaços sociais na rede

A reformulação e o repensar de conceitos podem ser constantes nas Ciências Sociais, porquanto moldados nos seios das transformações em que vivem as sociedades. Entretanto, ainda que evidente este caráter dinâmico dos conceitos desta natureza e suas múltiplas faces na construção dos saberes humanos, precisamos delimitá-los a fim de conferir maior clareza ao pensamento que se quer formular e possibilitar a elucidação de seu conteúdo, uma vez que o grau de veracidade advindo destas formulações é tanto mais abalizado quanto mais claras forem as suas disposições.

Para tanto, falaremos sobre o contexto e formação da Cibercultura, compreendendo o ciberespaço como *locus* privilegiado de sua formação para, em seguida, através da compreensão do conceito de convergência digital, pensarmos os novos contornos de espaços públicos democráticos que contribuirão para a formação da Ciberdemocracia, caracterizada pela mundialização econômica e cultural, acompanhada da era das Tecnologias da Informação e do Conhecimento, numa verdadeira praça virtual.

3.1 O CONCEITO DE CIBERCULTURA

O paradigma comportamental entre a interação de seres humanos e matérias não orgânicas está presente nas artes e narrativas humanas há longo tempo. O ser humano sempre criou e imaginou seres e objetos inspirados em sua imagem numa clara associação entre homem e máquina. Na mitologia grega, Pigmaleão esculpe uma estátua (FERNANDES, 2005) que ganha vida e se torna humana. No folclore judaico, o Golem (SINGER, 1982) é um ser feito de matéria inanimada que ganha vida. Em 1918, Mary Shelley publica, ainda que sem créditos, "Frankenstein", muitos dizem que a obra inspirada pelo mito de Golem (SHELLEY, 1997, p. 90). Em 1738 Vaucanson cria um pato mecânico que é capaz de bater as asas, alimentar-se sozinho e digerir a própria comida.

No fim da década de 50, o matemático estadunidense Norbert Wiener publica *Cybernetics: or the Control and Communication in the Animal and the Machine (1948)*. A obra traz os resultados da hipótese de que certas funções de controle e de processamento de informações seriam semelhantes em máquinas e seres vivos, bem como equivalentes e redutíveis aos mesmos modelos e às mesmas leis matemáticas. Assim, a teoria da simbiose entre o orgânico, o humano e a matéria ganha contornos científicos sob a ótica da cibernética.

Wiener (1984) entendia que a Cibernética seria um novo campo da ciência que incluiria não somente o estudo da linguagem, mas também o estudo das mensagens como forma de dirigir as máquinas e a sociedade, pautado pelas reflexões acerca da psicologia e do sistema nervoso. Wiener (1984) explica que a criação do termo *cybernetics* (cibernética), deriva do grego *kubernetes,* que significa piloto ou timoneiro, aquele que possui o controle, o governo da situação. Neste sentido, o timoneiro controlaria o navio tornando-se um só, construindo-se, assim, a relação entre o homem e a máquina.

A cibernética caracteriza-se por possuir uma forte interatividade entre sistemas de controle e processamento de informações, bem como a surpreendente aproximação entre os seres vivos e máquinas, expressada, destacadamente, conforme nos ensina Colli (2010, p. 24):

> [...] no avanço das pesquisas envolvendo o uso de tecnologias de mimetismo da vida — robótica, biônica \e nanotecnologia. Nesse campo do conhecimento, a relação entre maquinas. organismos humanos e textos — enquanto narrativa científica e informação fornecida na forma de linguagem para funcionamento e construção de *softwares* de computadores — supera limites clássicos de classificação que opõem a natureza (in)orgânica entre máquinas e homens .

A cibernética idealizada por Wiener (1984), embora não tenha se consolidado no plano científico como uma teoria das mensagens entre o corpo e a máquina, estimula hipóteses, novas teorias e pesquisas nos mais diversos campos da ciência, como a informática, a robótica e a ciência da informação. A cibernética também influencia a cultura moderna com modelos explicativos, consolidando, por exemplo, a compreensão do que hoje chamamos de Cibercultura.

Em sendo assim, seria despropositado, para não dizer inconcebível, um trabalho científico que, ao se propor tratar de questões sociais que se agregam à cibernética – ou seja, aos cibers, não se ocupar, também, de uma vertente assaz importante como é a Cibercultura, com seus potentes e variados tentáculos em todos os territórios do conhecimento humano.

A ideia que nos é dada pela cibernética de que há uma mistura da organicidade dos corpos humanos com a máquina também nos traz uma noção de que desta junção resulta a produção de novas formas de vida, onde a relação entre organismo e máquina sob a forma de textos, códigos e linguagens conduz a uma narrativa científica, a valores e culturas que se formam e se modificam nesta junção.

Entretanto, é um equívoco limitar-se o conceito de Cibercultura a uma simples junção do radical "ciber" – de cibernética - a um conceito simplista de cultura como um "cabedal de conhecimento de uma pessoa ou grupo social" ou, tão somente, ao "[...] complexo de

atividades, instituições e padrões sociais ligados à criação e difusão das belas-artes, ciências humanas e afins" (HOUAISS, 2009, p.583).

Definir "Cibercultura" é uma tarefa que demanda uma série de análises prévias, tendo em vista a extensão da sua abrangência e de possibilidades no cotidiano das pessoas e dos seus diferentes espaços de formação. Senão vejamos.

Lévy (2010, p.17) trata o termo como neologismo – afirmando que "[...] Cibercultura especifica aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço". Em sendo assim, pode-se afastar uma definição que se atenha ao reducionismo de entender Cibercultura como um conjunto de saberes acadêmicos veiculados pelas redes, ou tratados pela cibernética.

Convém dizer que a Cibercultura vai muito além de uma simples cultura tecnológica, ou pelo menos patrocinada pela tecnologia. Ela agrega elementos diversos e complexos, é um vasto constructo de alternativas e realidades que ultrapassa a visão simplista do que seja artes, ciências, conceitos ou valores veiculados em redes sociais. Ela consiste na verdadeira apropriação e transformação destes.

Neste sentido, Lemos (2014, p.18) defende que há três princípios fundamentais oriundos do fenômeno da cibercultura que resultam na: A) liberação do pólo de emissão, ou seja, a conversação na esfera global foi ampliada por meio de novos sistemas e instrumentos de comunicação (*blogs*, redes sociais, *wikis*, etc.). Em função da liberação da palavra, houve "o aumento da esfera pública mundial e da emergência de novas formas de conversação e de veiculação da opinião pública, agora também planetária". (LEMOS, 2014, p.25). No contexto dessa cultura pós-massiva, pode-se, concomitantemente, ser leitor e, também, produtor de conhecimento. B)A liberação da emissão desencadeia outro princípio, a chamada "inteligência coletiva", que conforme explica Levy é "[...] uma inteligência distribuída por toda parte, incessantemente valorizada, coordenada em tempo real, que resulta em uma mobilização efetiva das competências". (LEVY, 2003, p.28) a interação das informações e das comunicações de modo interconectado mundialmente, uma interconexão planetária, ou seja, a emissão da palavra só faz sentido se for propagada coletivamente. C) o terceiro princípio é o da reconfiguração cultural social e política. "Há, portanto, uma reconfiguração do sistema infocomunicacional global, onde, pela primeira vez, aparecem dois sistemas de retroalimentação e conflito: os sistemas infocomunicacionais massivo e pós-massivo". O primeiro é relevante, pois ajuda a formar o público, dando "um sentido de comunidade de pertencimento local, de esfera pública enraizada. O sistema pós-massivo permite a

personalização, o debate não mediado , a conversação livre, a desterritorialização planetária" (LEMOS, 2014, p. 26).

O que afirma André Lemos, professor da Universidade Federal da Bahia, vem ao encontro do discorrido por Lévy (2010, p. 19) sobre a Cibercultura, quando este escreve que "[...] se trata de uma nova forma de universalidade que inventa, [...] as perturbações que suscita na relação com o saber [...]".

A Cibercultura é instrumento de grande alcance social, com um ímpeto construtivo inimaginável, possibilitando uma teia de expansão de poderes capaz de, a par de conflitos naturais nas relações travadas nesse espaço virtual, construir uma nova forma de ver o mundo.

Destarte, podemos afirmar que o term**o** Cibercultura tem vários sentidos, mas podemos compreendê-lo como a forma sociocultural que advém de uma relação de trocas entre o ser humano, a sociedade, a cultura e as novas tecnologias. Isto, porque a compreensão do que significa a Cibercultura demanda adentrar um território povoado de análise a respeito de "hipertexto", ciberespaço e aprofundamentos sobre universalidade e totalidade.

Essa ambiência virtual é, a cada segundo, porto de acolhimento, estuário de inserções de textos, informações, imagens, formando, no final, um texto macro, chamado de hipertexto, algo poroso, fluido que permite ser vazado por outras tantas informações que nada mais são que subproduto das outras, numa reconstrução contínua de significados, o que lhe confere uma riqueza de produções incalculável, uma espécie de "sinfonia de Babel" no dizer de Lévy (2010, p. 110).

Ainda sob a visão de Lévy (2010, p. 109), "as pesquisas sobre as interfaces de navegação são orientadas, direta ou indiretamente, pela perspectiva última de transformar o ciberespaço em um único mundo virtual, imenso, infinitamente variado e perpetuamente mutante."

Essa imensidão que constitui o tecido virtual do ciberespaço, continuamente em mutação, com um viés labiríntico e de segura mobilidade, confere-lhe um caráter de universalidade. Todavia é uma universalidade livre, sem cunho de pragmatismo, sem conotação de posse desse ou daquele viés de pensamento, vontade ou ideologia. Esse desprovimento de compromisso com quaisquer correntes possíveis vai contribuir para se entender Cibercultura como algo em construção, mutável, dinâmico. Nada que se refira a uma cultura de per si veiculada pela rede que usa o ciberespaço.

Cibercultura é algo mais abrangente, universal no sentido de que tecida a um sem-número de mãos e, por isso mesmo, ela vai ser um produto inacabado, com práticas "reconfigurantes", em que, na sua edificação, qualquer tijolo é bem-vindo.

Acerca do caráter universal da Cibercultura, Amadeu (*online*[2]) afirma que:

> Cibercultura é universal, sem ser totalizante, todos podem ter acesso à rede, mas não para propagar um mito, proferir uma lógica, um credo, uma ideologia. Cibercultura é uma cultura composta de vários pedaços de culturas nacionais, culturas globais, prolifera através da e na expansão da Internet, com liberdade dos fluxos.

Assim, Amadeu, seguindo as ideias de Lévy trata dessas duas características de um modo muito didático e claro, dirimindo qualquer dúvida e retirando do termo Cibercultura a ideia tentadora de limitá-la a conhecimentos acadêmicos ou mesmo um modo de viver ou pensar de um povo em particular. Neste sentido, completa Lévy (2010, p.113) que "essa universalidade desprovida de significado central, esse sistema da desordem, essa transparência labiríntica, chamo-a de 'universal sem totalidade'. Constitui a essência paradoxal da Cibercultura".

É claro que as comunidades virtuais se sedimentam nas afinidades, nos modos de pensar pautados em identidades semelhantes, interesses convergentes, apreciações similares e etc. Mas também é verdade que não é isso apenas a que se pode chamar de Cibercultura, senão uma conjuminância desses blocos comunitários, dessas aldeias de pensamentos e ações. Esse entrelaçamento de territórios, de vontades, de modos de ver, tudo isso forja uma outra realidade que, por si, vai alimentando outras mais e tecendo essa malha sinérgica de uma estrutura Cibercultural.

Lévy (2010) traça um perfil histórico da caminhada das culturas através do tempo, sob a ótica da universalidade e totalidade da Cibercultura, dividindo-as em etapas:

> - a das pequenas sociedades fechadas, de cultura oral, que vivem uma totalidade sem ser universal;
> - a das sociedades "civilizadas", imperialistas, usuárias da escrita, que fizeram surgir um universal totalizante;
> - e, por último a da Cibercultura, correspondendo a da globalização concreta das sociedades, que inventam um universal sem totalidade (LÉVY, 2010, p.113).

Como se pode deduzir do exposto, a Cibercultura é o que se pode chamar de fenômeno capaz de demolir o desenho vertical das culturas, permitindo que por ali não só transitem os conhecimentos, os modos de vida, os padrões e valores, mas que suscite o milagre da reconfiguração para conceber o novo, com sentido, numa progressão e afã sem precedentes.

Enfim, a Cibercultura está longe de ser um produto acabado que tenha um inventor, um autor, ou que esteja pronta e posta em prateleiras para ser servida ao gosto de uma

[2] https://www.youtube.com/watch?v=eqJG9xmb0KE

demanda qualquer. É, sim, um processo de construção continuada, mutante, um tecido estampado numa policromia de vontades, entendimentos, valores, culturas e modos que, finalmente, perfazem um todo com sentido, reinventando-se a cada instante.

E arremata Lévy, apresentando- nos o veículo para essas possibilidades:

> Eis o ciberespaço, a população de suas comunidades, a ramificação entrelaçada de suas obras, como se toda a memória dos homens se desdobrasse no instante: um imenso ato de inteligência coletiva, sincrônica, convergindo para o presente, clarão silencioso, divergente, explodindo como uma ramificação de neurônios. (LÉVY, 2010, p.114).

Deste modo, não há como dissociar o termo Cibercultura de ciberespaço, porquanto este é uma espécie de líquido amniótico onde se gesta e se move a Cibercultura.

3.2 CIBERESPAÇO E SOCIEDADE EM REDE

As linguagens, quer sejam no âmbito do léxico, quer sejam nas suas formas icônicas de se estabelecerem, não escaparam da avalanche de alterações que o mundo contemporâneo impinge; também se modificam ao longo do tempo. Neste raciocínio, Lévy (2010, p.94) registra que "a palavra ciberespaço foi inventada em 1984 por William Gibson em seu romance de ficção científica *Neuroromancer".* No livro, esse termo designa o universo das redes digitais.

Na obra de Gibson (2003), o ciberespaço é uma alucinação consensual vivida diariamente por bilhões de operadores autorizados, em diferentes nações. Trata-se de uma representação gráfica abstraída dos bancos de dados de todos os computadores do sistema humano.

Num contexto atual o ciberespaço é comumente confundido com a Internet. Não devemos trocar os conceitos. A Internet, como conjunto de redes de computadores, é a base material onde se desenvolve o ciberespaço.

Podemos afirmar que o ciberespaço é um espaço móvel, paradoxal, um local invisível onde circulam conhecimentos, saberes e potências de pensamento num mundo virtual desterritorializante, ou seja, espaços que, mesmo não sendo palpáveis, existem de outra forma, noutra realidade. Eles estão em um local indefinido, desconhecido, com possibilidades que não se mostram como os espaços presentes nos computadores, tampouco nas redes, já que possuem caráter fluido (MONTEIRO, 2007).

Neste sentido, o ciberespaço é um mundo virtual onde são disponibilizados variados meios de comunicação e interação em sociedade, com dados, informações e conhecimentos mixados a imagens, sons, e hipertextos, de durabilidade incerta presentes em tempo real ou não.

É correto afirmar que seu advento trouxe à humanidade ganhos incalculáveis, quer na esfera científica, quer na teia vasta das relações humanas, aí se contabilizando mais liberdade, mais inclusão, mais possibilidade de troca de saberes. Todas estas transformações ocorreram em função da mundialização de uma nova cultura, especialmente em razão da velocidade das informações, das novas relações de comunicação e de produção do conhecimento.

Nesse contexto de ciberespaço, em que a rede de computadores fez surgir uma cultura *on-line*, os sistemas utilizados na educação humana, estão, portanto, sendo profundamente alterados. A agregação de tantos conteúdos com tamanha liberdade por todo o globo, no que se refere ao ciberespaço, faz com que se tenha a impressão de que não existem limites para reproduzir informações.

Castells (2007, p. 21) define esta sociedade que ocupa este ciberespaço como "sociedade em rede", ou seja, uma sociedade que utiliza as novas tecnologias como instrumento de informação, comunicação, articulação social, transformação e desenvolvimento em um espaço virtual desterritorializante.

Uma das características dessa sociedade é desconsiderar tempo e o espaço, já que tudo está conectado e interligado. Esta é uma sociedade em que o novo torna-se passado numa fluidez muito grande. Consequentemente, as mudanças que geram desenvolvimento instantâneo estão em todos os campos, sejam eles políticos, culturais ou econômicos. Assim, as transformações ocorrem a partir das novas tecnologias sem perder a interdependência global.

3.3 AS TECNOLOGIAS NA SOCIEDADE ATUAL

A tecnologia que viabilizou a viagem da sonda "New Horizons", da NASA- *National Aeronautics and Space Administration*, através de uma escalada cósmica de nove anos, por entre os desvãos de planetas e satélites, a se imiscuir na vida do nosso distante Plutão, expondo-lhe a face recoberta de gelo, tirando dele o silêncio do segredo, entregando ao mundo fotos, cujos ângulos de tomada atestam o quão inabitável aparenta aquele astro é a mesma que permitiu, em 20/05/2015, pesquisadores desvendarem e decodificarem um pergaminho de 1.500 anos, nos quais se encontram trechos bíblicos com teor praticamente idêntico ao disponível nas edições bíblicas

atuais. Com diversos usos e possibilidades, as tecnologias nos permitiram enxergar e pensar o mundo de forma diferente.

A tecnologia nos permite viajar e compreender mundos nunca antes visitados. Permite-nos, por exemplo, que mesmo sem possibilidade de nos deslocarmos fisicamente a uma cidade, possamos ter a oportunidade de vislumbrar os seus contornos, ou, ainda que a desconhecendo, possamos, através de um *smartphone*, utilizando-se do GPS, chegar ao endereço desejado ou mesmo escapar de um congestionamento. Ou, estando a quilômetros de distância, através de teleconferência, ouvir um professor ministrar aula com um nível de funcionalidade e saldo cognitivo bem próximo aos conseguidos numa exposição presencial, como o fazem os cursos universitários presenciais conectados, por exemplo. Também é verdade que, atualmente as microcâmeras e canetas espiãs estão sendo usadas como elementos probatórios. Além disso, já há no Brasil, atendimento médico a pacientes moradores em regiões não assistidas por profissionais de saúde especializados numa ou noutra área, realizado através de teleconsultas.

Dentro, portanto, dessa esteira de feitos concebida pela tecnologia, entre as quais a invenção/advento do computador, o ser humano se coloca como ator e sujeito de possibilidades dentre as quais, indubitavelmente, se destaca a Internet com todos os seus desdobramentos. Em prol da formação de uma globosfera, até desaguar na construção de uma sociedade do ciberespaço- tempo etereamente impalpável, mas que, como uma lembrança marcante, boa ou má - para onde quer que se vire, ela marca presença. É inegável que, embora composta de horizontes fugidios, mas envolventes e inexoráveis, a sociedade do ciberespaço é real e, por conseguinte, inegável.

Sendo assim, o efeito mais marcante da era da tecnologia é a Internet. Dentro dessa realidade, pode-se afirmar que se vive agora um tempo de quebra de paradigmas e eliminação de fronteiras, um momento de estreita ligação entre a tecnologia da informação digital e as expressões culturais.

O certo é que a tecnologia é uma realidade imperativa, que não admite qualquer esboço de transigência, tanto porque facilita o fluxo das tarefas, quanto pelo que carrega de confortável ao dia a dia das pessoas.

3.4 A INTERNET

A Internet é uma rede de computadores interligada virtualmente que permite a interconexão descentralizada de computadores através de um conjunto de protocolos denominado TCP/IP – *Transmission Control Protocol*/*Internet Protocol*. Originou-se de um

projeto militar do governo norte-americano, no princípio da Guerra fria, especialmente após o lançamento do satélite russo Sputnik em 1957 (primeiro objeto criado pelo ser humano posto à órbita terrestre) (PINTO)[3]. Preocupados com o avanço da nação rival, os EUA passam a aprofundar seus estudos no campo da comunicação.

Na década de 60, os norte-americanos desenvolveram um sistema em que, caso houvesse um ataque bélico, os computadores militares poderiam trocar informações entre si, de uma base a outra, preservando, assim, os dados. Foi então que surgiu uma rede, a *ARPANET*, criada pela *ARPA*, sigla para *Advanced Research Projects Agency Network* ou Agência de Pesquisa de Projetos Avançados, uma subdivisão do Departamento de Defesa dos Estados Unidos (CHATFIELD, 2012).

A *ARPANET* começou a funcionar em 1969, conectando-se a quatro endereços: Universidade da Califórnia (Los Ángeles), Stanford Research Institute, Universidade da Califórnia em Santa Bárbara e Universidade de Utah. A rede cresceu velozmente e em 1971, o primeiro correio eletrônico foi emitido por ela. Ressalta-se ainda que, dois anos depois, foi criado o método pioneiro de transferência de arquivos (File Transfer Protocol-FTP).

A palavra Internet surge pela primeira vez em 1974 num artigo escrito por Vinton Cerf, Yogen Dalal e Carl Sunshine. Tais estudiosos formulam e apresentam duas terminologias relevantes para o desenvolvimento da Internet: Internet *Protocol* (IP) e Trasmission Control Protocol (TCP). O TCP-IP facilitou a conexão entre redes e máquinas, compartilhando arquivos, dados e permitindo a movimentação do correio eletrônico (CHATFIELD, 2012).

Por oportuno, é bom salientar que, nos anos 70 e 80, a Internet passou a ser um importante meio de comunicação acadêmico. Professores, pesquisadores e estudantes universitários, inicialmente nos EUA, depois mundialmente, passaram a interagir, expondo suas dúvidas, compartilhando ideias, bem como apresentando descobertas e soluções científicas.

Na década de 90, a Internet passa a permear o mundo, alcançando a população em geral. Nesta fase, conforme ensinam Dullius, Franco e Hipller (2012)[4]:

> A Arpanet foi desmantelada em 1990 sendo substituída pela Nsfnet, popularmente conhecida como Internet. A Internet se tornaum sistema mundial público de redes de computadores, podendo ser conectado por qualquer pessoa ou computador, previamente autorizado. Robert Caillaiu e Tim Berners-Lee, ambos os engenheiros do CERN – Centre Eoropéen por La Recherche Nuclaire, do HTML – HiperText

[3] http://brasilescola.uol.com.br/historia/sputnik.htm
[4] http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html

> Markup Language e dos *Browser*s criaram a WWW – *World Wide Web* – esta que foi decisiva para o crescimento da Internet.

Houve, dessa forma, uma considerável transformação com sites mais velozes, criativos e visualmente atrativos. Logo depois, foram criados o HTML- *Hiper Text Marked Language*, o HTTP- *Hyper Text Transfer Protocol* e as poucas primeiras páginas no CERN- *Centro de Estudos de Energia Nuclear*, na Suíça. O Web *Browser* Mosaic 1.0 foi lançado em 1993. No ano seguinte, já se consolidava um crescente interesse público pela Internet.

No Brasil, a era da Internet começa tardiamente, no ano de 1991, com a chamada Rede Nacional de Pesquisa-RNP. Tratava-se de uma operação acadêmica subordinada ao MCT (Ministério da Ciência e Tecnologia). Saindo das fronteiras acadêmicas no período entre 1994-1995, as páginas da Internet vão, gradualmente, alcançando o restante do público. Nesta época, por iniciativa do Ministério das Telecomunicações e Ministério da Ciência e Tecnologia, ocorre a abertura da Internet ao setor privado, havendo uma importante melhora da velocidade fazendo com que a rede avançasse, sendo inclusive, utilizada para o comércio. No final da década de 90, ocorre uma expansão de provedores de acesso. No início do século XXI, mais de 600 milhões de pessoas estavam conectados à rede. E, em 2007, esse número passou a ser de um bilhão e 234 milhões de usuários (DULLIUS; FRANCO; HIPLLER, 2012)[5].

> Enquetes realizadas pelo Ibope Media revelam que, em 2013, o Brasil possuía 105 milhões de internautas, tornando-se o 5º país mais conectado do mundo. As estimativas são que, em até final de 2015, a nação ocupe o 4º lugar, ultrapassando o Japão. Segundo estudos realizados pela Fecomércio-RJ/Ipsos, o número de brasileiros conectados à Internet aumentou de 27% para 48%, no período entre 2007 e 2011. A *lan house* vem em primeiro lugar (31%), como o principal local de acesso. Em seguida, o local de residência do próprio usuário (27%), bem como a residência de parente ou de amigos, com 25%. (G1, 2013)[6]

3.4.1 O acesso à Internet no mundo

A expansão da Internet permitiu toda essa movimentação da aldeia global, com a simultaneidade de informações entre as pessoas por todo mundo, transmitindo mensagens, imagens e conhecimento.

No ano 2000, havia 400 milhões de pessoas conectadas à Internet no mundo. Atualmente, são 3,2 bilhões. A maior parte dessas pessoas está em países emergentes – para cada internauta morando em um país desenvolvido, há dois nos países emergentes. Apesar

[5] http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html

[6] http://g1.globo.com/mundo/noticia/2013/08/entenda-o-caso-de-bradley-manning-condenado-por-vazar-segredos.html

desse avanço, mais da metade da população mundial ainda está fora da Internet e apenas em seis países, todos europeus, o número de assinaturas fixas excede 40%. No continente Europeu, 82,1% das casas já possuem conexão à rede, enquanto que, no continente Africano, apenas 10,7%. (G1, 2015)[7].

O contraste é grande: enquanto países como Noruega, Dinamarca e Islândia têm mais de 90% da população conectada, nos países em desenvolvimento, a média da população que acessa à Internet é bem mais baixa: cerca de 35% - porcentagem pequena, ainda mais se comparada a certas regiões extremamente urbanizadas na China, onde a União Internacional de Telecomunicações (UIT) verificou mais de três assinaturas móveis de banda larga por habitante, segundo a Organização das Nações Unidas (ONU, 2015)[8].

O relatório anual da UIT, sobre o uso de banda larga no mundo, mostrou que, 57% da população mundial ainda não tem acesso à Internet. Segundo a ONU, houve avanços, mas estes foram extremamente desiguais. De 2014 para 2015, 300 milhões de pessoas conquistaram o acesso à rede mundial de computadores, somando 3,2 bilhões (ONU, 2015).

A conexão móvel cresceu ainda mais consideravelmente no mundo. A UIT afirma que, em 2000, eram 738 milhões de assinaturas de conexão móvel no globo terrestre. Atualmente, são mais de 7 bilhões. A justificativa é que essa forma de acesso é mais ampla – em 2015, os planos 3G cobrirão 69% da população mundial (G1, 2015)[9].

3.4.2 As gerações da Web

O mundo virtual vai-se transformando gradualmente, com a participação a cada ano de novos internautas, novos programas e a criação de aparatos tecnológicos mais avançados. Um importante marco desta fase ocorreu em San Francisco, no ano de 2004. Trata-se do Congresso Web 2.0 encabeçado por Tim O'Reilly, um grande *expert* do universo tecnológico. O referido evento procurou discutir e analisar a evolução da Web. Preleciona Chatfield (2012, p. 44)

> cómo la Web ha evolucionado hacia una robusta plataforma para La innovación a través de muchos medios y dispositivos-desde el teléfono móvil hasta la televisión, desde el telefono hasta el buscador. La clave de la respuesta estaba en el usuário: girando alrededor de la capacidad de buscar, crear, recopilar, compartir y categorizar

[7] http://g1.globo.com/mundo/noticia/2015/07/pergaminho-hebraico-de-1500-anos-e-decifrado-gracas-tecnologia.html
[8] http://www.dji.com.br/diversos/declaracao_universal_direitos_humanos.htm
[9] http://g1.globo.com/mundo/noticia/2015/01/programa-de-espionagem-vazado-por-snowden-esta-ligado-muitos-paises.html

> contenidos, interconectar estas actividades, y hacerlo todo en un entorno virtual cada vez más rico.

Nas duas últimas décadas, a Internet evoluiu consideravelmente. Houve um crescimento relevante no tocante aos dados, aos usuários, aos programas e novas tecnologias que proporcionaram uma desenvoltura significativa na Web.

Chatfield (2012) vem corroborar o entendimento teórico de que a Web evoluiu de modo surpreendente, semelhante a um programa dinâmico, rico em versões e preciso no tocante às suas características. Tal processo evolutivo é considerado uma etapa, uma geração.

Segundo Sabino (p. 38, 2007)[10]:

> É consensual que a Web 1.0 foi a primeira geração da Web. Nesta fase, a principal preocupação era a própria construção da Rede, torná-la acessível e comercializável. As áreas de interesse centravam-se no acesso à Internet através de ISPs, nos primeiros *web browsers*, em protocolos como o http e o XML, na criação de sites e portais, etc..

A Web 2.0 destaca-se, primordialmente, pela possibilidade de os usuários dialogarem, exporem suas ideias por meio de uma plataforma consideravelmente interativa que é o *blog*. Instaura-se, nesta fase, a cultura da colaboração *on-line*, da participação em massa, do trabalho social em rede (redes sociais, como o *Orkut, facebook, twitter*), dos *bookmarks* (marcadores sociais), da captação de notícias, da busca, da pesquisa.

Um dos exemplos mais contundentes desta inovação é a *Wikipedia*, introduzida em 2001 como uma enciclopédia virtual com informações de alcance universal, implementada por voluntários que ajudam a mantê-la.

Observa-se, nessa fase, a consolidação da autonomia e da liberdade dos usuários, como participantes ativos na cultura digital, já que, antes, o espaço virtual possuía menor mobilidade, com pouca interação, reservado aos *experts* com programas e protocolos mais específicos e técnicos.

A terceira geração da Internet denominada de Web 3.0, assim batizada por John Markoff em 2006, surge caracterizada por apresentar uma interação maior entre o computador e o ser humano, especialmente no campo da linguagem, facilitando o diálogo entre eles justamente por proporcionar a utilização e organização das informações de modo perspicaz. Essa terceira geração é chamada de "Web inteligente", ou seja, na visão de Sabino (2007), seria:

[10] www.cin.ufpe.br/~hsp/Microsoft-web.pdf

> [...] um tipo de Web, em que os conteúdos podem ser registrados de maneira a serem compreendidos, interpretados e processados por determinados agentes de software, os quais passam a pesquisar, partilhar e integrar a informação disponível de uma forma mais eficiente.

Trata-se de uma das características da Web semântica, em que é possível organizar e utilizar os dados e informações de modo mais preciso e inteligente. A Web 3.0 tem a missão de conectar informações, já a Web 2.0 tinha a função de conectar pessoas. A Web semântica, assim designada, permite a participação e cooperação entre o usuário e a máquina.

Diante da evolução das ferramentas e usos da Internet, depreende-se que, desde a concepção do computador moderno por Turing, acompanhado do processo rápido das informações e sua forma quantificável revelada por Claude Shannon e Maxwell, o universo virtual já se modificou muito e continuará a fazê-lo.

Os cientistas e estudiosos do tema investigam novas maneiras de manipular informações para realizar novas revoluções no atual contexto. A atual geração pode utilizar qualquer aspecto do universo físico para estabelecer a ordem e surpreender com novos usos e potencialidades a serem reveladas com o poder da informação. E, assim, o conhecimento humano ganha relevância nunca antes vista, tornando-se valoroso, surpreendente e, conforme seja adequadamente utilizado, revela-se como um dos maiores bens em favor da humanidade.

3.4.3 A Internet e as Interconexões Sociais

Aprofundando o estudo das tecnologias de informação e suas interconexões sociais, continuaremos a estudar a Internet, destacando sua importância como um marco na teia das relações sociais do mundo contemporâneo.

Segundo Castells, entre o final do século passado e o limiar deste, três processos autônomos desencadearam um novo modelo baseado em redes:

> As exigências da economia por flexibilidade administrativa e por globalização do capital, da produção e do comércio; as demandas da sociedade, em que os valores da liberdade individual e da comunicação aberta tornaram-se supremos; e os avanços extraordinários na computação e nas telecomunicações possibilitados pela revolução microeletrônica. Sob essas condições, a Internet, uma tecnologia obscura sem muita aplicação além dos mundos isolados dos cientistas computacionais, dos hackers e das comunidades contra culturais, tornou-se a alavanca na transição para uma nova forma de sociedade-a sociedade em rede-, e com ela para uma nova economia (CASTELLS, 2003, p.8).

Diego Vecchio, escritor argentino, numa entrevista a Claufe Rodrigues para a Globonews, na Festa Literária Internacional de Paraty afirma que:

> Há uma possibilidade de viajar, sem viajar (efetivamente) com a Internet. É a circulação da informação, que é muito distinta, uma aceleração também, uma saturação de informação, e isso fez com que os espaços locais estejam mais deslocalizados do que antes. Digamos que qualquer ponto do planeta pode entrar em contato com outro ponto, de um modo muito mais fácil do que antes (VECCHIO).[11]

Assim, as possibilidades transformadoras da Internet incluem a desvinculação entre território como meio físico, instituindo um ciberespaço em que a questão da localização não seja pressuposto básico para a sociabilidade. O formato de interação humana passa por um redesenho em que não há limitações territoriais.

Há quem sustente que essa imersão no mundo virtual tem levado o indivíduo a um perigoso isolamento, podendo culminar num "[...] colapso da comunicação social e da vida familiar, na medida em que indivíduos sem face praticam uma sociabilidade aleatória, abandonando ao mesmo tempo interações face a face em ambientes reais" (CASTELLS, 2003, p. 98).

Assim, há duas importantes questões a serem consideradas: uma é o isolamento propriamente dito; a outra é a advento da figura sem face, a faculdade do anonimato, que pode dar margem a comportamentos danosos a outras pessoas. Entende-se que, à medida que não haja exposição da pessoa real, o fictício pode representar um perigo à sociedade como um todo.

É provável que esse silêncio do anonimato esteja, por outro lado, ligado a uma profunda necessidade de se veicular ou "disseminar uma imagem de uma identidade que não possui, pela vontade de pertencer a um grupo maior dominante e, em muitos casos, completamente distinto daquele que constitui, na verdade" (TAVARES; BARBOSA; SANTOS, 2015).

Essa necessidade de ser aceito no grupo está bem clara no quadro da Hierarquia das Necessidades desenhado pelo psicólogo americano Abraham Maslow. Ele desenvolveu um gráfico, muito claro e didático, para expressar as necessidades humanas, suas abrangências e seus patamares.

> Depois de satisfeitas as necessidades fisiológicas e de segurança, começará a emergir como dominante a necessidade *social* ou de *participação* na estrutura hierárquica das necessidades. [...] as pessoas são seres sociais, sentem necessidade

[11] <www.globosatplay.globo.com/glonoews/V/4330299/>.

> de pertencerem a vários grupos e de serem aceitas por estes (HERSEY; BLANCHARD, 1986, p. 34).

Elisabeth Noelle-Neumann, pesquisadora alemã, após um estudo pormenorizado, entre 1965 e 1972, a respeito de um segmento do eleitorado alemão que mudava, na reta final das campanhas, o seu voto, lançou-se numa pesquisa, em que detectou um fenômeno das relações sociais na comunicação a que chamou de "A teoria da espiral do silêncio". Trata-se de um comportamento tal que, ante opiniões entendidas como dominantes, grupos minoritários acabam por se capitular e tender a seguir as escolhas e orientação da maioria, que, muitas vezes, nem sempre representa a sua opção. A sede por pertencer a um grupo e por ele ser aceito pode levar o comportamento do internauta a se enquadrar nessa "tendência cíclica ao silêncio" (TAVARES; BARBOSA; SANTOS, 2015)[12].

Ainda sobre esse silêncio e esse anonimato, Sherry Turkle, pioneira dos estudos de construção da identidade na Internet, é bem enfática ao explicar tais posicionamentos, concluindo que não há uma alienação proposital naqueles posicionamentos. Tanto assim, que assegura:

> [...] a noção do real existe. As pessoas que vivem vidas paralelas nas telas são, não obstante, limitadas pelos desejos, a dor e a mortalidade de suas pessoas físicas. As comunidades virtuais oferecem um novo contexto alegórico em que se pensar sobre a identidade humana na era da Internet [...]. Em suma a representação de papéis é uma experiência social válida, mas não constitui uma proporção significativa da interação social da Internet hoje (TURKLE apud CASTELLS, 2003, p. 100).

O que é possível afirmar a respeito do papel da Internet na vida cotidiana é que, analisando prós e contras (como as questões que envolvem o "vício", o anonimato, o silêncio para auscultar a opinião da maioria) o efeito é positivo nas interconexões sociais, bem como há um ganho na construção e no acesso do conhecimento, no senso de liberdade, além da relevante fluidez que os *e-mail*s possibilitam na comunicação com amigos, familiares, colegas de trabalho etc.

Há, portanto, uma empatia na construção de laços entre os internautas, ainda que não sejam fortes, ainda que, vez por outra, a figura que se apresenta do outro lado não seja, efetivamente, aquela que está espelhada, em palavras, pensamentos e fotos, no monitor da máquina à sua frente. Hoje a Internet está integrada à vida profissional e pessoal da sociedade, apesar de ainda não termos uma total inclusão digital, o mundo virtual é uma realidade que mudou tanto a forma de pensar e agir como a de comunicar-se.

[12] http://revistas.ucg.br/index.php/panorama/article/view/3457/2026

Entretanto, a capitulação do homem a esse facilitador, abalou, inclusive, a psique humana, chegando ao território das fobias. Nas ruas, onde quer que estejam, as pessoas, em geral, estão sempre "plugadas", a tal ponto de haver correntes que sustentam a tese de que a tecnologia aproximou distâncias, mas distanciou os indivíduos, posto que grande parte do nosso tempo cotidiano é gasto em mensagens recebidas, ligações telefônicas, *e-mail*s a serem enviados ou lidos e interações em redes sociais.

A tal forma isso se estabeleceu que o permanecer todo o tempo conectado ultrapassou os limites do que se pode chamar de hábito sadio e se tornou um vício: a "nomofobia". Este neologismo resulta da junção de três radicais, sendo "no" referente a "não", "mo" de "móvel" e "fobia", de origem grega, que significa "medo exagerado". Trata-se da "fobia de ficar sem um aparelho de comunicação móvel", com sintomas que vão desde confusão mental, isolamento, até outros somente verificados em usuário de drogas.

Em um artigo escrito por Christiane Lima[13], a autora revela dados interessantes sobre esse novo vício:

> Em fevereiro, um estudo realizado com cerca de mil pessoas no Reino Unido, país onde a palavra "nomofobia" surgiu em 2008, revelou que 66% dentre estes se diz "muito angustiado" com a ideia de perder seu celular. Em outra pesquisa, desta vez com jovens da Universidade de Maryland, nos EUA, constatou-se que a dependência de celulares, computadores e tudo que esteja relacionado à tecnologia pode ser considerada semelhante ao vício em drogas. O estudo avaliou 1.000 alunos com idades entre 17 e 23 anos, em dez países, que ficaram durante 24 horas sem celulares, redes sociais, Internet e TV. Segundo a pesquisa, 79% dos estudantes avaliados apresentaram desde desconforto até confusão e isolamento com a restrição ao uso de eletrônicos. Outro sintoma relatado foi o de coceira, uma sensação parecida com a de dependentes de drogas que lutam contra o vício. Alguns estudantes relataram, ainda, estresse simplesmente por não poder tocar no telefone. Pela primeira vez, vício na rede foi comparado com o abuso de outras coisas, como drogas e álcool.

Consoante o que é explanado acima, não seria de todo despropositado assegurar que a tecnologia acaba por exercer uma forte ingerência no comportamento humano, que, grosso modo, poder-se-ia entender nociva numa análise superficial. O poder das tecnologias possibilita a cada dia que a sociedade desenvolva, por meio de uma nova arquitetura infraestrutural, mecanismos que possam moldar os contornos das sociedades futuras.

A tecnologia é hoje alvo de apropriação, transformação e experimentação. A Internet é uma espécie de tecnologia de comunicação e quando ela é utilizada como modelo de interação e aproximação, torna-se um novo padrão sociotécnico, caracterizado pela maleabilidade, tornando-se uma constante prática social.

[13] http://elo.com.br/portal/colunistas/ver/228318/nomofobia--sera-que-voce-tem-e-nao-sabe-.html

Entretanto, a Internet, ao fornecer as bases para a criação do ciberespaço e para o aprofundamento de uma Cibercultura, mais que promover interconexões sociais e novas linguagens de comunicação, possibilitou o desenvolvimento das bases de uma nova cultura democrática a Ciberdemocracia de que trataremos a seguir.

3.5 A CIBERDEMOCRACIA

Ciberespaço, Cibercultura e Ciberdemocracia são conceitos interconectados que favorecem o processo de inteligência coletiva que resulta do compartilhamento, da colaboração e da integração dos indivíduos nos espaços virtuais. Ao formular novos saberes, através da Cibercultura, no ciberespaço, os seres humanos constroem verdadeiras comunidades virtuais, abrindo novos espaços de comunicação.

A governança, necessariamente, passa pelo ciberespaço, segundo nos ensina Lévy (2002), porquanto este é um lugar que propicia o desenvolvimento de múltiplas linguagens humanas e a democracia, utiliza-se inevitavelmente do uso da linguagem.

Uma vez que o ciberespaço pressupõe maior liberdade, ele se torna de suma importância para o exercício da expressão, com todas as vantagens dela advindas, revelando-se um campo profícuo para o exercício da cidadania. Neste sentido:

> A extensão do ciberespaço nos leva, em um mesmo movimento, a mais liberdade (individual e coletiva) de uma parte; e a mais comunicação e interdependência de outra. O crescimento da liberdade é evidente: o ciberespaço permite uma liberdade de *expressão e comunicação* em escala planetária absolutamente sem precedentes (LEMOS; LÉVY, 2010, p. 52).

Entretanto, ao falarmos em inserção no ciberespaço por parte do cidadão, que passa a contribuir para a Cibercultura e posterior surgimento da Ciberdemocracia, não podemos perder de vista os problemas enfrentados pela exclusão digital e que constituem verdadeiros obstáculos para o pleno desenvolvimento das expectativas ciberdemocráticas.

Os desafios que nos são lançados pelo exercício da Ciberdemocracia não podem ser analisados sem um estudo prévio da compreensão de sua formação e exercício, que discutiremos nos tópicos a seguir.

3.5.1 Democracia e Formação do Espaço Público

Para Norberto Bobbio (1986, p. 39), a democracia é compreendida como "um conjunto de regras que consente a mais ampla e segura participação da maior parte dos cidadãos, de forma direta ou indireta, nas decisões que interessam à toda coletividade".

A Democracia que hoje conhecemos foi inspirada na forma de governo grega presente em muitas das suas cidades-Estados, notadamente da cidade-Estado grega de Atenas. O procedimento democrático era caracterizado por conceder o exercício do poder e decisões políticas diretamente aos cidadãos (que, na pólis grega, se resumiam a filhos de mães atenienses maiores de vinte anos, excluídos mulheres, escravos e estrangeiros). O sistema se mantinha através de reuniões em um espaço genuinamente político, a ágora, uma praça pública destinada às discussões sobre assuntos públicos diversos. O conceito de democracia na Grécia pouco se assemelhava ao conceito moderno de democracia e era pensado em contraposição à República. A Democracia era o governo de muitos exercido de forma direta, enquanto a República era o governo de poucos, exercida através de representantes.

Com a Revolução Gloriosa na Inglaterra, precisamente em 1688, inicia-se o estabelecimento de novas bases teóricas para a instituição da democracia moderna no Ocidente. Resgatando e reconstruindo as ideias dos teóricos do medievo, os teóricos da república desenvolvem novos mecanismos de aperfeiçoamento do ideal democrático, como a da divisão do poder (Executivo, Legislativo e Judiciário) e a representatividade, que serão posteriormente reforçados no século XVIII com o Iluminismo e as Revoluções Americana (1776) e Francesa (1789) (BOBBIO; MATTEUCCI; PASQUINO, 1998).

No momento em que as revoluções burguesas começam a ocorrer, o Estado Europeu se caracteriza pela concentração de poder nas mãos do monarca, onde a vontade do Rei era a lei (*regis voluntas suprema Lex*). Este não respondia pelos seus atos perante os súditos e possuía atuação ilimitada e carente de maior responsabilidade: *rex legibus solutus* (Direito Divino de governar) (BOBBIO; MATTEUCCI; PASQUINO, 1998).

Neste cenário, marcado por contestações ao Estado e à estrutura social, surge a esfera pública burguesa, que passa a assumir um significado relevante nos processos de transformação social e política vivenciados neste período. Segundo Habermas, a esfera pública burguesa surge em espaços culturais públicos, transformando-se num “campo tensional entre o Estado e a sociedade civil” (HABERMAS, 1989).

A razão que conduz à formação da esfera pública burguesa é a existência de um público economicamente poderoso que consome informações, discute suas preocupações

culturais e materiais em variados fóruns informais (cafés e salões) e formais (clubes de leitura e associações de comércio), sempre buscando a influência nos espaços políticos de formação do poder.

Inicialmente a esfera pública burguesa, na sua forma política, encontra uma antecessora apolítica e não somente burguesa - a esfera pública literária (*literarische Öffentlichkeit*): a Respublica Literarum de Erasmus e dos Renascentistas - que constituía um campo de treino para uma reflexão pública crítica ainda que preocupada consigo própria. A referida esfera passa também a discutir questões políticas e sociais, dando origem à esfera pública burguesa na sua forma política, que se constrói no encontro entre os herdeiros da sociedade aristocrata e humanista, em que se baseava a esfera pública literária, e a camada intelectual da burguesia em ascensão (HABERMAS, 1989).

Pode-se entender a esfera pública burguesa "como a esfera de pessoas privadas, reunidas em um público", para defender a sua liberdade econômica e atacar o próprio princípio de dominação vigente, através da racionalização da sociedade (HABERMAS, 1989).

A queda do Estado absolutista e o estabelecimento do Estado Democrático provocaram a ampliação da esfera pública, porque o ideal democrático implicava numa maior participação dos cidadãos nos governos e, portanto, numa maior legitimidade e acordo da opinião pública; entretanto, ao contrário do que era de se esperar, essa ampliação não significou um aumento expressivo da força da opinião pública sobre as decisões políticas (RAMOS, 2008)[14].

Com o desenvolvimento do sistema político de representação, a disputa pelo apoio desta opinião não se restringia ao estrato dos parlamentos. Ele se dimensionou através das estratégias dos partidos políticos. Neste momento, a esfera pública burguesa perde em força argumentativa e ganha em ação estratégica, pois a necessidade de se manter no poder a justificava. Neste sentido, as leis do mercado "também penetram na esfera reservada às pessoas privadas enquanto público, o raciocínio tende a se converter em consumo e o contexto da comunicação pública se dissolve nos atos estereotipados da recepção isolada" (HABERMAS, 1989, p. 191). Neste contexto, as ideias liberais ganham mais força no interior da esfera pública burguesa e vão moldando os contornos da Democracia Representativa Liberal.

Entretanto, a grande transformação da democracia para a compreensão do modelo democrático contemporâneo reside, sem dúvida, na reconciliação pós 1945 da democracia e

[14] periodicos.ufpb.br/index.php/primafacie/article/viewFile/7244/434

do liberalismo sob o traço conceitual da Democracia Constitucionalista e no regaste dos Direitos da Pessoa Humana, reconstituindo a lógica histórica da compreensão do que se convencionou chamar de Estado Democrático de Direito (RAMOS, 2008).

Neste sentido, o Estado Democrático de Direito é aquele que: a) tem o seu fundamento na soberania popular; b) possui a necessidade de providenciar mecanismos de apuração e de efetivação da vontade do povo nas decisões políticas fundamentais do Estado (princípio democrático); c) se estrutura a partir da divisão das funções do poder; d) é também um Estado Constitucional; e) possui em um sistema de garantia dos direitos humanos em todas as suas expressões; f) garante a existência de órgãos judiciais, livres e independentes para a solução dos conflitos entre a sociedade, entre os indivíduos e destes com o Estado; g) busca realizar a democracia política, social, econômica e cultural com a promoção da justiça social (princípio da justiça social); h) respeita os direitos da pessoa humana e os expressa através de direitos fundamentais; i) observa o princípio da igualdade formal e material, da legalidade – a lei formada pela legítima vontade popular e informada por princípios da justiça – e da segurança jurídica – através do controle dos excessos de produção normativa; j) possui um órgão guardião da Constituição e dos valores fundamentais da sociedade, com atuação livre e desimpedida, constitucionalmente garantida.

Muito se tem discutido sobre a questão de a democracia ser ou não o modelo ideal de governo. Com todas as suas constatações lacunares, com todas as suas deficiências, esta ainda é considerada a forma de governo mais desejável.

Hodiernamente, a democracia traz uma conotação que, embora respeitante aos princípios de igualdade e liberdade, também e principalmente "está ligada às questões da segurança e direitos humanos, enquanto princípios e bases fundamentais das sociedades contemporâneas" (SOUZA, 2006, p. 8).

Cientistas políticos têm defendido uma terminologia de conceito minimalista. Num artigo, sobre tal assunto, Vóigt (2014) afirma que:

> No conceito minimalista, são considerados democráticos regimes cujos representantes são eleitos por meio do voto livre, em eleições periódicas constitucionalmente estabelecidas e que haja alternância de poder caso a oposição ganhe, pois o representante foi eleito de forma legítima e todos aqueles submetidos a esse Estado aceitam o jogo democrático (VÓIGT, 2014, p. 33).

Um conceito minimalista parece esvaziar as potencialidades da democracia e a reduz ao simples governo representativo da maioria.

Nessa perspectiva, debate-se sobre a necessidade de uma participação social concreta, para a efetiva representação popular e a existência de procedimentos que possam viabilizar esta participação. No cerne desta discussão, encontram-se os novos delineamentos do espaço público como o espaço público digital, bem como a existência de uma ágora digitalizada que permite um amplo exercício da liberdade de expressão, influenciando a própria natureza jurídica da democracia.

3.5.2 Ciberdemocracia e Espaço Público Virtual

Para Lévy (2002) o governo das sociedades passa pelo ciberespaço, porquanto este aumenta e transforma a capacidade de comunicação humana que, por sua vez, desempenha um importante papel na evolução da governança política.

Neste sentido, a cidadania e a democracia pressupõem a linguagem. A linguagem aqui é compreendida em seu aspecto mais amplo, não somente como o simples uso da palavra, articulada ou escrita, mas como um sistema de signos expressos ou captados pelos órgãos dos sentidos como meio de expressão e comunicação entre os indivíduos (RAMOS, 2008).

É a partir da linguagem que se constrói a estrutura social, porquanto ela confere a interação para que os indivíduos possam erigir as relações necessárias para desenvolver uma identidade social (sociedade), para construir e reproduzir suas crenças (cultura) e para influenciar, de forma definitiva, a formação de seu caráter através da interação com outros sujeitos (personalidade) (HABERMAS, 2002).

Neste sentido, a linguagem é a mediadora das relações entre os seres humanos, e promotora do entendimento, fim último da comunidade.

Os ciberespaços, assim, constituem-se em verdadeiros espaços públicos virtuais de maior liberdade e de comunicação e interdependência. Assim, se a sociedade se caracteriza sobretudo pelas interações entre os indivíduos que a compõem através da linguagem que une o mundo subjetivo ao mundo social, a comunicação assume grande importância nas democracias.

Podemos, assim, reconfigurar, de certa forma, as bases da democracia e do seu palco de discussão (espaço público) para as novas necessidades da sociedade em rede.

A esfera pública decorre da reunião de sujeitos privados que se reúnem discursivamente em espaços públicos para formar a opinião pública (HABERMAS, 1989).

Já a esfera pública virtual decorre da utilização do ciberespaço pelos sujeitos privados que integrantes da sociedade em rede formam uma inteligência coletiva (LÉVY, 2002).

Se antes falávamos em opinião pública, devemos, no contexto da sociedade em rede, falar em inteligência coletiva, porquanto a opinião pública, moldada no contexto dos espaços públicos, formará-se-á em listas de discussões, fóruns, chats, sítios interligados e outros dispositivos de comunicação próprios da sociedade em rede (LÉVY, 2002).

Neste sentido, "a noção de opinião pública qualificará prioritariamente comunidades linguísticas mais do que cidadãos de um Estado" (LÉVY, 2002, p.53).

A expansão das funcionalidades do ciberespaço, enquanto meio conversacional livre, aberto, multidirecional, interativo e planetário, possibilitaria debates de temas e ações que interessariam a sociedade em rede de forma independente e longe de centros polarizadores.

O ciberespaço, enquanto instrumento de cidadania, também poderia contribuir através da governança eletrônica, conferindo maior eficácia ao setor público e desburocratizando o acesso a procedimentos administrativos ou mesmo propiciando algum tipo de participação direta.

A Cibercultura, neste contexto, torna-se a base de um processo de emancipação social em direção a uma democracia em escala planetária. A Inteligência coletiva, como uma dinâmica social e comunicacional, regida pela colaboração em rede e suportada pelo ciberespaço, reconfigura as estruturas sociais, as instituições e as práticas comunicacionais rumo à Ciberdemocracia.

Lemos e Levy (2010), evocando uma dimensão ética para a inteligência coletiva, configura a Ciberdemocracia como a arte do diálogo aberto, responsável e plural.

Neste sentido, podemos definir a Ciberdemocracia como o conjunto de procedimentos utilizados pelas comunidades virtuais que, a partir do uso da linguagem, em um espaço público virtual (ciberespaço), constrói uma governança global, através da transparência, respeitando-se a cultura da diversidade, através de uma ética da inteligência coletiva.

3.5.3 Democracia e racionalidade comunicativa: contribuições para se pensar a Ciberdemocracia

Jürgen Habermas (1997) faz a crítica à visão liberal sobre a democracia afirmando que ela restringe algo amplo, a uma ética individual, qual seja, a escolha de governantes pelo sufrágio, através de uma simples eleição onde o voto anônimo apenas quantifica uma escolha, sem o concurso de uma discussão mais aprofundada. A crítica vai na mesma direção da feita por Lévy ao falar sobre Ciberdemocracia (LÉVY, 2002).

Ao criticar a democracia liberal e republicana, o filósofo alemão busca algo, no seu entendimento, qualquer coisa que transcenda a dualidade estabelecida por estas visões, concebendo uma democracia procedimental fundada em uma ética da discussão que tem como foco a linguagem através do uso da razão comunicativa.

A racionalidade comunicativa tem o objetivo de resgatar a autonomia da razão a partir de pressupostos comunicativos de interação social, onde a razão não se subordina a um modelo pré-construído de racionalidade, mas se molda a partir das relações dos sujeitos em processos de entendimento acerca do mundo e da sociedade (HABERMAS, 1997).

O discurso, óbvio, não se processa isoladamente; demanda o concurso do diálogo, daí a conotação dialógica de todo o processo de análise, quer seja no âmbito político, quer nas tomadas de decisão. Para Habermas, a ética da discussão sedimenta a democracia. E para a construção de uma sociedade democrática, necessário se faz "lançar mão de dois instrumentos":

> a) Da justiça – que diz respeito à liberdade subjetiva dos indivíduos e;
> b) Da solidariedade – o bem de todos os cidadãos que vivem e partilham um mundo da vida objetivo e subjetivo. Assim, tanto a justiça como a solidariedade devem se reportar a uma só e mesma fonte moral. A moral deverá, através da linguagem, permitir a formação de um ponto de vista central, através do qual os sujeitos socializados possam compensar suas fraquezas. Ela deverá ser universal e transcender os limites da vida cotidiana e concreta de uma tribo, uma cidade ou um Estado (BRENNAND; BERTEN; MEDEIROS, 2006, p. 35).

Ao se analisar a questão da liberdade subjetiva, defendida por alguns, depara-se, invariavelmente, com um aspecto muito bem explorado pelo filósofo alemão, que é o fato de que "a identidade individual detém vulnerabilidades e fragilidades crônicas [...]" (BRENNAND; BERTEN; MEDEIROS, 2006, p. 38). Este entendimento é reiterado pelos mesmos autores, ao afirmarem que "É importante salientar que Habermas, em sua teoria moral, está preocupado com a vulnerabilidade estrutural do ser humano" (BRENNAND; BERTEN; MEDEIROS, 2006, p. 38). Mais adiante, ainda ressaltam que "[...] é perceptível a preocupação, por um lado, de salvaguardar a dignidade de cada indivíduo em particular e, por outro, de salvaguardar as relações intersubjetivas através das quais os indivíduos se conservam como participante de uma comunidade". (BRENNAND; BERTEN; MEDEIROS, 2006, p. 38).

Assim sendo, há de se convir que o indivíduo inserido na sociedade está vulnerável também às leis, aos ditames do Estado, ao julgamento dos pares do seu grupo de ação, aos

conceitos místicos da sua comunidade religiosa, além de, naturalmente, à sua própria natureza.

Habermas prega a prática de uma discussão coletiva, num território tal, numa espécie de ágora contemporânea onde se possam albergar todos os estratos sociais e os diversos matizes ideológicos para que se construam soluções coletivas respaldadas no discurso, numa viga dialógica onde se estruturem pensamentos para a busca de um caminho pelo qual passe uma moral matricial de leis e códigos.

A formação racional da vontade para Habermas (1997) pressupõe um espaço público como uma ampla prática argumentativa, onde todos os participantes procuram estabelecer um consenso. Através deste amplo debate, que leva em conta as concepções individuais e também os valores de toda sociedade, estabelecer-se-ão as normas que terão como destinatários seus próprios autores, reconstruindo, assim, um sistema de direitos que tem origem na associação voluntária de cidadãos que legitimamente elaboram seu direito positivo.

Fica bem claro que esta espécie de território comporta o sujeito que é, ao mesmo tempo, agente e destinatário de todas as decisões e direitos ali configurados, capaz de contribuir para a instauração de um processo democrático mais abrangente no que tange ao consenso. E aqui, é bom que se frise, consenso não presume unanimidade, mas assunção de uma deliberação fruto de análise, crítica e vasta discussão (HABERMAS, 2003 apud SELVATTI, 2015)[15].

Esta ética discursiva, formulada pelo filósofo alemão e por ele defendida, vem suprir as lacunas deixadas pela concepção liberalista calcada, por um lado, na visão liberal (escrutínio, voto), que se "[...] apoia na ideia de um Estado guardião da sociedade fundada sobre a economia, e a republicana, numa sociedade ética institucionalizada pelo Estado" (BRENNAND; BERTEN; MEDEIROS, 2006, p. 41).

Na visão habermasiana, o Estado de Direito demanda uma organização do poder público formada em consonância com os preceitos jurídicos e éticos, mas só haverá legitimidade, quando o direito for legitimamente instituído através de procedimentos.

O autor alemão revela o Direito e sua dupla natureza: a constitutiva e a instrumental. Através desse proceder jurídico, o código de poder é formado viabilizando a transformação do poder comunicativo em administrativo. Por esse caminho, verifica-se que, na Administração Pública, o poder concentrado deverá regenerar-se gradativamente a partir do poder comunicativo. No entendimento de Jorge Lubenow:

[15] http://www.ambitojuridico.com.br/site/index.php?n_*link*=revista_artigos_leitura&artigo_id=10621

> Através do caráter procedimental, que garante formalmente igual participação em processos de formação discursiva da opinião e da vontade e estabelece, com isso, um procedimento legítimo de normatização. Nesse caminho via procedimento e deliberação, que constitui o cerne do processo democrático, pressupostos comunicativos de formação de opinião e da vontade funcionam como a "eclusa" mais importante para a racionalização discursiva das decisões no âmbito institucional (LUBENOW, 2010)[16].

Amartya Sen (2011) também critica a democracia representativa exercida nos moldes liberais afirmando que:

> É evidente que o voto secreto tem um papel muito importante inclusive para a expressão e a eficácia do processo de argumentação pública, mas isso não é a única coisa que importa, e pode ser visto apenas como uma parte – reconhecidamente uma parte muito importante – do modo como a razão pública opera em uma sociedade democrática. [...] a própria eficácia das votações depende fundamentalmente do que as acompanha, como a liberdade de expressão, o acesso à informação e a liberdade de discordância. Por si só, o voto secreto pode ser completamente inadequado, como mostram abundantemente as insólitas vitórias eleitorais de tiranias que governam regimes autoritários [...] (SEN, 2011, p. 361).

Percebe-se, no excerto acima, uma perfeita consonância com o pensamento habermasiano. Quando Amartya afirma que "a própria eficácia das votações depende do que as acompanha", pode-se, perfeitamente, compreender isso como a prática de uma discussão coletiva, o que é contemplado na Teoria Discursiva de Jürgen Habermas.

Em outro trecho do livro "A Ideia de Justiça", Sen (2011) se posiciona explicitamente em conformidade com Habermas, sobretudo na questão da argumentação e da existência dessa ágora imaginária para o processo dialógico. Observe-se: "[...] Habermas fez uma contribuição verdadeiramente definitiva para o esclarecimento do amplo alcance da argumentação pública e, em particular, da presença dupla, no discurso político, de 'questões morais de justiça [...]" (SEN, 2011, p. 359).

Ainda reiterando este entendimento de que há efetivamente pontos de interseção entre o discurso desses dois pensadores, é pertinente transcrever um trecho em que Amartya corrobora o modo de pensar de Habermas, especificamente no que tange à discussão pública, bem como a íntima ligação entre justiça e democracia, qual seja:

> O mais importante é observar que a totalidade dessas novas contribuições ajudou a trazer o reconhecimento geral de que os pontos centrais de uma compreensão mais ampla da democracia são a participação pública, o diálogo a interação pública. O papel crucial da argumentação pública na prática da democracia coloca todo o tema da democracia em estreita relação com o tópico central deste livro, isto é, a justiça. Se as exigências da justiça só podem ser avaliadas com a ajuda da argumentação

[16] http://www.scielo.br/scielo.php?pid=S0100512X2010000100012&script=sci_arttext

> pública, e se esta argumentação está constitutivamente relacionada com a ideia de democracia, então existe uma íntima conexão entre a justiça e a democracia, que partilham características discursivas (SEN, 2011, p. 360).

No final, quando o adjetivo "discursivas" conclui o pensamento, percebe-se a similaridade de orientação do entendimento entre os dois filósofos sobre o diálogo e o aspecto discursivo na construção de uma democracia mais efetiva e condizente com uma sociedade moderna dotada de posturas e anseios diversos, mas absolutamente capaz de gerar soluções para uma convivência harmoniosa, sem, necessariamente, a intervenção, de cima para baixo, de qualquer ente, ainda que seja o Estado.

As críticas ao modelo representativo liberal de democracia e a concepção de novos modelos de participação e gestão democráticas nos fazem enxergar novas possibilidades para o exercício da democracia. A complexidade da nossa atual organização social exige o pensar de novos procedimentos em termos de participação. O crescimento da sociedade em rede, das comunidades virtuais sem territórios, a explosão da liberdade de expressão no ciberespaço nos levam a renovar nossa condição de cidadão em novos espaços virtuais de formação da vontade. A mundialização da economia e da comunicação, a globalização e a aproximação dos indivíduos através dos ciberespaços nos conduzem à formação de uma sociedade civil planetária que se expressa em um espaço público sem delimitação territorial.

O eixo comum, central, a ponte principal que nos liga nestes novos espaços é a linguagem. Neste ponto, os debates sobre uma ética discursiva têm a contribuir na discussão sobre a racionalidade que deve guiar o uso da linguagem e da comunicação no exercício da cibercidadania, uma vez que estas interações se dão em espaços públicos virtuais de interesses divergentes, aproximando a dicotomia entre público e privado.

As críticas à democracia representativa liberal são muito similares nas obras de Habermas, Sen e Lévy. A coincidência se justifica porque o próprio termo Ciberdemocracia é um neologismo, usado para definir a liberdade e a democracia que se exercita através do universo da cibernética. Senão vejamos.

3.5.4 Ciberdemocracia: ativismo político-social e vivências na rede

O ativismo no ciberespaço ou ciberativismo corresponde a um ativismo peculiar, empreendido no meio *on-line.* O ciberativismo é um termo recente e consiste na utilização das redes por grupos politicamente motivados que procuram difundir informações e

reivindicações sem intermediários, buscando apoio para debater e trocar informações, organizar e mobilizar outros indivíduos para ações, dentro da rede e fora dela.

O ambiente virtual propiciou o surgimento de uma mídia livre, um novo espaço público onde muitos ganham voz para expor e discutir sobre seus posicionamentos ideológicos sem a necessidade de um líder. Ele possibilita a formação de grupos que defendem suas causas e movimentos sociais que se articulam, atuando politicamente, mobilizando a sociedade para transformar o cenário político-social em algum aspecto. Aproveita-se a oportunidade que o ciberespaço proporciona com sua amplitude, visibilidade e alcance global para o engajamento social. Exemplos de tal prática são as petições *on-line* através das quais são compartilhados pedidos de assinatura ou simples publicações expondo o ideal defendido (MARTINS, 2015)[17].

Desde os anos 90, quando se popularizou o uso dos computadores, vemos o espaço virtual revolucionar as formas de manifestação social. O movimento Zapatista foi um dos primeiros ciberativismos a ganhar dimensão. Nele, a Internet foi utilizada como meio de propagação de ideias e manifestações em busca de uma transformação, que, nesse caso, foi a criação de uma rede de solidariedade transnacional pela Internet.

Um evento marcante sobre o tema no Brasil foi o Fórum Social Mundial, realizado em Porto Alegre, em 2001. Este promoveu a difusão de informações e reivindicações e consagrou a existência do ciberativismo. Ao longo dos anos, tais práticas evoluíram ganhando novas perspectivas. No final de 2003, surgiu o *Anonymous*, movimento que possibilitou o compartilhamento de posições políticas anônimas, através de fóruns *on-line* (MATOS, 2014).

Como se vê, o ciberativismo tornou o exercício da cidadania mais efetivo, pela facilidade de articulação, divulgação de ideias e manifestações legítimas. É óbvio que tudo isso, conforme acima frisado, não escapa a questionamentos quanto a limites que devem ser observados, mas muito mais no tocante a territórios éticos e jurídicos relacionados à censura. Não resta, porém, qualquer dúvida a respeito da perfeita possibilidade do exercício da Ciberdemocracia no âmbito da blogosfera.

O papel da Internet tem-se mostrado bastante eficaz como espaço alternativo para discussão de assuntos políticos, robustecendo e rediscutindo os temas de maior interesse. Uma vez postado na rede, qualquer assunto toma uma dimensão nem sempre vista em outros canais midiáticos.

[17] http://www.publico.pt/mundo/noticia/nova-lei-sobre-espionagem-nos-eua-e-um-primeiro-passo-para-reformas-profundas-1697825

A respeito dessa rapidez e da possibilidade de atingir-se uma gama bem mais efetiva de leitores e participantes, a Revista Galileu estampou, na sua capa, a seguinte manchete: “Caiu na Net. E agora, dá pra tirar?” (LOUREIRO, 2014). A par de tratar de assuntos como o Cibercrime, o ponto crucial ali abordado é a questão da virulência com que as informações se espalham, bem como o viés democrático com que se discute o que é postado. Claro que há um temor tácito de exposição de pensamentos nem sempre compartilhado, ou mesmo aceito, pela comunidade virtual.

Sobre isso Gabriela Loureiro, que assina o referido artigo, afirma que “Há uma teoria da ciência da política e da comunicação para isso: a ‘espiral do silêncio’, ou a tendência a ficar quieto quando se sente que as pessoas à sua volta não compartilham da sua opinião”. Entende-se que essa “espiral do silêncio” pode, à primeira vista parecer uma autocensura, contudo pode ter a ver com o senso de aceitação inerente ao ser humano. Para minimizar os efeitos desse choque de visão, “uma alternativa seria trocar o botão “curtir” por “respeitar” no Facebook.

Analisando esta face democrática da cibernética acerca da possibilidade infinita de acessos a todos os assuntos, inclusive os de natureza política, Loureiro (2014) comenta que:

> Algumas décadas depois, a Internet ganhou um peso significativo nas eleições e hoje as redes sociais teoricamente oferecem oportunidades infinitas de mobilização. Da Primavera Árabe (que derrubou ditadores muito enraizados no poder – à parte nossa) ao desafio do balde de gelo, ativistas usam a web para causar um impacto real na política. Se ditadores foram derrubados depois de protestos convocados no Facebook, o que mais as redes poderiam fazer pela democracia?

A Ciberdemocracia não é apenas algo circunscrito à liberdade de falar, comprar e relacionar-se. Vai além desses aspectos. Já se ventila a real possibilidade de se criar um governo mundial, facilitado por esse novo espaço público. Tanto assim que Lévy sentencia que “dirigimo-nos a passos largos para uma situação em que todos os documentos e todos os sinais produzidos pela nossa espécie farão virtualmente parte de um único metatexto planetário” (LÉVY, 2002 p. 30-31). E arremata, que: “A Ciberdemocracia é uma espécie de aprofundamento e de generalização por parte destas abordagens, de uma diversidade livre em espaços abertos de comunicação e cooperação” (LÉVY, 2002 p. 31).

O ciberespaço faculta o aumento da visibilidade e da transparência, que são ingredientes fundamentais para a democracia.

Percebe-se que a Internet é mais eficiente se a compararmos com os demais meios de comunicação da segunda metade do século XX, pois permite expressão direta, sem o concurso de um intermediário através do jornal, rádio ou televisão.

Lévy arremata que "Esta mutação da esfera pública constitui um dos fundamentos da Ciberdemocracia" (LÉVY, 2002, p. 56).

Outro aspecto importante da Ciberdemocracia é o do acesso ao conhecimento em educação. Escolas municipais, estaduais e federais já contam com um parque de máquinas (computadores), através do qual o alunado de todas as classes sociais tem acesso à rede de computadores. Esse recurso didático não substitui os livros, porém complementa-os. O acesso aos saberes e a construção do conhecimento se dão de forma democrática, equânime e coletiva. Lemos e Lévy constatam que:

> O governo federal criou a "Casa Brasil" (telecentros e rádios comunitárias) e o projeto "Computador para Todos". Dezenas de milhões de usuários já foram beneficiados com projetos de inclusão digital por todo o Brasil. Dados mostram que há crescimento, embora de forma desigual pelas regiões do país. As mais beneficiadas são as regiões Sul e Sudeste. A divulgação da construção do Modelo Brasileiro de Inclusão Digital e das metas governamentais do Plano Plurianual revela que o governo federal está preocupado com o processo de inclusão digital (LEMOS; LÉVY, 2010, p. 152).

Outro ponto a se considerar sobre a extensão dos recursos internéticos é que o Presidente da República está também no ciberespaço por meio do sítio "Presidência da República", casa oficial do presidente na Ciberdemocracia brasileira. Lemos e Lévy registram que:

> Esse portal apresenta informações sobre a agenda do presidente, do vice-presidente, dos Palácios, a legislação (códigos, constituição, decretos não numerados, projetos de lei, medidas provisórias, resenha diária), dados históricos (galeria dos presidentes), principais programas de governo e notícias (LEMOS; LEVY, 2010, p. 145-146).

A Folha de São Paulo de 09/03/2015 trouxe, numa manchete, o fato de um paciente internado há 46 anos no Hospital das Clínicas de São Paulo, por tetraplegia, ter lançado um *blog* intitulado "Sejam Bem-Vindos", com uma visibilidade impressionante. Paulo Henrique, autor do *blog*, afirma, numa das suas postagens: - *"Bem, o que eu quero passar para muitos é sobre minha experiência de vida. Claro que morando aqui no Hospital das Clínicas, há uma série de restrições que deixam, pela falta de experiência, muitas dúvidas e questões. A diferença é que nas questões temos a oportunidade de debater, expor situações as quais as ideias são as que devem ser levadas em conta. O que pretendo expor são sentimentos e*

emoções sobre a minha vida, mas de uma forma que sejam explícitas em contos e poesias. Claro que irei explorar outros mundos, criando, a quem lê, interesse em detalhes jamais imaginados".

Neste sentido, o ciberespaço se configura em *locus* privilegiado de vivências, permitindo ao ser humano compartilhar realidades em um espaço virtual amplo de saberes, ideias e experiências que, de outro modo, não poderia experimentar.

3.5.5 Cidadania, Mobilização Social e Construção de Identidades no Ciberespaço

Juridicamente, já se estabeleceu uma diferenciação entre cidadão e indivíduo, sendo este apenas o ser humano em si, enquanto o outro é alguém dotado de consciência dos seus direitos e de sua quota de responsabilidade no tecido social do ambiente em que vive.

A pós-modernidade caracteriza-se pela insurgência de um movimento de forte crítica à racionalidade atual, com forte contestação às concepções de cidadania, democracia e participação política modernas, cujo foco é a dualidade entre Estado e Sociedade civil. As críticas se baseiam, sobretudo, no pressuposto de que o conceito de cidadania proposto pela Modernidade é inapropriado, visto que oculta diversos espaços de formação de poder, como o ciberespaço por exemplo, bem como diversas formas de opressão e dominação existentes na sociedade (RAMOS, 2008)[18].

Destarte, os espaços públicos virtuais também são espaços latentes de participação democrática e de produção e transformação das condições de vida existentes na comunidade.

No ciberespaço, o cidadão é comumente chamado de net-cidadão. O sufixo "net" advém da parte final do vocábulo Internet. Dele, surgem expressões como net-crime, ou Cibercrime, net-consumidor e net-cidadão. Sobre este último, Poster (2010, p. 328) afirma que: "[...] em contraste com o cidadão na nação, o nome muitas vezes dado ao sujeito político constituído no ciberespaço é "netizen (net+citzen) ou net-cidadão."

Nos movimentos sociais levados a cabo através das manifestações de ruas, a construção e presença do net-cidadão, sobretudo nas redes sociais, tem-se mostrado de suma importância para a disseminação das ideias que se pretendem veicular, bem como vem-se tornando uma força agregadora e formadora de opinião dos debates coletivos, realizados tanto presencialmente, quanto através das redes.

[18] periodicos.ufpb.br/index.php/primafacie/article/viewFile/7244/434

É nessa variável de cidadania veiculada pelas redes sociais, com a inegável força do net-cidadão como sujeito e ator das suas convicções e arbítrios, que vamos tratar os movimentos de rua no mundo e, sobretudo, no Brasil.

Lévy (1997 apud POSTER, 2010, p. 334) registra que "[...] os net-cidadãos serão múltiplos, dispersos e virtuais, nós de uma rede de inteligência coletiva."

Qual seria o segredo de os movimentos sociais urdidos através das redes serem tão poderosos a ponto de arregimentar milhares e milhares de pessoas?

A resposta pode estar na questão da horizontalidade das comunicações, em contraponto com a verticalidade impingida pela televisão, jornais e outros meios de comunicação. Enquanto nestes meios as avaliações de fatos ou pessoas vêm prontas, impressas ou ditas por uma âncora de jornal, as concepções formalizadas através do ciberespaço são abertas, construídas por uma face coletiva, porquanto são tecidas por milhares de pessoas que têm voz, produzem suas próprias avaliações e as submetem à chancela de uma multidão de cibernautas regada a muita capilaridade e permeabilidade. "A digitalização tem permitido a integração de uns e outros a novas tecnologias, passando da informação a uma verdadeira comunicação autenticamente interativa" (CREMADES, 2009, p.18). As pessoas reavaliam, endossam, ou não, o que foi veiculado, tudo consoante uma dinâmica peculiar a este instrumento de multiplicação que são as redes.

O *facebook*, *twitter* e *blogs*, os aplicativos *whatsapp* e *telegram*, manuseados através dos aparelhos móveis multifuncionais, são amplamente utilizados como pontos principais para a informação e mobilização social necessárias para alcançar determinados objetivos, sejam eles profissionais, sociais ou pessoais.

Embora o acesso à Internet e suas ferramentas ainda não alcancem a todos, é indiscutível que esse meio tecnológico tem grande potencial para a sociedade global.

As cientistas sociais Débora Zanini e Laiz de Souza, em análise feita na *Hashtag* #MídiasSociais asseguram que

> Uma das características principais das redes sociais é o fato delas terem tirado de um aspecto vertical a comunicação de grandes meios de comunicação. Quando você lê uma reportagem ou assiste a TV, a informação vem fechada e pronta para você. Com as redes sociais isso muda completamente. Aquele modelo de comunicação onde há um comunicador e um receptor da informação muda: o produtor de conteúdo e o receptor dialogam entre si e mudam de posição constantemente – o diálogo é horizontal.[19]

[19] <http://hashtag.ms/blog/nossas-cientistas-sociais-analisam-a-importancia-das-redes-sociais-para-os-movimentos-populares/>.

É fato que as mídias tradicionais têm cumprido, sim, seu papel de repercussão e reflexão de ideias e ações, todavia inegável é que, no âmbito das redes, tanto pela sua imensa capilaridade, quanto por facultar uma maior liberdade de opinião, a democracia sedimenta-se e se amplifica, posto que o cidadão registra seu apoio ou rejeição ao que quer que esteja sendo veiculado.

As tecnologias emergentes funcionam como um verdadeiro canal participativo de expressão da opinião pública. É o poder da informação, previsto quatrocentos anos antes por Francis Bacon. Quanto maior o acesso à informação em curto tempo, maior o poder em várias searas da atividade humana. É a chamada supremacia do *soft power.*

Observa-se uma nova forma de jornalismo participativo, *on-line,* com *links* variados, notícias diversas sobre esporte, moda, economia, saúde, política, entre outras, representado pelos *Weblogs*, *ou blogs*. E, em muitos sites, o leitor torna-se também um propagador da notícia, participando ativamente, redigindo e noticiando, como é o exemplo do *Ohmynews.com*, na Coréia do Sul, com mais de dois milhões de internautas, que leem e também escrevem, sendo protagonistas da notícia.

A Revista norte-americana Time noticia anualmente as personalidades mais influentes do mundo. Em 2006, excepcionalmente, não foi destacado nenhum nome em especial. Pelo contrário, o destaque, segundo Javier Cremades era *YOU* (Você), simbolizando os milhões de usuários da rede , ou seja: " indivíduos que utilizam ou criam conteúdos para a Internet e que, na prática, estão conseguido alterar, de maneira geral, a natureza da era da informação e, de maneira particular, a própria democracia e os direitos do cidadãos"(CREMADES, 2009, p. 86).

É essa transformação que estabelece a sociedade em rede, que é composta por redes globais, nacionais e locais que se interagem de forma dinâmica e sistêmica estabelecendo um sistema peculiar de comunicação.

> O sistema de comunicação da sociedade industrial era centrado em torno da mídia de massa, caracterizada pela distribuição massiva de uma mensagem unidirecional de um para muitos. A base da comunicação na sociedade em rede é a teia global de redes de comunicação horizontal que inclui a troca multimodal de mensagens interativas de muitos para muitos sincrônica e assincronicamente (Castells, 2007, p. 2463).

Toda essa capacidade de participação coletiva em escala mundial está mudando a sociedade, fazendo nascer o chamado micropoder. Nos dizeres de Cremades:

> [...] o micropoder está mais ativo do que nunca. Sua capacidade de criar redes e gerar globalização tem mudado todos os âmbitos relevantes da vida social e tende a impor sua própria lei, sendo por isso respeitado, e deve ser considerado como força emergente mais excepcional deste início de século XXI (CREMADES, 2009, p.17).

Há inúmeras formas de comunicação e por meio da utilização das tecnologias vigentes, tais como celulares, computadores, Internet, dentre outras, está ocorrendo uma espécie de revolução da informação. Os indivíduos tornam-se detentores de uma parcela de poder que antes era predominantemente institucional e estatal.

Todas estas expressões de cidadania baseadas na força de um instrumento virtual renderam e estão rendendo muitas manifestações que vêm provocando mudanças em nível global. Numa passagem sobre o histórico dos movimentos sociais que levaram multidões às ruas de vários países, tanto no Oriente como no Ocidente, pôde-se fazer remissão ao *impeachment* do Presidente das Filipinass, em 2001, os protestos na Coreia do Sul, em 2006 (contra a importação de carne dos Estados Unidos), a reivindicação por mudanças no sistema de ensino no Chile, em 2006, o acampamento do movimento *Occupy* do lado de fora da Catedral de St Paul, em Londres, com cartazes expondo mensagens contra a ordem estabelecida – todos mobilizados através de redes sociais.

Na Tunísia, um dos primeiros da série intitulada de "Primavera Árabe", em que pese ter um poético nome de "Revolução dos Jasmins", iniciada no final de 2010 e encerrada em janeiro de 2011, foi aguerrido, culminando com a queda do homem forte, Ben Ali, no poder há 24 anos. Depois de décadas de silêncio, sem lideranças significativas, o povo foi às ruas para lutar por direitos. No Egito, como retaliação à manifestação, o então presidente Hosni Mubarak mandou cortar a Internet já que esse era o meio pelo qual os manifestantes se organizavam nacional e internacionalmente, obtendo como resposta ao seu ato um outro mecanismo de acesso ao *twitter* via celular disponibilizado pelo Google.

A revolução egípcia, batizada por três nomes (Dias de Fúria, Revolução do Lótus e Revolução do Nilo) fez Mubrak desistir de se candidatar novamente a novas eleições.

As manifestações e protestos ocorridos no Oriente Médio e no Norte da África, ganharam corpo multiplicando-se através das redes sociais e fazendo com que milhares de pessoas se organizassem virtualmente para depois ir às ruas discutir a situação do governo ditatorial árabe e, posteriormente, pressionar para mudar a situação política vigente.

Essa mobilização ativista só foi possível graças ao espaço virtual democrático proporcionado pelas tecnologias da informação, capaz de permitir debates e produção de

conhecimento que, inevitavelmente, acarretaram novas ideias, lutas e questionamentos para, posteriormente, possibilitar uma mudança significativa na sociedade.

Com isso, constata-se que a Ciberdemocracia pode promover a universalização da informação e do conhecimento para que, através dos novos meios de comunicação, seja possível não só a difusão destes como também o seu uso como instrumento para a transformação social. Para Castells (2003, p. 114) "o ciberespaço tornou-se uma ágora eletrônica global em que a diversidade da divergência humana explode numa cacofonia de sotaques".

Ainda no âmbito internacional, não se pode olvidar de outro relevante movimento planejado através das redes sociais, em que a população organizou uma manifestação, com data e hora marcadas, para protestar contra a crise econômica global e foi intitulado de "*Ocupe Wall Street*". Essa mobilização começou via *Facebook*, *Twitter* e *blogs*, também em setembro de 2011, os protestos dos "indignados" tomou corpo e recebeu a adesão de cidadãos de um total de 951 cidades em 82 países.

Dentre os enfrentamentos orquestrados por movimentos socioespaciais, com rescaldos conflituosos, que se fizeram registrar na Europa, pode-se destacar, exemplificativamente, o ocorrido em Portugal com o "Geração à Rasca", (em português, o termo rasca significa dificuldade), ou M12M – Movimento 12 de Março, o M15M – Movimento 15 de Março na Espanha e outros mais na Islândia, Itália e Grécia. Os recentes protestos na Grécia (junho/julho 2015) levaram multidões às ruas, em resposta ao arrocho imposto pelo Fundo Monetário Internacional, condição importante para a ajuda àquele país.

Vale ressaltar, que os movimentos aqui citados, apesar de terem motivações, dimensões e finalidades diferentes, possuem um aspecto comum, sua forma de organização, ou seja, o uso da tecnologia da informação como meio principal de comunicação e organização. Em todos os exemplos descritos acima, as tecnologias digitais estiveram presentes exercendo papel fundamental na mobilização e organização dos ativistas sociais.

É possível que essa febre mobilizadora internacional tenha criado um gancho para um fenômeno verificado no Brasil a partir de junho de 2013, os movimentos reivindicatórios de rua, assunto a ser tratado a seguir.

3.5.6 Os movimentos de rua no Brasil

É importante registrar que, antes das manifestações de junho de 2013, alguns protestos, ocorridos no Brasil, serviram de ensaio e também ganharam força através das redes

sociais, como: o "Churrascão da Gente Diferenciada", realizado em São Paulo, quando, em dois dias, através das redes sociais, *twitter e facebook*, 4 mil pessoas se reuniram para a sua realização. O protesto foi uma crítica ao governo municipal paulista que interrompeu as obras de construção da Estação Higienópolis de metrô por pressão da associação de moradores do bairro, que temia ver o espaço invadido pela "gente diferenciada" das periferias da cidade.
Ainda em São Paulo, outro movimento teve uma característica similar, chamado de 'A Marcha da Liberdade'. Esta manifestação tinha o objetivo de protestar contra a violência policial ocorrida na "Marcha da Maconha". No referido movimento, o grito de ordem era: "Não somos uma organização. Não somos um partido. Não somos virtuais. Somos REAIS. Uma rede feita por gente de carne e osso. Organizados de forma horizontal, autônoma e livre". Partido Socialista dos Trabalhadores Unificado (PSTU, 2015). Esse trecho destaca o quanto o manifesto virtual está presente nas atuais formas de reivindicações sociais,

Em junho de 2013, estourou nos quatro cantos do país, o movimento "Vem Pra Rua". Esse movimento entrou para a história como uma das grandes manifestações civis brasileiras. O Brasil foi palco de um movimento, cujo mote reivindicatório aparente teria sido o aumento das passagens de ônibus, mas que trazia, em seu bojo, uma esteira bem mais consistente e plural de reivindicações: a luta contra a corrupção, os gastos com a Copa do Mundo, a incompetência administrativa, a arrogância de políticos - a maioria deles refratária à veemência das demandas democráticas -, e a derrubada do Projeto de Emenda Constitucional 37, a PEC 37 - entendida como uma mordaça imposta ao Ministério Público, que não teria mais competência investigatória criminal.

Como resultado prático dos protestos restou a queda da referida emenda rejeitada pelo plenário da Câmara dos Deputados por 430 votos contrários e somente 9 a favor, bem como a redução de 15 para 13 do número de salários anuais dos deputados, como ocorre com os trabalhadores em geral. Percebeu-se, também, como substrato desse alçar de bandeiras, um movimento sísmico na base do poder, o que teria motivado reuniões ministeriais e uma tendência a auscultar as ruas.

O movimento "Vem Pra Rua" se diferenciou dos demais movimentos sociais brasileiros pela forma como foi organizado, uma vez que contou basicamente com ações desenvolvidas através das redes sociais e da comunicação alternativa até então pouco utilizada no Brasil, demonstrando que o universo da comunicação em rede pode ser maior do que o da grande mídia.

Figura 1- Movimento "Vem Pra Rua", em junho de 2013

Fonte: Souza, (*online*)[20]

Em seu ápice, o movimento conseguiu a mobilização de milhões de pessoas, das mais variadas etnias e orientações, idades e de todos os cantos do Brasil. Essas pessoas já não estavam mais protestando só contra o aumento da tarifa do transporte público e a violência policial; as reivindicações também envolviam questões como os gastos públicos, corrupção, qualidade dos serviços públicos, reforma política, ética governamental e a democratização dos espaços públicos e ações governamentais.

Em entrevista à Revista Época, em novembro de 2013, Pierre Levy se pronunciou dizendo que: - "*Quando soube dos protestos no Brasil, que foram organizados pelas mídias sociais, eu entrei no "Twitter" e participei. Eu "retuitei" em Português alguns temas do protesto [...] Há muitos anos, a Internet é uma nova ferramenta de expressão da população, uma nova forma de coordenar movimentos sociais.* (LÉVY)"[21]

A principal característica dos participantes desse movimento era que eles não estavam inseridos em nenhum outro movimento social tradicional. Os jovens, universitários ou secundaristas levavam cartazes feitos à mão com múltiplos posicionamentos a respeito do movimento, deixando clara a diversidade do protesto sobre a realidade político-social do país.

Neste cenário de mobilização social pelas redes surge a chamada "geração M". Uma geração composta por jovens que antes usavam as ferramentas tecnológicas somente como

[20] Informação retirada do site <http://umadosedesimpatia.blogspot.com.br/>.
[21] Entrevista concedida a Revista Época. Disponível em: <http://epoca.globo.com/ideias/noticia/2013/11/pierre-levy-o-que-acontece-aqui-nao-e-por-bdemocraciab-e-sim-contra-bcorrupcaob.html>. Acesso em: 20 jul. 2015.

meio de informação e que, após esse momento, passam a utilizá-las como mecanismos para reivindicar direitos.

Diante das manifestações diretas de democracia, no primeiro momento, o governo tentou descaracterizar o movimento não conferindo muita credibilidade ao mesmo. Entretanto, à medida que este se fortalecia tornou-se inevitável uma resposta governamental às reivindicações feitas, apresentando medidas concretas para acalmar os ânimos e tentar acabar com as manifestações nacionais. Tanto o Executivo, como o Legislativo se viram obrigados a diminuir a indignação e a revolta popular que cresciam nas ruas, mas que tinham como sede, os espaços virtuais, aumentando, em proporções inimagináveis, as informações e campanhas contra os atos governamentais. Entre essas medidas o Congresso Nacional votou uma série de concessões, a chamada "agenda positiva", onde tornou a corrupção crime hediondo e arquivou a PEC 37. Também houve a revogação dos recentes aumentos da tarifa do transporte em várias cidades do país.

Os meros vinte centavos aumentados no preço das passagens de ônibus foram apenas a "Gota d'Água" decantada por Chico Buarque e Paulo Pontes, tão somente o pontapé inicial, aquilo que fez entornar o copo, não se suportar mais na carga de desconfortos que vem recaindo sobre o povo.

Corrobora este pensamento o sociólogo espanhol Manuel Castells (apud PORTAL FRONTEIRAS, 2013), tido como um intelectual sempre "conectado", que, questionado pelo "Fronteiras do Pensamento 2013", sobre os protestos da Avenida Paulista em 11 de junho de 2013, afirmou: - "*Todos os movimentos sociais na história são, sobretudo, emocionais. Não são pontualmente reivindicativos. Não é o transporte. Em algum momento, há um fato que provoca a indignação. Ao sentir a possibilidade de estarem juntos, ao sentir que há muitas pessoas que pensam o mesmo fora do âmbito institucional, surge a esperança de fazer algo diferente. O quê? Não se sabe. Mas, com certeza, não é o que está aí.*[22]

Há um ponto para se deixar bem claro: o processo de comunicação e arregimentação para as manifestações não contou com a colaboração e apoio de nenhuma mídia televisiva, jornais escritos, ou mesmo veículos radiofônicos. Tampouco teve a adesão de qualquer figura política, pelos menos até que as ruas atestassem o sucesso das manifestações. Tudo foi arquitetado por meio das redes sociais.

[22] Manuel Castells, ao ser entrevistado pelo "Fronteiras do Pensamento 2013". Disponível em: <http://www.fronteiras.com/artigos/manuel-castells-analisa-as-manifestacoes-civis-brasileiras>.

Indubitavelmente, forma-se uma cultura nova, a cibercultura, algo dinâmico e abrangente, capaz de uma mecânica silenciosa, mas que demonstra uma competência magnífica para a partilha e produção de conhecimentos novos.

Adriana Alves Rodrigues, no seu artigo "Redes sociais e manifestações: mediação e reconfiguração na esfera pública", sustenta que "As redes sociais na internet têm sido largamente exploradas para o ativismo *on line,* ou ciberativismo, caracterizado pela logística das relações sociais em rede".

Estamos, por conseguinte, diante de uma nova arquitetura da informação, de um novo modelo de se levantarem bandeiras, fazer reivindicação, diante de uma nova fonte geratriz de sentimento de cidadania.

Para Lévy (2002):

> [...] a multiplicidade de expressões na internet enriquece a política e permite a formação de uma esfera pública mundial. 'O monopólio das expressões públicas não existe mais. Todo mundo está se expressando pelas redes sociais. Essa é a verdadeira liberdade de expressão'.

Neste sentido, as formas de comunicação virtual são importantes armas políticas não se limitando somente ao espaço da Internet, pois, estabelece em torno de si uma rede muito mais ampla, capaz de conectar-se, não só ao espaço virtual, mas também, ao espaço local. Essa comunicação possibilita a interação entre "o espaço virtual das redes telemáticas e os espaços concretos da cidade" (LEMOS, 2015) [23]. Na rede social, há a mobilização, discussão e organização; nas ruas, o encontro e a concretização do que se propõe.

Em março de 2014, menos de um ano após os movimentos "Vem para a Rua", a Polícia Federal e o Ministério Público deflagraram a operação "Lava Jato" para investigar um esquema bilionário de desvio e lavagem de dinheiro envolvendo a maior empresa estatal do país, a Petrobras. Segundo os órgãos responsáveis pelas investigações, grandes empreiteiras organizadas em cartel pagaram propina a diretores e gerentes da estatal, causando enormes prejuízos aos cofres públicos, configurando-se no maior esquema de corrupção do país.

Novamente, um movimento ocorrido em 15 de março de 2015, no Brasil, levou cerca de 1milhão e meio de pessoas às ruas. Desta vez, bem mais organizado e com pautas reivindicatórias mais bem definidas. Rogerio Chequer, um dos líderes do "Vem pra Rua", assegurou, em entrevista para um canal de televisão brasileiro, que já esperava que o número de presentes às manifestações de 15 de março/2015 chegasse mesmo a ultrapassar 1 milhão de

[23] http://www.institutodofuturo.com.br/CIBER.html

pessoas como calculou a PM. O instituto Datafolha, entretanto, avaliou em 250 mil. O Movimento Brasil Livre – MBL gostou do que viu na Avenida Paulista, mas um de seus líderes pediu mais presença, mais gente. Para tal, redobrou seu trabalho através do instrumento que se tem mostrado eficaz: a Internet e suas redes sociais.

Figura 2- Movimento ocorrido em 15 de março de 2015

Fonte: Botelho, 2015[24].

Tais movimentos se repetiram a 12 de abril de 2015, só que sem a mesma força do de 15 de março, nem por isso menos impetuoso e importante. Em que pese, segundo os organizadores, ter contado com ¼ do número de participantes do movimento análogo de 15 de março, O Movimento Brasil Livre, que participou do protesto, avaliou as manifestações como extremamente positivas. As postagens, nas redes sociais, davam conta de que o curto interregno de apenas um mês entre uma manifestação e outra (15 de março/12 de abril) possa ter sido um dos motivos de presença menor da população nas ruas. Além desses dois grupos, estiveram em cena nos movimentos de rua, o grupo Revoltados Online e o Movimento Limpa Brasil – MLB, todos eles usando do mesmo mecanismo para a informação e a mobilização popular, qual seja contando com o concurso efetivo das redes sociais.

Nessa perspectiva, a importância dos ciberespaços para o estreitamento do diálogo entre as populações e os governos ganha espaço frente às representações políticas e sociais tradicionais, que não se apresentam como meio suficiente para a mediação de comunicação

[24] http://thiaguinhobotelho.blogspot.com.br/2015/07/impeachment-ja.html

verdadeira e profícua em uma sociedade em rede. A Internet, para a sociedade em rede, torna-se mais que uma ferramenta gerencial e organizacional, torna-se também suporte para o fortalecimento dos ciberespaços também como espaços públicos virtuais, que passam a refletir muitas ações da sociedade e o que se espera dela, alterando seu movimento conforme essa sociedade se altere.

Esses movimentos recentes demonstram que os espaços digitais proporcionaram uma ampliação da cidadania e uma nova modalidade de vivenciar a democracia que não a representativa. O povo, organizado nas ruas e virtualmente atento, através das mídias digitais, das informações de corrupção, presentes na atual fase do país, faz com que "gritem" por mudanças, por posturas éticas, faz com que cobrem das autoridades atitudes concretas que transformem condutas e realidades sociais.

3.5.6.1 Os Black Blocs e a construção de identidades no ciberespaço

Nos protestos de junho de 2013, houve também a participação dos "Black Blocs", manifestantes usando roupas pretas e com os rostos encapuzados, que criticavam o capitalismo e a globalização, depredando patrimônios públicos e privados.

Podemos considerar a participação dos "Black Blocs" como uma forma violenta de ativismo. Surgem na Alemanha, na década de 80, e se caracterizam por manifestações anárquicas e violentas. Não possuem estrutura organizada. Podem ser grupos distintos, com ideologias e objetivos também distintos. *Black Blocs* não possuem líder, tampouco são uma organização. Os *Black Blocs* seguem um modelo de ativismo que se espalhou utilizando-se de várias mídias, inclusive através da Internet[25]

Devido a essas ações, o embate entre a polícia e os manifestantes foi inevitável, o que gerou, por parte do governo, propostas mais repressivas no intuito de conter a violência. Uma dessas ações foi o uso da Lei de Segurança Nacional, criada em 1935 e reformulada no período da ditadura em 1983 para conter práticas que afrontem a integridade territorial, os chefes de Estado, a democracia e a soberania nacional.

Segundo a Anistia Internacional, o uso da referida lei pelas autoridades brasileiras foi impróprio, uma vez que tal dispositivo foi criado para combater o crime organizado e não manifestações oriundas de movimentos sociais. O caráter violento das manifestações,

[25] Can´t Stop The Kaos. Manifesto autônomo publicado em Vancouver em 2010. Dísponível em: https://toleratedindividuality.files.wordpress.com/2015/02/cant-stop-kaos-a-brief-history-of-the-black-block1.pdf

entretanto, permitiu o seu enquadramento no crime de organização criminosa, previsto no art. 2º da Lei nº 12.850/2013.

Os críticos dessas medidas argumentaram que a estratégia usada pelo governo foi equivalente a criminalizar o livre direito à manifestação e protesto. Mesmo quando o debate ainda girava em torno do que seria considerado vandalismo e sobre a legitimidade ou não destes protestos, a repressão policial foi intensa. Para alguns, a postura adotada pela polícia demonstrava uma tentativa de revidar os protestos, alegando que era preciso tal ação porque havia a infiltração de grupos violentos entre os manifestantes.

A presença dos "Black Blocs", cada vez mais tácita e estética, nos noticiários acontece paralelamente à diminuição da quantidade e diversidade de manifestantes nos atos, ou seja, ocorre uma intensificação da polarização entre os que apóiam e os que condenam a destruição do patrimônio público e privado como forma de protesto. Nas manifestações de junho de 2013, pequenos grupos atacaram bancos, guaritas policiais, prédios do poder público, empreendimentos e lojas privadas, dentre outros.

Houve a convocação das tropas especializadas em violência urbana para reprimir e impedir que os vândalos continuassem a depredar patrimônios.

Diante desse cenário, vários projetos de leis foram propostos, em todos os níveis, federal, estadual e municipal, para tentar limitar ou restringir o direito de protesto e criminalizar as manifestações e manifestantes que se utilizassem da violência ou do anonimato, proibindo o uso de máscaras nos protestos, criando novos tipos penais para determinadas ações presentes nas manifestações ou, simplesmente, aumentando penas de tipos penais já previstos, tais como: lesão corporal e homicídio caso praticados durante protestos. Também houve proposta para a tipificação do crime de "terrorismo", previsto genericamente na Lei de Segurança, mas sem tipicidade, que, se aprovado, poderá conduzir à criminalização dos movimentos sociais e seus manifestantes quando se utilizem de violência.

A adesão de cidadãos aparentemente inofensivos a estes movimentos decorre da formação de identidades no ciberespaço.

Até pouco tempo atrás as teorias da comunicação definiam como mídia de massa apenas a imprensa, o cinema, o rádio e a televisão. Atualmente, entretanto, a Internet já é tratada como uma nova mídia de massa. Se os processos comunicativos, no interior da cultura de massa, são objetos da Comunicação, os seus efeitos e a sua interação com a cultura e sociedade também podem ser objeto de estudo das mais variadas ciências cognitivas. A influência da globalização e da mídia, particularmente da Internet e dos meios digitais, na

constituição de identidades contemporâneas é um tema que merece melhor atenção em virtude da fluidez com que as informações e interações ocorrem neste espaço (SILVEIRA, 2004).

Conforme já discutimos, a Internet e o computador são mais do que meios de comunicação e instrumentos de trabalho, são também meios de interação e organização sociais e estão presentes em boa parte dos lares ao redor do mundo. A circulação das informações na rede e o seu respectivo impacto sobre os diferentes campos da relação humana fazem com que a influência da Internet abranja toda a sociedade (SILVEIRA, 2004)[26].

Caracterizado pela liquidez dos novos tempos (BAUMAN, 2001 apud NÓBREGA, 2010) inseridos em um espaço ciberespacial desterritorializado, os indivíduos constroem suas identidades de forma fluida, múltiplas e multifacetadas. Diferente da personalidade pautada pela tradição e fortemente influenciada pelo grupo, a identidade construída no ciberespaço também se torna mais pessoal e subjetiva, em constante construção e transformação, deixando de ser simplesmente imposta pelo grupo, para ter uma maior amplitude de escolhas (NÓBREGA, 2010).

Neste sentido,

> A pós-modernidade propiciou que as identidades se formassem em torno do lazer, da aparência, da imagem e do consumo. Consequentemente tornaram-se frágeis os laços que a delimitavam. Dentro da mídia, as redes sociais de relacionamentos como, Orkut, Twitter, Facebook, My Space, *Link*edin e jogos como o Second Life, dentre outros, configuram-se como um cenário amplo em que é permitido construir e divulgar a - ou as, já que o plural revela-se sempre mais adequado para falar de identidade - concepção identitária que se deseja (NÓBREGA, 2010, p. 7)[27].

A Internet tanto é um ambiente virtual capaz de gerar cooperação e participação democráticas inigualáveis como o contrário também é verdade. Castells (2000 apud SILVEIRA, 2004) nos alerta para o fato de que as redes são também extensões físicas do homem que lhe permitem não apenas se comunicar de formas diferentes mas construir verdadeiros espaços de sociabilidade.

Neste sentido, SILVEIRA (2004, p. 6) nos mostra que:

> Investigar o papel da Internet na textura da experiência também é avaliar como ela influencia a transmissão de valores e altera as relações entre as culturas locais e a cultura global. Provavelmente, o efeito mais aparente da Internet em relação às culturas locais é o de exacerbar os efeitos das mídias convencionais há bastante tempo denunciados pelas teorias críticas derivadas da escola de Frankfurt: favorecer o avanço sem fronteiras da indústria cultural, unificando valores, crenças, estilos de

[26] http://www.scielo.br/scielo.php?script=sci_arttext&pid=S141498932004000400006&lng=en&nrm=iso
[27] http://revistas.ucg.br/index.php/fragmentos/article/viewFile/%201315/899

> vida e determinando padrões de consumo, com o conseqüente enfraquecimento de identidades culturais e de laços comunitários tradicionais.

Assim, pertencer a uma determinada comunidade virtual é compartilhar de um mesmo território, que, desterritorializado, se torna universalizante, mas que permite participar de uma construção de identidade e representação simbólicas adquiridas também por intermédio de uma escolha, carregando consigo a segurança de sentimento de pertença, ao lado de várias outras pessoas que pensam e agem da mesma forma, reforçando o seu ideal de grupo e comunidade.

No ciberespaço, é comum a confusão de identidades, porquanto são múltiplas as escolhas. Essas escolhas são aquelas que pessoas com interesses e visões em comum fazem ao unir-se a determinados grupos com o objetivo de adquirir uma identidade que não é mais possível obter nem na cultura local, nem na cultura global, formando-se verdadeiras tribos. (SILVEIRA, 2004).

Tais tribos são amparadas na alteridade, que se constitui um princípio básico da identidade. A partir do momento em que os grupos ou comunidades virtuais se intitulam como tribos elas passam a fundar dois polos distintos: um "nós", que engloba os indivíduos semelhantes, em contrapartida com um "eles", que abarca o que seriam "os outros" (NÓBREGA, 2010, p. 98)." Enquanto o "nós" é visto como regra e algo que deve ser seguido, "os outros" são vistos como desviantes da norma, algo a ser evitado e por vezes, até mesmo repudiado "(SILVA, 2000, apud NÓBREGA, p. 98). Em que pese o internauta ter a pseudo ideia de que ao acessar o espaço virtual ele se auto representará, de modo genuíno ou como sendo algo muito distinto em relação aos outros, no mundo real, o que realmente acontece "[...] é um declínio da individualidade. De acordo com Maffesoli (1998), com a necessidade de identificação com o grupo, há um descolamento do próprio ego em nome do ego da comunidade. É o que ele chama de tribalismo pós-moderno" (NÓBREGA, 2010, p. 98).

Nestas relações opostas, entre o eu e o ele, existe sempre um desequilíbrio de poder, porquanto a oposição de interesses exige a subsunção de um pelo outro. Quando o sentimento de pertença à tribo adquire proporções exageradas, há uma tendência do indivíduo a nutrir sentimentos e estimular comportamentos de ódio contra o outro, tais quais os movimentos sociais e políticos violentos, o fundamentalismo religioso ou o terrorismo. O poder gerado pela construção de identidades no ciberespaço não se limita à formação destas identidades, mas se estende a necessidade de exibi-las reunindo tribos ou grupos com características semelhantes e excluindo, por conseguinte, grupos diversos.

A mobilização social, como ação planejada de pessoas que se reúnem em torno de um desejo ou ideal comum, também é fruto da reunião de grupos, que rompem a tradicional separação entre esfera pública e privada e toma para si a tarefa de efetivar o seu ideal comum. Os movimentos sociais se tornam violentos quando há um desequilíbrio de poder na oposição de interesses de grupos distintos, onde um desconstitui a identidade do outro, construindo a sua a partir da submissão de outras por meio da violência.

No Brasil, os movimentos levantados pelos "Black Blocs" foram representativos deste tipo de mobilização. As ações exacerbadas (fora da ordem e da pacificação) praticadas pelo grupo foram arrefecendo, não se repetindo nas manifestações posteriores. As articulações políticas, pelas redes, continuaram. Os movimentos de rua vivenciados por nós foram expressões de ciberativismo que, construído no ciberespaço, toma corpo fora dele. Nasce com isso uma nova conjectura de que a era da tecnologia da informação, dos novos meios de comunicação e das redes sociais, podem, sim, proporcionar meios, até mais eficientes, de mobilização político-social que, embora passível de desvios, podem se tornar um importante espaço de mobilização.

3.6 A RELAÇÃO ENTRE CIBERDEMOCRACIA E CIBERCRIME

Na trajetória da humanidade, o conhecimento representou uma importante mola propulsora, gerando transformações e mudanças significativas. O grande desafio da era da informação é constituir mecanismos eficazes que filtrem e desmembrem as práticas lícitas das ilícitas, uma vez que, no mesmo espaço em que se trocam conhecimentos, também vicejam fenômenos criminais complexos. O aspecto transformador, rico em potencialidades, que representam os diversos usos dos ciberespaços para a Ciberdemocracia, consubstanciados em seu potencial de liberdade, na possibilidade de formação de novas identidades e na desterritorialidade são, justamente, os que representam seu maior perigo. Quanto maior a potencialidade, maior o seu risco, o que nos conduz a um verdadeiro dilema. Devemos promover uma reflexão para que o propósito da Internet prevaleça como meio de se disseminar conhecimento, contribuir coletivamente para as causas humanas, simplificar a vida e construir uma sociedade igualitária com oportunidades equânimes, sem que isso represente um risco à paz social.

É necessário reduzir os malefícios que o anonimato presente na Internet possibilita e conscientizar-se eticamente para que possamos construir obstáculos quanto à presença da

criminalidade na Internet. E isso deve ser realizado sem que se perca a liberdade e o ensejo democrático que as diversas possibilidades de uso do ciberespaço nos oferecem.

Entretanto, as medidas protetivas e repressivas no combate aos delitos praticados na rede ou por intermédio dela não estão se mostrando eficazes e parecem insuficientes para o leque de possibilidades do ciberespaço, deixando lacunas perigosas. A dificuldade consiste, sobretudo, em orientar e educar as gerações que crescem neste ambiente e aquelas que estão se adaptando ao mesmo, de forma que todos possam tomar as precauções e diligências da vida virtual.

A gama de possibilidades oferecidas pela Internet e sua vasta rede de informações e comunicação devem ser utilizadas sem esquecer os deveres do mundo real e das instituições tradicionais, como a ética e a justiça, sem que seja necessário construir censuras.

Diego F. Migliorisi, sobre a regulação acerca do uso de ferramentas da Internet e apropriação do ciberespaço afirma que:

> Los usuarios de Internet no debemos permitir que la regulación se transforme en censura, ni que el libre albedrío convierta el ciberespacio en un lugar caótico y anárquico. Debemos sostener las banderas de la equidad y la justicia, construyendo barreras contra el Cibercrimen y estabeleciendo parámetros claros para que el control no afecte el preciado derecho de la liberdad de expresión y la intimidad de las personas, y cuidando que, su ejercicio, no afecte derechos de terceros. (MIGLIORISI, 2014, p. 263).

Diante do que foi narrado, vê-se a necessidade de uma conjunção de forças. A lei, por si só, não será capaz de frear e despertar nos indivíduos a consciência dos limites diante dos desafios impostos pelo mundo virtual. O projeto de conscientização e humanização do espaço digital não é tarefa de um organismo só, nem de um só internauta apenas. Continua a ser uma construção coletiva. É um projeto que deve ser estimulado na consciência dos usuários digitais com o intuito de criar uma população compromissada em cultivar a função criadora e transformadora da Internet, que é a de construir novo saberes, interações, direitos e conhecimento sob os preceitos éticos da sociedade.

As incertezas ainda são muitas quando pensamos os efeitos de existir e coexistir no ciberespaço. Dentre os diversos problemas enfrentados pelo usuário das redes de computadores, destacam-se:

> A falta de certeza com relação à proteção das informações e dos dados compartilhados contra acessos não autorizados; a não garantia da identidade dos usuários; a incerteza quanto ao uso devido dos dados e informações veiculados; a não garantia de veracidade da informação difundida; a dúvida com relação à proteção contra a cópia não autorizada de programas, dados e informações; a

> possibilidade de invasão por vírus prejudicando todo o sistema de arquivo de dados; a possibilidade de modificação deliberada de dados e informações; a não manutenção da privacidade. Estas são algumas das questões éticas que permeiam a utilização das NTIC (TRAUTMANN, 2002, p. 11).

Nesse espaço digital quase infinito, funde-se o público com o privado, o que dificulta enxergar a linha tênue de separação entre eles. Com isso, os seres humanos vão se automatizando e, por vezes, se perdendo no frenesi das massas. Nessa trama virtual, há, de um lado, a liberdade de manifestar-se e, de outro, o desejo de ocultar-se. Mas no seio do convívio social digital, aquele que tecla menos e não interage tanto, começa naturalmente a ser excluído. Daí há quase um imperativo virtual de se fazer presente o tempo todo.

> O sentido de participação se reflete também na obrigatoriedade de conexão, bem como nas atualizações constantes (não somente tecnológicas, mas também nas tendências, como as redes de relacionamento — Orkut, Facebook ou Twitter), mas expõe principalmente a fragilidade da condição em que a humanidade se encontra: a de se publicizar constantemente, e não somente o que reconhece como sendo o *eu* (o ego); parte do inconsciente [6] — esta codificada precariamente pela linguagem, pela cultura e pelas representações possíveis no aparelho psíquico humano — se põe à mostra para que qualquer ente conectado possa, com um pouco mais de habilidade, penetrá-lo, interpretá-lo e julgá-lo. O que se processava no privado, posto em significação pela consciência, mas retratando o inconsciente, torna-se público intencionalmente ou não (GODOI, 2014).

Na virtualidade, torna-se difícil conhecer a si mesmo, como numa lição socrática, muito menos conhecer e vislumbrar o alcance dos reais contornos do outro. Ao mesmo tempo em que sentimos temor do desconhecido, também nos sentimos atirados, com os sensos aguçados, em direção à descoberta de tantas experiências. O saber sobre si e sobre o outro sempre foi um desafio com limitações e dificuldades decorrentes da nossa condição humana. Pensar uma racionalidade que nos oriente nas vivências do ciberespaço é deveras importante para coibir comportamentos danosos a si e à sociedade.

> Existem, hoje, dimensões morais [ou uma única moral quando se considera a Cibercultura como um todo (ciberespaço, extensões protéticas ou modificações genéticas)] e nelas são propostos deveres religiosos e modernos ainda vigentes. Acredita-se, contudo, ao refletir mais precisamente o sentido da moral, no surgimento de outra forma desta, que não somente subverte as morais com as quais se convive, como demonstra que o dever-ser (em um mundo em rede) é aquele no qual se deve compartilhar, e desse modo pode-se eliminar o dever das instituições em detrimento do dever permissivo da conexão.Em outras palavras, a moral, o dever-ser, o certo para que se estabeleçam relações sociais é, hoje, o que "eu quero que seja", pois isso é compartilhado com um extenso grupo ao redor do globo e, portanto, legitima o objeto compartilhado (GODOI, 2014).

As dificuldades em se construir um senso ético e moral nos espaços virtuais se devem à sua intangibilidade e simplicidade. Embora a era da rede digital permita que as pessoas

viajem virtualmente de modo rápido e econômico para estabelecer a comunicação com outras pessoas do outro lado do planeta, o acesso fácil e rápido pode não garantir a real comunicabilidade entre os indivíduos, sendo semelhante a mais uma viagem de turismo em que se tiram fotos, conhecem-se os locais principais, mas dificilmente se trava um diálogo franco com os habitantes do lugar. O desafio é aliar informação adequada à comunicação efetiva, para se evitar a queda num vazio virtual. Essa regra é válida para a conversação, o diálogo entre pessoas, instituições, governos e nações.

A Cúpula Mundial da Sociedade de Informação teve a iniciativa de contribuir para se criar uma dinâmica salutar entre as esferas do poder público, dos agentes econômicos e da sociedade civil objetivando a formação de uma governabilidade das redes com normas claras para as relações travadas entre os referidos atores sociais. Exemplo de verdadeira regulação ciberdemocrática, os esforços da Cúpula esbarraram nos mais diferentes entraves políticos e econômicos decorrentes do monopólio de algumas nações e empresas digitais, bem como das legislações internas de outros países, da cultura, tradições, princípios e valores dos diversos povos.

Assim como existiram, ao longo da história humana, lutas, disputas por terras, nações e poder, na era tecnológica, há uma disputa crescente de domínio do ciberespaço, seja por organizações monopolistas, seja por indivíduos ou grupos que desejam se apoderar da "net" para desestruturar sistemas, cometer delitos econômicos, atacar pessoas, articular ações terroristas ou desorganizar e manipular os sistemas de segurança nacionais no mundo digital.

> O problema ético que subjaz a este debate é a ideia de que a humanidade só pode sobreviver se os processos de conhecimento do mundo, que nos permite criar novas condições de vida e melhorá-las, não estejam bloqueados por grupos ou monopólios que queiram tomar proveito às custas do que é comum a todos. Esta é a "tragédias dos comuns" (Garret Hardin), ou seja, o direito de manter aberto o espírito e o conhecimento humano, bem como os seus produtos, sempre corre o risco de ser utilizado por grupos particulares, em detrimento dos interesses comuns (CAPURRO apud LARA, 2014, p. 6).

Para Trautmann (2002) as discussões sobre o sentido da vida, a solução dos conflitos inerentes à nossa condição humana e à nossa convivência social, a tensão entre o ser e o dever ser não podem ser meramente reduzidas a um problema técnico. Para o autor, as pessoas devem continuar buscando respostas às perguntas fundamentais da vida pessoal e coletiva.

> [...] Viver e conviver num mundo onde não existem distâncias ou fronteiras, onde estar aqui e poder ir a qualquer lugar virtualmente e estabelecer o certo e o errado nesta convivência é o questionamento da atualidade. Toda cultura e cada sociedade instituem uma moral, ou seja, os valores que definem o bem e o mal, a conduta

> correta e o proibido. Porém, a existência de valores morais não implica a existência de uma ética, ou seja, de uma reflexão crítica que discuta e problematize os valores morais (TRAUTMANN, 2002, p. 30).

"Equilibrar o cientificamente possível com o eticamente admissível é o grande desafio deste novo século" (IUSKNOW, 1999, p. 6). Apesar do acesso a tantos recursos científicos e tecnológicos ter-nos trazido múltiplas possibilidades, trouxe, também, muitos questionamentos, especialmente no tocante às novas formas e condições de convívio e de existência do ser humano no ciberespaço.

4 TIPOLOGIAS DO CIBERCRIME E TRATAMENTO JURÍDICO-NORMATIVO

Neste capítulo, analisaremos os métodos modernos na execução dos Cibercrimes, assim como os agentes da delinquência no ciberespaço. Faremos uma tipologia dos principais crimes cibernéticos tais quais: pirataria, espionagem, pornografia, pedofilia, crimes de ódio, *ciberbullying*, fraudes eletrônicas e terrorismo virtual. Serão analisadas em conjunto, as leis que tratam sobre o tema, bem como legislações gerais e específicas. Em seguida, buscaremos compreender os preceitos do Marco Civil e suas consequências jurídicas no país. Ao final do capítulo, também investigaremos os principais pontos da Convenção de Budapeste e seus reflexos no Brasil, caso o país se torne signatário. Para isso é imprescindível conhecer as principais ameaças e os meios de consumação dos referidos crimes, assim como sua legislação em vigor, a fim de possibilitar, em momento posterior, a análise das formas de prevenção e combate ao Cibercrime.

4.1 O CRIME

O crime é um fenômeno social, episódio na vida de um indivíduo que o coloca à margem do que é desejável em um sistema jurídico. Entretanto, o crime não é um fato destacado da vida social. Um crime tem sua história e, em torno dele há circunstâncias, fatos e sujeitos que nos contam uma narrativa sobre ser ou estar no mundo em um tempo circunscrito, sob uma ótica que reflete apenas parcialmente a realidade de quem por ele é atingido.

Continuando o raciocínio acima, o crime poderia ser facilmente um fato cotidiano ou um acontecimento perturbador na vida dos sujeitos que se encontram por ele atingidos se não fosse sua ilicitude, tipicidade e culpabilidade.

No entendimento do célebre jurista brasileiro Francisco de Assis Toledo (1994, p. 80), o crime é um fato humano que lesa ou expõe a perigo os bens jurídicos (jurídico-penais) protegidos. É uma ação típica, ilícita ou antijurídica e culpável.

Para Rogério Greco (2014, p. 151), tipicidade é a conduta, fenômeno do mundo físico, que apresenta características específicas e busca sua adequação a um fato da vida real, a um modelo abstrato de tipo penal definido em lei; já a ilicitude se caracteriza pela proibição no momento de agir, e se conduzir de determinada forma, sem que haja exceção também prevista pela norma. A culpabilidade, por sua vez, é a motivação, as circunstâncias subjetivas que carecem de uma melhor investigação e que leva o sujeito a praticar a conduta.

A ideia de um conceito sobre crime existe desde o momento em que a sociedade decide atribuir uma punição para condutas indesejáveis por esta. Essa reprovação muda no espaço e no tempo, segundo os valores e interesses que diferentes sociedades buscam proteger, razão pela qual, quando se analisa a história do crime, a visão que cada época tinha sobre o fato, percebe-se que o sentido, a interpretação da ação criminosa e a maneira de reprimi-la invariavelmente são diferentes.

Beccaria (2006) utiliza-se da teoria do Contrato Social de Rousseau para explicar a origem das penas e delimitar o direito de punir. Neste contexto, o indivíduo sacrifica uma parcela de sua liberdade para viabilizar a sua sobrevivência pacífica na sociedade, devendo esta, em prol da qual se sacrifica oferecer-lhe segurança e paz social. A sanção para os que descumprem o acordo se configura na pena ou na necessidade de retribuir, seja com o intuito educativo ou punitivo (a depender da sociedade que a aplica), o descumprimento do acordo social, através da invasão às liberdades alheias. Contudo, as penas não podem exceder a porção mínima de liberdade depositada por cada indivíduo.

Assim, "[...] A reunião de todas essas pequenas porções de liberdade constitui o fundamento do direito de punir. Todo exercício de poder que deste fundamento se afastar constitui abuso e não justiça; é um poder de fato e não de direito; constitui usurpação e jamais um poder legítimo" (Beccaria, 2006, p. 19).

Atualmente, o Código Penal Brasileiro e outras normas de natureza penal tipificam condutas criminosas reservando-lhes penas. A referida legislação não explica o conceito de crime, este é desenvolvido pela doutrina.

O objetivo deste trabalho não é descrever tipologias de crimes, apenas conceituá-los segundo pressupostos compreensíveis ao leitor para melhor compreender a natureza das condutas indesejáveis à vida em sociedade.

4.2 OS CIBERCRIMES

Conforme já explanado, o conceito de crime adquire contornos diversos de acordo o desenvolvimento das sociedades. Em razão do avanço tecnológico ocorrido nas últimas décadas, o crime deixou de ser concebido e idealizado somente na esfera social habitual. Vê-se o crime também em uma realidade de outra esfera social: o espaço cibernético da web e das redes sociais.

A revolução tecnológica proporcionou uma grande velocidade de transmissão de informação e de renovação de tecnologias e facilidades, aprimorando a produção do

conhecimento, a capacidade de armazenamento de dados e mais uma série de benefícios ocasionados principalmente por conta do advento da Internet. Esta, consoante já dito, é uma rede mundial de computadores interligados a um protocolo padrão que é a base para o funcionamento de toda a gama de redes. As transformações advindas da globalização e da era da informação, a sensação de quebra de fronteiras e a facilitação de acesso a espaços desterritoalizantes, bem como a possibilidade de construção de múltiplas identidades facilitam o fenômeno do crime.

É fundamental a percepção de que o ser humano adquiriu uma maior fonte de liberdade na era da informação, um poder potencial que, administrado de forma errônea, gera consequências não desejadas na sociedade.

O problema chamou atenção das nações, desde o final da década de 1990, quando a Internet se disseminava. Um subgrupo das nações do G8, constituído pelos países mais desenvolvidos mundialmente, fez uma reunião na França, na cidade de Lyon, objetivando analisar os problemas relacionados à criminalidade decorrentes da ampliação das redes. Foi esse grupo que cunhou o termo "Cibercrime" de forma genérica, referindo-se aos crimes realizados pela Internet ou através de tecnologias digitais (BARBAI, 2013, p. 48).

Cumpre, entretanto, destacar que há uma dificuldade em determinar os bens jurídicos que devem ser tutelados pelo Direito Penal ao se falar em Cibercrimes. Percebe-se que comumente a conduta geradora de danos é a mesma que aquela considerada para os bens jurídicos comuns, entretanto é necessário vislumbrarmos também bens jurídicos não convencionais quando o tema em questão for o Cibercrime, visto seu caráter diferenciado quanto às outras espécies de infrações já tipificadas pelo ordenamento jurídico.

O estudo do fenômeno criminal relacionado ao ciberespaço apresenta inúmeras denominações no Brasil. Fala-se em “Direito da Informática”, “Informática Jurídica”, “Direito do Ciberespaço”, “Direito Eletrônico”, “Direito da Internet”, “Direito Virtual”, “Direito Digital”, dentre outras. Essa gama de nomenclaturas desenvolvidas faz com que surjam também denominações para os diversos crimes realizados no ambiente virtual que podem ser chamados de: “delitos informáticos”, “delitos virtuais”, “crimes” de “Internet”, “digitais”, “informáticos”, “telemáticos”, etc.” Percebe-se que não há consenso quanto a um nome específico para se referir aos delitos relacionados com os computadores e redes. Essa inconformidade também é percebida fora do direito pátrio

> No âmbito do direito internacional, [...] num estudo intitulado ‘Desafio de definir o cybercrime e particularidades criminológicas’ publicado na revista ‘Law and Technology’ da Masaryk University, República Tcheca, Zavrsnik relaciona, do

> mesmo modo, dez denominações para o fenômeno criminal, com as seguintes denominações em inglês: computer crime (crime de computador), computer-related crime (crime relacionado ao computador), crime in information science (crime da ciência da informação), ICT crime (crime de TIC – telecomunicações, informática e comunicações) [...] cybercrime (Cibercrime) e hig tech crime (crime de alta tecnologia) (MORAIS NETO, p. 25, 2009)[28].

O desafio de se estabelecer uma definição genérica para o fenômeno, assim como, um esclarecimento maior do mesmo, além de uma análise mais precisa, preocupa países do mundo inteiro, como Canadá, Austrália, Reino Unido, e outros. A União Europeia, distintamente, agrupou medidas de proteção de cunho social nacional e até mesmo transnacional a partir da Convenção sobre o Cibercrime, ratificada por vários países.

> Durante a participação em duas conferências que deram suporte a esta pesquisa, a SPCI 2008 - The First International Conference on Security, Privacy and Confidentiality Issues in Cyberlaw, realizada na cidade do Cairo, Egito e CYBERSPACE 2008, na cidade de Brno, República Tcheca, os pronunciamentos dos conferencistas de diversos países versaram, também, sobre a dificuldade de se chegar a um termo comum às condutas delituosas também se fizeram evidentes. Entretanto, foi possível observar que no âmbito das discussões acadêmicas e das apresentações dos conferencistas o termo mais empregado foi 'cybercrime' [...] (MORAIS NETO, 2009).

Na doutrina internacional, o termo 'Cibercrime' é o mais empregado. Já no Brasil, os autores preferem "crime informático" (praticado mediante emprego dos recursos de informática: computadores, impressoras, rede virtual), por acreditarem ser mais amplo e considerarem a definição Cibercrime restrita ao delito praticado na rede virtual.

Os crimes cibernéticos estão integrados no rol dos crimes informáticos que não exigem uma rede para se constituírem. O computador pode ser meio ou objeto final da execução criminosa. Segundo o mestre em ciências criminais, Maciel Colli (2010, p. 44), "os Cibercrimes pressupõem o envolvimento de mais de um computador ou dispositivo telemático ou eletrônico. Além disso, estas máquinas devem estar conectadas entre si por uma rede, seja ela material, seja ela imaterial (por exemplo, as redes *wireless*)."

O ciberespaço é uma esfera intermediária entre o mundo imaginário ou virtual, e o mundo real. Nesse ínterim, delitos cibernéticos ocorridos nesse ambiente são desprovidos da presença física do autor do fato. Sendo assim, os cibercrimes passam a ser caracterizados por uma conduta antijurídica e culpável, realizada por intermédio de um computador com possibilidade de conexão à Internet.

---

[28] http://www.ccj.ufpb.br/pos/wp-content/uploads/2013/07/Arnaldo-Sobrinho-Cibercrime-e-Coopera%C3%A7%C3%A3o-Penal-Internacional.pdf

Rossini conceitua "delito informático" como "uma conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, como o uso da informática em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática que tem por elementos a integridade, a disponibilidade e a confidencialidade. Para ele, o "delito informático" é gênero, do qual "delito telemático" é espécie, dada a peculiaridade de ocorrer no e a partir do inter-relacionamento entre os computadores em rede telemática usados na prática delituosa" (ROSSINI, 2004, p. 110, apud DULLIUS, HIPLLER e FRANCO, 2012).[29] Muitos crimes admitem execução no ambiente cibernético, Colares cita alguns:

> crimes contra segurança nacional, preconceito, discriminação de raça, cor e etnias, pedofilia, crimes contra a propriedade industrial, interceptação de comunicação de informática, lavagem de dinheiro, pirataria, calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação de direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, incitação ao crime, falsa identidade, inserção de dados em sistema de informação, falso testemunho, exercício arbitrário das próprias razões e jogos de azar (COLARES, 2002 apud DULLIUS; HIPLLER; FRANCO, 2012).

Nesse sentido, pode-se concluir que os denominados "delitos informáticos" não se tratam de crimes e contravenções penais restritos apenas ao âmbito da Internet, mas também abrangem os sistemas virtuais e até mesmo um computador "offline", que funciona como ferramenta para a concretização da conduta.

Assim, percebe-se uma certa universalidade na definição do crime de informática: faz referência à conduta tipificada em lei, a qual o computador tenha funcionado como instrumento para a concretização material do crime, a partir de seu objeto. Dessa forma, tal definição demonstra a diferenciação existente entre estes crimes e os demais, além do meio de execução – caracterizado pelo distanciamento entre a vítima e o agente.

Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados (ou a sua transmissão). Em síntese, consiste na utilização de um sistema de informática a fim de lesar um bem ou interesse juridicamente protegido. Como aqueles que integram a integridade corporal, a liberdade individual, o patrimônio público ou privado, ou quaisquer outras categorias protegidas pela norma jurídica penal.

Vale ressaltar que nem toda ação feita através do computador será caracterizada como sendo um "crime de informática". É preciso diferenciar os crimes comuns praticados pelo uso ou contra computadores, dos "crimes de informática" propriamente ditos.

[29] http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html

Dessa forma, os crimes descritos na legislação penal podem ser cometidos por meio do computador, entretanto existem novas condutas criminosas, oriundas de novos comportamentos sociais e avanços tecnológicos que, mesmo trazendo danos, ainda não conseguiram ser tipificadas pela nossa legislação.

Segundo Ferreira (1992, apud DULLIUS; HIPLLER; FRANCO, 2012)[30], é possível diferenciar os crimes virtuais dos crimes cometidos pelo uso do computador. Ele indica alguns destes:

a) Manipulação de dados e/ou programas, a fim de cometer uma infração já prevista pelas incriminações tradicionais;
b) Falsificação de dados ou programas;
c) Deterioração de dados ou programas;
d) Divulgação, utilização ou reprodução ilícita de dados e programas;
e) Uso não autorizado de sistema de informática.

Em resumo, "crime de informática" pode ser entendido como uma conduta ilícita e punível, cometida através de meios eletrônicos de processamento de dados e interligados entre si e em rede. Constitui um crime doloso, por estar presente o animus, a intenção de causar o dano. E, por isso, admite a modalidade tentada, que também será punível.

O meio pelo qual essas condutas podem ser praticadas envolve computadores, *modens, fax, softwares*, dentre outros instrumentos digitais. Os criminosos desvendam informações das mais diversas áreas, como: militares, bancárias e governamentais. Há uma pluralidade de *animus* nas condutas realizadas, desde uma simples brincadeira até a prática do terrorismo, podendo até mesmo desafiar sistemas de proteção de um país.

4.3 CLASSIFICAÇÃO DOS CIBERCRIMES

Os Cibercrimes podem ser compreendidos como puros, impuros ou mistos. O Cibercrime puro diz respeito a condutas ainda não tipificadas explicitamente no Código Penal ou legislação correlata, tendo como objetivo a invasão do sistema de computadores, bem como a adulteração dos dados e sistemas da máquina. O impuro, ou também denominado comum, faz referência a tipos penais previstos em lei, havendo variações no meio em que ele ocorre. Neste tipo criminoso, a Internet é utilizada como mero instrumento para a realização do delito já tutelado pelo Direito Penal. O crime cibernético misto é relativo à conduta a qual

[30] http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html

se faz imprescindível o uso da Internet, independente da natureza do bem que for violado (WANDERLEI, 2012).

Esses crimes também podem ser classificados pelo ordenamento jurídico como crimes de informática próprios ou impróprios. Os próprios são os realizados através de computadores ou sistemas de informática, exclusivamente. Já os impróprios podem ser praticados por diversos meios, além dos meios informáticos.

Como dito, o cenário virtual e suas tecnologias facilitam a execução de crimes e ampliam as possibilidades para a realização de tal prática. O crime acaba sendo acentuado por esse poder da Internet de divulgação imediata que detém um alcance incalculável. Ao longo do desenvolvimento tecnológico, esse poder foi-se potencializando cada vez mais. Anteriormente, existiam vários dispositivos comunicativos (como o telefone, o rádio, o computador, a calculadora, a televisão) e cada um era vinculado a uma função específica. Hoje, existem dispositivos que integram várias funções, como entretenimento, comunicação e transmissão de dados.

Um *smartphone*, por exemplo, permite o envio de mensagens instantâneas, visualização de fotos, conversação em redes, além de outras funções advindas dos mais diversos aplicativos. Em um mesmo suporte físico, existem vários aplicativos. A essa multifuncionalidade tecnológica dá-se o nome de Convergência digital. Este é só um exemplo do poder que a Internet oportuniza, e, a partir de tantas atribuições, pensamos no crime dentro deste contexto. A convergência digital é mais uma facilitação e permite diversidade nas formas de execução do crime. Uma pessoa pode ameaçar a outra por meio de várias redes sociais, mensagem ou telefone, por exemplo.

O uso da rede que, pelo que se propõe, é legítimo e profícuo acaba sendo realizado de maneira hedionda e ímproba. Existem inúmeros tipos de Cibercrimes disseminados por aqueles que não se conscientizam dos limites entre o público e o privado e de seus direitos e deveres no mundo virtual.

Embora conscientes da ocorrência de condutas criminosas, estamos longe de considerar aceitável o cometimento de crimes, estando sempre presente a indagação acerca da motivação dos agentes para tal. Analisar a personalidade e os padrões comportamentais dos autores que praticam crimes cibernéticos, de alguma forma, pode auxiliar no entendimento do fenômeno criminal e contribuir para a sua diminuição.

4.4 OS AGENTES DA CIBERDELINQUÊNCIA

Esse conteúdo pode ser bastante útil aplicado ao contexto do Cibercrime, para que se entenda a motivação dos delitos virtuais a partir de estudos sobre os perfis dos agentes e o tipo de delito que eles tendem a cometer. Desse modo, há algumas denominações utilizadas para caracterizar os autores dos ilícitos virtuais. Antes de explicitar as referidas nomenclaturas, vale esclarecer que o termo *hacker* é erroneamente utilizado como sinônimo de agente criminoso virtual, ou seja, aquele que invade um sistema computacional para fins ilícitos. Pelo senso comum, ele utilizaria seus conhecimentos profundos de sistemas operacionais e linguagens de programação para invadi-los com o objetivo delituoso.

Em muitos meios de comunicação e até mesmo em alguns trabalhos acadêmicos, os termos *Hacker* e *Cracker* são utilizados equivocadamente. Por isso, faz-se necessária uma breve distinção entre as duas nomenclaturas. A título de ilustração serão inicialmente apresentadas três notícias jornalísticas a seguir:

a) "Hackers roubam mais de US$ 1 bilhão em ataques a bancos"

b) "Cracker ataca outra empresa de MS e exige 3 mil dólares para devolver dados"

c) "Hacker que mira sites racistas e homofóbicos promete mega-ataque no Dia das Bruxas."

No caso "a", o termo *hacker* foi utilizado de modo inapropriado, pois, apesar de aparecer em muitas notícias associado a "roubo cibernético", à criminalidade, a expressão *hacker* é atribuída a programadores que utilizam suas técnicas, seus conhecimentos para invadirem sistemas, mas sem a finalidade criminosa. Trata-se de um *expert* em computação que estuda os sistemas, as programações e possuem habilidades avançadas, no entanto sem fim ilícito. Cassanti complementa que tais habilidades, em muitos casos, são utilizadas "pela própria polícia em investigações ou até mesmo no desenvolvimento de *softwares* com o intuito de limar brechas de segurança, criar novas funcionalidades ou adaptar as antigas" (CASSANTI, 2014, p.2). Na notícia acima, uma quadrilha intitulada de Carbanak, utilizou um vírus, infectou os sistemas das empresas com um *malware*, monitorando assim as máquinas, realizando operações que retiravam e transferiam dinheiro diretamente dos bancos, sem abordar ou atacar clientes. Segundo investigações, os envolvidos nestes "roubos cibernéticos" são integrantes da Rússia, Ucrânia e China. Eles atacaram mais de 30 países, como Alemanha Estados Unidos, Canadá, China, Ucrânia e Rússia.

Analisando o caso “b”, a palavra “Cracker” foi devidamente utilizada. No próprio texto, o jornalista esclarece didaticamente o significado do termo: “Mais uma empresa do Estado foi atacada por *crackers* (pessoas que quebram códigos de segurança com fins criminosos” (TONHATI, 2015)[31]. Os *Crackers* são conhecidos por realizarem práticas criminosas, mas de forma "profissional". Eles possuem alto conhecimento informático podendo romper a proteção de sistemas e *softwares* e se apropriarem de informações sigilosas destes. Eles analisam falhas do sistema e se aproveitam delas para invadirem a empresa, que acaba tendo prejuízos em grandes proporções (CARVALHO, 2005). O verbo em inglês “to crack” significa o ato de quebrar. “Entre as ações, estão a prática de quebra de sistemas de segurança, códigos de criptografia e senhas de acesso a redes, de forma ilegal e com a intenção de invadir e sabotar para fins criminosos”. (CASSANTI, p.2, 2014).

O caso “c” seria uma forma de ativismo. O *hacker* acaba invadindo o sistema para protestar e, em alguns casos, tirar a página do ar. No exemplo mencionado, um *hacker* anônimo ativista invade sites de grupos preconceituosos e discriminatórios (racistas, homofóbicos). Neste ano realizou mais de vinte ataques, dentre eles, contra o site godhatesfags.com ("deusodeiahomossexuais.com" em tradução livre), além de páginas da facção autodenominada "Estado Islâmico". Possuindo uma conta no *Twitter* sob o pseudônimo de *Amped Attacks*, ele invade as referidas páginas que pregam a discriminação e o ódio utilizando técnicas que conseguem destruí-las ou infectá-las até derrubá-las, impedindo o acesso. São ataques de “negação de serviço” (também denominados de DDoS Attack, a abreviação em inglês para Distributed Denial of Service). No caso em comento, a finalidade não é criminosa, mas uma forma de “ciberprotesto”.

Dado o exposto, nota-se que *hackers* e *crackers* são exímios conhecedores de programas e sistemas, possuindo habilidades prodigiosas, mas há entre eles uma importante diferença: os primeiros utilizam o amplo conhecimento para o bem, já os últimos, para fins criminosos.

Há outras denominações específicas de agentes ou atacantes virtuais, como são especificados a seguir.

Os denominados *Scripts Kiddies*, semelhantes aos *Lammers* e *Wannabes* - conhecidos por invadirem sistemas com intuito criminoso, porém de forma amadora. Estes violam sistemas de organizações diversas por meio de instrumentos disponíveis na web e com um

[31] http://www.midiamax.com.br/policia/251980-cracker-ataca-mais-empresa-de-ms-e-exige-us-3-mil-dolares-devolver-dados.html

conhecimento técnico mínimo, diferente do *cracker*, que age com muito profissionalismo (CARVALHO, 2005).

Os *Cyberpunks* também possuem alto grau de conhecimento, entretanto o utilizam para alertar a rede de computadores mundiais sobre as novas vulnerabilidades de sistemas e protocolos, e auxiliar no desenvolvimento de *software* protetor. Esses *hackers* corrigem as falhas e fazem testes de vulnerabilidade propiciando aos usuários a utilização dos sistemas de forma segura para suas operações. Eles objetivam aprimorar a privacidade de dados a partir do uso da criptografia. Esta é uma ciência que possui a função de transformar dados comuns em dados que não possuem significado e não são passíveis de interpretação quando são acessados por uma terceira pessoa não autorizada (o atacante). Assim, as informações continuam confidenciais e invioláveis. O dispositivo de segurança do sistema pode não resistir à invasão, mas o acesso às informações fica inviável. Eis, então, uma ideia muito importante que previne grandes prejuízos financeiros para organizações e garante a segurança de protocolos digitais, de dados de redes privadas virtuais e de certificados digitais, por exemplo (CARVALHO, 2005).

Os Caders são especialistas em furtar informações bancárias, especialmente, os dados de cartões de conta corrente, poupança, bem como cartões de crédito. Eles compram *on-line*, fazem transações e movimentações bancárias utilizando os números que foram "roubados" virtualmente, ou gerados por meio de *softwares* próprios para tais finalidades (CASSANTI, 2014, p. 2).

Já os *Insiders* focam na prática criminosa, geralmente a espionagem industrial, a engenharia social e subornos. Os atacantes que integram essa categoria costumam ser funcionários e ex-funcionários da própria empresa que violam os dados confidenciais ou prejudicam o sistema. Aproveitam-se do conhecimento da dinâmica referente à organização, seus processos e o acesso a certas informações e sistemas a ela referentes.

Há também, os pichadores virtuais, os *defacers*, especialistas em pichar páginas como forma de protesto.

Spammers, que na descrição de Cassanti disseminam "*e-mail*s com correntes e vírus que podem danificar e roubar informações dos usuários, como senhas bancárias" (CASSANTI, 2014, p. 3).

Os *Coders*, diferentemente, compartilham o que aprenderam objetivando a produção de novo conhecimento e práticas visando o desenvolvimento tecnológico. São conhecidos por criar programas e reproduzir ensinamentos sobre o tema. Na mesma perspectiva, seguem os *White Hats*, *que* visam corrigir e analisar inseguranças de sites. Os *Black Hats* invadem

sistemas a fim de roubar informações sigilosas e, assim, beneficiarem-se financeiramente. Por fim, existem os *Phreackers* que são agentes de fraudes telefônicas, adulteram também contas de operadoras, etc (CARVALHO, 2005).

São diversos os modos de ataques comuns na Internet, principalmente devido ao fato de muitos dos criminosos saírem impunes. No Brasil, devido ao sistema carcerário ser precário, o Judiciário acaba optando por penas alternativas. A maioria desses crimes cibernéticos não é praticada com grave ameaça ou violência. Isso favorece os cibercriminosos, pois muitos não são presos num primeiro momento, ou quando o são, ficam livres mais facilmente e tornam a delinquir. Os agentes dos crimes como fraude bancária e pornografia infantil tendem a ser reincidentes facilitando a continuidade dos ataques. A seguir, o QUADRO 1 mostra alguns dos ataques mais comuns:

Quadro 1 – Ataques comuns

Lojas virtuais falsificadas	São centenas – muitas vezes com preços bem abaixo do comum e contendo muitas promoções. É comum surgirem em maior quantidade em períodos como final de ano e *Black Friday*, quando oferecem produtos pela metade do preço, atraindo consumidores para as compras. Geralmente, usam nomes muito semelhantes aos de lojas consagradas pelo consumidor. Fazem a venda e, quando a promoção acaba, simplesmente excluem o site deixando o comprador sem o dinheiro nem o produto.
Phishing	Algo muito frequente é uma maneira de fazer a pessoa informar os dados pessoais, achando que eram para alguma finalidade, quando na realidade estão sendo roubados por criminosos. Geralmente é feito através de *e-mail*s informando que a pessoa ganhou um prêmio ou algo do tipo, e, para isso, é necessário passar os dados.
Kit boleto	São mais sofisticados, e aproveitam uma forma de pagamento exclusiva no país. Os agentes exploram táticas, como o *phishing*, para instalar um software na máquina da vítima. Quando o consumidor gera um boleto pela Internet, o programa automaticamente altera o código de barras, direcionando o pagamento para uma conta bancária controlada pelo hacker. Também há os que se passam por instituições bancárias e mandam *e-mail*s cobrando falsas dívidas.
Concursos via Facebook	Os criminosos se passam por uma companhia aérea ou grande loja e lançam promoção na rede. Para participar do sorteio, a pessoa precisa informar vários dados pessoais, que depois são usados para golpes.
Aplicativos maliciosos	Existe uma série de aplicativos feitos especialmente para roubo de dados em *smartphones* ou computadores. Eles também enviam mensagens de texto com cobrança adicional sem que os consumidores saibam. No geral, eles são apresentados como com um aplicativo promissor e cheio de facilidades, mas, ao serem baixados pelos usuários, são usados para roubo de dados.

Fonte: Elaborado pela autora, 2015.

O que também contribui para a grande ocorrência desses ataques são o baixo grau de informação de que a população dispõe em relação aos riscos digitais. Boa parte dos internautas é ingênua ou desavisada, e acaba sucumbindo às práticas dos criminosos. Para alguns estudiosos especialistas em Direito e Ciência da computação, o tema segurança digital deveria ser abordado nas escolas, organizações, na sociedade como um todo, pois o mundo tornou-se digital (PINHEIRO, 2013).

Outros tipos de invasões e ataques estão descritos na tabela de ameaças, Apêndice G deste trabalho.

4.5 CIBERCRIMES COMUNS NO UNIVERSO DIGITAL

Neste tópico, serão apresentados e analisados alguns tipos de Cibercrimes com características e peculiaridades próprias. Alguns menos lesivos, outros com alto grau de ofensa jurídica, deixando marcas e consequências indeléveis na esfera social. As espécies delitivas apontadas na pesquisa são ilustrativas e exemplificativas, não havendo o intuito de esgotar o rol de crimes cibernéticos, mas passar as principais ações que tipificam alguns crimes virtuais.

Verifica-se que, em alguns casos, tais crimes do ciberespaço trazem apenas um modo de agir, o chamado *modus operandi* novo, mas seu conteúdo ofensivo continua sendo o mesmo previsto na legislação penal em vigor. Por outro lado, serão analisados alguns casos que não encontram descrição legal no ordenamento jurídico pátrio, necessitando de legislação específica, ou, pelo menos, regulamentações que possam acompanhar o avanço tecnológico hodierno.

4.5.1 A espionagem

Desde os primórdios, a informação, enquanto produto da linguagem, apresentou-se como um bem importante. Os registros mais antigos das aventuras dos povos mostram que a busca por informação e a espionagem eram práticas comuns exercidas por agrupamentos humanos, exércitos e povos. O espião ou espiã é a pessoa que pratica o ato de espionagem. Espiar, em um contexto léxico, significa espreitar. A espionagem é a atividade formada por um conjunto de técnicas e práticas de observar, de forma dissimulada, com o intuito de obter informação e conhecimento, para si ou para outrem.

Em sua Ilíada, Homero descreve como os gregos, na ocasião do cerco à cidade de Troia (Ílio) se valeram de incursões ao acampamento troiano para obter informações estratégicas. Avançando na História, inúmeros casos de espionagens, informações e contrainformações definiram o rumo de conflitos, quedas e ascensões de impérios. Durante a Segunda Grande Guerra, a sorte dos aliados começou a mudar depois da quebra do código Enigma, sistema de criptografia dos alemães. A partir dele, os aliados podiam prever as atividades militares do Reich bem como localizar suas posições bélicas. Podendo "prever o futuro", o destino das Forças do Eixo estava selado em uma série de reveses que culminou com a derrota total da Alemanha e seus aliados.

Individualmente, personalidades históricas se destacaram na arriscada, misteriosa e, de certa forma, glamourosa, atividade de espionar. Mata Hari, uma das mais célebres espiãs da era moderna, ficou imortalizada na literatura e no cinema. Depois de transitar pelas altas rodas do oficialato alemão e francês durante a Primeira Guerra Mundial, a holandesa teve um fim trágico diante de um pelotão de fuzilamento em outubro de 1917. No cinema, o mais famoso personagem, o agente britânico "com licença para matar", James Bond, encarna o arquétipo do cerne da espionagem: uso de todos os recursos econômicos, materiais e tecnológicos, na viabilização de operações clandestinas, à revelia de autoridades e governos, em muitos casos, como em uma esfera de moral à parte, cometendo uma série de ilegalidades, entre destruições e assassinatos.

No livro '1984', a mais conhecida obra de ficção de George Orwell, é traçado um perfil sinistro de uma sociedade totalmente controlada, onde todas as esferas da vida privada são vigiadas e monitoradas por um governo autoritário, que usa a informação como ferramenta de controle e alienação da população. Nessa realidade cinza, os seres humanos têm suas existências esquadrinhadas pelo "Grande Irmão", representação do fascismo institucionalizado em escala global.

Ficções à parte, vivemos em uma realidade onde, se não temos charmosos espiões com "licença para matar", como os do cinema, temos agentes de carne e osso: espiões dos mais variados serviços secretos, *mariners*, *seals*, entre outros membros de esquadrões de forças especiais, executando operações secretas e ilegais nos mais diferentes rincões do planeta. Com o advento dos satélites, da Internet e das demais tecnologias digitais de comunicação, a humanidade, se por um lado experimenta um nível de conectividade nunca antes imaginado, por outro nunca foi tão vigiada, controlada e teve sua vida influenciada pelo controle de informações. Diante de tal quadro, se George Orwell fosse vivo, talvez veria o seu romance "1984" como uma ficção inocente.

Além dos agentes e demais funcionários das agências de inteligência, a espionagem e controle de informações ocorrem, sobretudo, nos meios virtuais, executados por programas espiões, robôs – *softwares* inteligentes – super antenas e super câmeras, *drones*, entre outras tecnologias de ponta. A Internet, bem como o sistema de telefonia, nunca foram meios seguros. Se por um lado, o mundo avança no desenvolvimento de tecnologias que buscam a segurança e a privacidade na rede, por outro, proliferam artefatos tecnológicos e superprogramas que buscam burlar as travas de segurança bem como rastrear o tráfego de informações na Internet e nas ligações telefônicas.

A espionagem eletrônica tem-se potencializado nos últimos anos, já que o mundo está cada vez mais conectado. O monitoramento tem-se tornado cada vez mais habitual, pela presença de tecnologias ao nosso redor continuamente. A prática não está resumida a invasões a computadores. Funcionários das empresas, ou terceirizados, podem contribuir para tais crimes, algumas vezes até sem sequer imaginar que o estão fazendo.

> A fragilidade está nas pessoas, principalmente no funcionário, seja ele próprio ou de empresa fornecedora (terceirizado), por diversos tipos de motivação, é envolvido para permitir o acesso ao ambiente (deixar a porta aberta), ou ele mesmo agir em nome de quem o contratou (pode ser coletando e enviando informações, pode ser apagando as mesmas na rede, entre outras situações). Há ainda o "laranja", que seria aquela pessoa envolvida na espionagem por ingenuidade, inocência, ou até mesmo negligência (PINHEIRO, 2013).

Considerando-se que os mais diversos interesses ditam as regras da geopolítica, a espionagem afigura-se como recurso sedutor aos governos e regimes políticos que pretendem a hegemonia em determinada região ou setor econômico. Sabe-se que o que determina o nível de monitoramento e buscas ilegais de informações de determinado governo, ou organização comercial é o seu poderio econômico. Diante desse fato, sempre houve a suspeita, e até concordância tácita, de que as potências mundiais, sobretudo os EUA, algumas nações europeias, e a Rússia direcionam suas antenas ao chamado mundo subdesenvolvido e, em alguns casos, em desenvolvimento. Assim sendo, surgiram iniciativas que procuram contrapor e clarear zonas cinzentas no obscuro mundo de informações e contrainformações. Julian Assange e o site *Wikileaks* são os nomes mais conhecidos nessas práticas contestadoras. Recentemente, outro personagem emergiu do velado lago dos segredos e espionagens em nível mundial.

Edward Snowden, um norte-americano ex-funcionário da CIA, veio a público denunciar o esquema global de monitoramento e espionagem implantado pela Casa Branca. Snowden relatou minúcias da operacionalidade das agências de informação ianques, e do

PRISMA, o seu superprograma de espionagem e monitoramento, por meio de uma reportagem ao jornal britânico *The Guardian,* onde confirmou a suspeita mundial de que os norte-americanos estariam vigiando, espionando e exercendo controle sobre diversas pessoas ao redor do mundo, inclusive em solo brasileiro, no qual o governo norte-americano realizou operações ilegais por intermédio de monitoramento das atividades de funcionários do governo e da Presidente da República, tema de que trataremos, no capítulo 5 deste trabalho.

Criticando a leniência dos poderes públicos diante das revelações de Snowden em relação à espionagem perpetrada pelo governo norte-americano a membros do alto escalão do governo brasileiro, o professor do Departamento de Ciência da Computação da Universidade de Brasília, Pedro Rezende, em entrevista ao jornalista Pedro Canário, afirma que o Estado Brasileiro "nunca perdeu sua vocação de colônia ou o pendor de suas elites para o alinhamento automático ao mais próximo império da vez, por baixo do verniz de tal defesa" (REZENDE, 2014)[32].

A partir do vazamento de documentos, foi descoberto que a Agência de Inteligência Estadunidense realizava o monitoramento de ligações, *e-mail*s e outras informações, de deputados, ministros e até mesmo do Gabinete da Presidência da República, o que configura uma grave violação da soberania do Estado. Ainda, segundo informações do ex-agente da CIA, os Estados Unidos monitoram quaisquer governos, independentemente do alinhamento político, em todos os continentes.

A espionagem industrial, por exemplo, é uma espécie de espreita que objetiva o furto de informações estratégicas confidenciais, a fim de se obter vantagem econômica. Isso é chamado no âmbito das empresas de *benchmarking.* A ação de grupos que roubam informações de uma empresa comercial, com tal fim, por exemplo. Ou, até mesmo a ação de uma empresa que realiza a invasão e tem acesso a informações de seus concorrentes, podendo assim realizar ações que os prejudiquem. Um agente que se infiltra na empresa na categoria de funcionário dessa, acaba tendo acesso facilitado a documentos sigilosos, e outros meios. A prevenção de tal prática, assim como da espionagem em termos gerais, pode ser realizada por meio do cuidado com a orientação devida aos funcionários para evitar os *insiders* (conforme visto, são pessoas infiltradas com o objetivo de realizar espionagem), regulamentação de uso de dispositivos móveis, o controle mais rígido sobre as informações confidenciais, utilização de um profissional experiente para evitar a infiltração de *softwares*, sistemas de segurança

[32] http://www.cic.unb.br/~rezende/trabs/entrevistaCJ.html

para dificultar o acesso aos computadores, realização de *backup* e restauração de dados, frequentemente (SILVA, L., 2015).

A prática de espionagem, constantemente negada por governos ou agências de inteligência, é denunciada e severamente repreendida em muitos países. Costumeiramente, as agências de inteligência omitem a prática, apesar de assumirrem publicamente, operações de contraespionagem. A espionagem pode ser definida como:

> A Atividade de Inteligência ou Serviço de Informação ou Serviço Secreto ou *Espionagem* é a implementação de um sistema de coleta de dados e informações para identificação de ameaças e oportunidades para uma organização com o escopo de ajudar o líder ou tomadores de decisão na elaboração de planos estratégicos ou execução de ações táticas e operacionais de ataque, manutenção e defesa dessa organização. Informação é o produto resultado do trabalho sistemático de coleta, análise e entrega de dados e informações chamadas Atividade de Inteligência (MONTALVÃO, 2015).

Em todas as legislações internacionais, o crime de espionagem é severamente punido. Nos Estados Unidos, a prática é punida com a pena de morte ou prisão perpétua. Se o crime for praticado por um natural do país, o delito é enquadrado como crime de traição, o que, geralmente, acarreta pena capital.

A lei Nº 7.170, DE 14 de dezembro de 1983, que versa sobre os crimes de espionagem, define as penas máximas em 30 anos de reclusão – maior penalidade permitida na Lei brasileira – além do crime ser também objeto da Legislação Especial Militar.

4.5.2 Pirataria

Alguns crimes cibernéticos são vistos como uma prática social comum e habitual. Este é o caso da pirataria. De acordo com o art. 1º do Decreto 5.244/2004, que regulamenta o Conselho nacional Contra a Pirataria e Delitos Contra a Propriedade Intelectual– CNCP, constitui crime de pirataria: “a violação aos direitos autorais de que tratam as Leis nos 9.609 e 9.610, ambas de 19 de fevereiro de 1998“. Esse conceito remete para duas leis, que regulamentam respectivamente “os direitos de autor de programa de computador” e “os direitos de autor e os que lhe são conexos“.

O conceito posto pela Lei é impreciso e vago. Os direitos supracitados são os chamados Direitos Autorais utilizados em referência ao rol dos direitos dos autores de suas obras intelectuais que podem ser literárias, artísticas ou científicas. A pirataria, em um

contexto jurídico, significa romper a proteção jurídica dos direitos do autor de obras intelectuais.

A denominada "pirataria", alimenta uma economia informal, mas provoca grandes prejuízos à economia brasileira. Segundo o sistema FIRJAN de informação, a pirataria movimenta U$ 2,2 bilhões ao ano no Brasil, o país perde 2 milhões de empregos devidamente formalizados, cerca de R$ 40 bilhões de impostos por ano não são arrecadados e as empresas são bastante prejudicadas. A pirataria é tipificada no artigo 184 do Código Penal. Diz respeito à reprodução, venda ou distribuição de produtos sem o pagamento dos direitos autorais. Os produtos pirateados mais comuns são: CDS, DVDS, acessórios, roupas e brinquedos. É muito realizado também o *downloading* de músicas e livros de maneira ilegal.

Diante de um meio onde a informação é disponibilizada e compartilhada tão fácil e rapidamente, muitas pessoas têm a falsa impressão de que têm o direito de se apropriar da criação alheia. Com o avanço tecnológico, houve a desmaterialização da obra em seu primitivo suporte físico tradicional. Do livro, ela passou a ser veiculada em CDs, *pendrives* ou até mesmo *on-line*. A pirataria, em tempos atuais, é fruto da reprodução indevida de diversas espécies de obras, programas de computador, artigos, bancos de dados, imagens, livros digitais, músicas, entre outros. É necessária a conscientização dessa moderna formatação e veiculação das obras, para que se possa utilizar dos benefícios que ela traz assim como compreender que, ainda que em ambiente digital, existe limite entre o público e o privado e deve-se manter o respeito aos direitos do autor. Assim, devem-se criar novas formas de proteção atualizadas pelo contexto em que o mundo está inserido hodiernamente. Hoje, existem *softwares* que possibilitam a criação de uma chave de proteção da obra original na Internet e não permitem a manipulação de edição da obra.

Além disso, no Brasil, os produtos culturais são vistos como artigo de luxo, pois materiais como CDS e livros, por exemplo, são extremamente caros comparados à renda salarial mínima do brasileiro. E a pirataria possibilita a aquisição de "cópias" desses produtos por um preço muito mais acessível (o que não justifica a prática delituosa). Por esses motivos e principalmente por ser uma prática rotineira, muitos defendem a aplicação do princípio da Adequação Social (que afasta a tipicidade penal de certas condutas com o argumento de uma aceitação social dessas), presente no Código Penal, para afastar tal crime.

> [...] com a facilidade de acesso e as tecnologias de reprodução, a situação de infração deixou de ser uma exceção, uma ocorrência pontual, para se tornar não apenas comum, mas também "socialmente aceita". Já ouvi frases como "mas se não é para copiar por que tem o gravador de CD/DVD?" (PINHEIRO, 2013, p. 142).

Porém, o Estado tutela os direitos autorais garantindo a sua proteção na Constituição Federal. E, apesar do dilema doutrinário, a lei é clara e está em pleno vigor. A súmula 502 do STJ (Supremo Tribunal de Justiça) reforçou ainda o entendimento sobre a criminalização da pirataria e a não admissão de possibilidade de aplicação do princípio de adequação social.

É fato que a Internet democratizou o acesso às informações e conhecimentos, conteúdos dos mais variados, além de permitir uma série de oportunidades e auxiliar na revelação de novos talentos. No entanto, deve-se ter cuidado com toda essa facilidade de "copiar" para não se chegar a um estágio de estagnação do conhecimento e da criação, do próprio pensamento. O direito autoral, que visa proteger a inovação e a remuneração do criador para retornar o investimento que esse fez no desenvolvimento de sua criação, é legítimo e não pode ser ignorado. “Não se pode permitir a formação de uma geração de plagiadores, de copiadores, de pessoas que dizem "achei no Google". O Direito deve proteger o autor para proteger a própria evolução da Sociedade” (PINHEIRO, 2013, p. 143).

4.5.3 Pornografia Infantil e Pedofilia *on-line*

O crime mais denunciado da Internet em 2013, de acordo a SaferNet, foi a pornografia infantil associada à pedofilia *on-line*. Estes delitos, assim como a pornografia em geral, têm alcançado grande proporção danosa por conta da facilidade que a tecnologia oferece para proliferação de páginas na Internet que contêm material de pornografia infantil. É comum a exibição de fotos de adultos explorando sexualmente crianças e adolescentes, ou a exibição de fotografias expondo a nudez infantil, ainda que com o intuito não sexual.

Este tipo condenável de delito é empreendido, na maioria das vezes, por associações de pedófilos que se valem da rapidez, amplitude e impunidade oferecidas no ciberespaço para compartilhar, distribuir e comercializar o material reprovável. A Internet, popular e acessível, parece o meio mais propício para se realizarem práticas como essa. Muitas crianças e adolescentes são expostos a esses riscos por conta da popularidade das redes sociais, nas quais, publicam fotos e informações pessoais e não imaginam os perigos que correm com tal atitude. As redes sociais são um lugar onde o acesso e a distribuição de pornografia e a pedofilia pode ser realizada de forma discreta e ágil através de perfis falsos que, muitas vezes, enganam as vítimas, uma vez que passam uma imagem amigável, cordial, interagindo e criando proximidade, de modo que não se levantem suspeitas. Assim, faz-se o compartilhamento anônimo e a cópia das imagens do perfil do menor e, também, a prática da pedofilia.

> É interessante acrescentar que criminosos com esse tipo de desvio de conduta procuram realizar atividades que permitam que tenham contato com suas potenciais vítimas, e, no âmbito da Internet, esse tipo de comportamento se repete. Além disso, as redes sociais representam verdadeiras "vitrines" para esses criminosos escolherem suas vítimas, que dificilmente fazem ideia do perfil psicológico desse tipo de pessoa (JORGE; WENDNT, 2013, p. 100).

Por conta dessa exposição realizada tão naturalmente nos dias hodiernos e da facilidade para a conduta criminosa em tal espaço, é essencial o acompanhamento familiar. Há necessidade de que os pais tenham ciência do conteúdo postado pelos filhos nas redes e do perfil das pessoas com quem estes realizam contato, oferecendo uma proteção que normalmente exerceriam em espaços físicos.

Existe uma cultura social que repudia esses tipos de prática, associando os menores de idade a uma imagem de pureza e inocência e pregando sua necessidade de cuidado e proteção. Ainda assim, o uso do meio virtual para tais crimes viola o direito da criança e do adolescente, sua dignidade sexual e integridades moral e psíquica, mesmo havendo o distanciamento físico.

O marco jurídico de proteção e reconhecimento dos direitos das crianças e adolescentes surgiu com a Constituição Federal de 1988, que trata os menores com prioridade por estes apresentarem pouca ou nenhuma capacidade de defesa. A Lei 8.069/90 do Estatuto da Criança e do Adolescente (ECA) reforça tal princípio constitucional no sentido de abordar os seus direitos e garantias fundamentais e considerá-los como sujeitos de direitos para que eles não sejam tratados como seres inferiores pela sua condição de dependência. Visando prevenir ainda mais os menores, contra abusos sexuais e ampliando a sua proteção legal, surgiu também a Lei 10.764/03 que modifica o art. 241 do ECA. Observando a grande incidência do crime ainda com tais avanços jurídicos, foi sancionada a Lei 11.829/2008 (resultado da CPI da pedofilia) que intensificou a proteção infantil visando aprimorar o combate à produção, venda e distribuição de pornografia infantil, criminalizando a aquisição do material e várias condutas de pedofilia na Internet. A identificação do endereço IP do usuário do computador, que realizou as operações criminosas na web, vai contribuir para se buscar a identidade do agente. Porém, ainda assim, por conta da grande facilidade da execução do crime por meio virtual há a potencialização dos delitos de pedofilia e pornografia infantil, que continuam ocorrendo em proporção preocupante.

4.5.4 Crimes de ódio virtuais

Os crimes de ódio realizados no espaço virtual parecem exprimir uma contradição, pois um meio que tem um potencial tão grande para unir pessoas e realizar conquistas presta-se a práticas segregacionistas típicas dos tempos mais bárbaros e beligerantes. São declarações de racismo, homofobia, xenofobia, neonazismo, intolerância religiosa, e outras disseminadas nas redes a todo o momento. Um exemplo notável foi visto durante as eleições de 2014, quando esse crime ficou em evidência e houve um grande aumento de denúncias relacionadas a declarações preconceituosas - por parte de opositores à reeleição de Dilma Rousseff - contra o Nordeste e outras regiões, onde houve predominância de votos a favor da então candidata.

Discursos carregados deste teor degradante de discriminação a grupos sociais específicos, além de exporem as vítimas, por conta da grande repercussão que a Internet possibilita, também garantem uma certa apologia e incitação a atitudes e ideias agressivas e preconceituosas.

> A Internet pode unir as pessoas, mas também as pode dividir, tanto a nível individual como em grupos mutuamente suspeitos, separados por ideologias, políticas, posses, raças, etnias, diferenças de geração e até mesmo de religião. Ela já tem sido utilizada de maneiras agressivas, quase como se fosse uma arma de guerra [...]. (FOLEY, 2002, p. 5).

A atuação de grupos racistas, entre outros, na web, se desenvolve pela veiculação de imagens, vídeos, comentários de cunho discriminatório, entre outras declarações que ofendem a etnia, raça, cor, religião ou nacionalidade. Tais atos estão previstos no Código Penal, como crime inafiançável, conforme a Lei 9.459/1997. As provas para tais crimes são obtidas pela geração de *logs* (registro de eventos realizados no sistema computacional) que identificam o dono do conteúdo discriminatório na Internet. Além disso, é utilizada a infiltração de policiais que simulam interesse em fazer parte de grupos racistas para obterem informação sobre eles e provas incriminatórias (WENDT; JORGE, 2013, p. 101).

Muitos desses crimes são cometidos por grupos conhecidos como neonazistas. Esses grupos resgatam a ideologia do nazismo dos anos 30/40, acreditando em uma raça soberana que seria a "raça pura ariana". Mesmo não se intitulando racistas, é claramente visível que suas práticas possuem tal caráter. Eles cometem atos de discriminação contra negros, homossexuais, índios, nordestinos, dentre outras minorias. Além disso, realizam reuniões para disseminar o ideal e integrar, cada vez mais, jovens ao grupo. Eles propagam o ódio racial,

atribuindo os problemas sociais de um país a tais minorias e ferindo a integridade física e psíquica destas frequentemente.

Os crimes de ódio virtuais citados acima, apesar de realizados na Internet estão claramente previstos na Declaração Universal dos Direitos Humanos que assegura a igualdade e liberdade sem distinção de raça, cor, sexo, língua, religião, opinião de qualquer natureza, origem social ou nacional e qualquer outra condição. Praticado frequentemente contra minorias sociais, este tipo de crime intensifica os problemas de desigualdades sociais e marginalização no país. É uma prática ignorante, por parte daqueles que não sabem se relacionar com as diferenças sociais e culturais, logo no país do multiculturalismo. Esta prática ilícita fere a dignidade humana e se classifica como um crime coletivo por ser facilmente ampliado nas dimensões virtuais, agravando, ainda mais, sua ilicitude. Os perigos apresentados e a complexidade do problema despertaram a atenção da Secretaria de Direitos Humanos da Presidência da República do Brasil que decidiu utilizar *software* para mapear ocorrência deste tipo de crime na Internet. O *software* identifica ofensas a grupo de pessoas e encaminha as denúncias ao Ministério Publico.

4.5.5 O *bullying*, as ofensas à honra e a apologia ao suicídio

O *bullying c*aracteriza-se por ser um ato em que se emprega a violência verbal e/ou física praticada por um agente ou por um grupo contra outrem com o objetivo de intimidar, ridicularizar ou causar dor. É comumente praticado nas escolas, especialmente entre crianças e adolescentes. Etimologicamente o vocábulo *bullying* origina-se do substantivo inglês Bull que traduzido para o português quer dizer touro. E, ao acrescentar a letra y, transforma-se num adjetivo significando brigão, tirano, valentão (MELO, 2011). O touro é um animal de porte físico robusto que intimida e causa medo, subjugando um ser humano comum.

Assim, o *bullying* pode ser uma agressão física, psicológica ou verbalizada. Simbólica ou não, é um tipo de violência que pode ocorrer nas escolas, nos locais de trabalho ou até mesmo, no ambiente familiar. A educadora Cleo Fante menciona: "Por consenso entre os pesquisadores brasileiros, o termo *bullying* é utilizado somente na relação entre crianças e adolescentes. Entre pares adultos é utilizado o termo assédio moral" (CLEO apud CASADO, 2015)[33]. O assédio moral remonta à antiguidade e esteve presente em várias agremiações humanas, ocorrendo de forma silenciosa, porém intensamente de modo nocivo. Em diversas

[33] http://www.viajus.com.br/viajus.php?pagina=artigos&id=4231&idAreaSel=20&seeArt=yes

searas do convívio humano, o referido assédio acontece, podendo ser laboral, prisional, homofóbico, militar, dentre outros. Casado (2015) observa ainda que "o *bullying* tem sido a nova nomenclatura dada ao assédio moral e pode ser perpetrado de diversas maneiras"

No entendimento de Melo, o *bullying* seria:

> uma agressão física, psicológica, verbal, moral, sexual, material ou virtual; praticada por uma ou várias pessoas contra uma mesma vítima;de forma repetitiva;por um período prolongado de tempo;sem motivo aparente; baseada numa relação desigual de poder dificultando a defesa da vítima, e que deixa sequelas, marcas, consequências (MELO, 2011, p. 21).

O *Bullying* praticado de modo virtual é fruto do novo contexto tecnológico e recebe a denominação de ciberbullying. Assim, por meio de *e-mail*, rede social, vídeo, imagens, SMS, *WhatsApp*, blog ou site em que alguém é ridicularizado, insultado, ofendido, difamado ou intimidado, estará sendo vítima de um *ciberbullying*. Esse fenômeno ofensivo cresceu juntamente com as redes sociais nesse terceiro milênio e, semelhante ao *bullying* comum, possui três personagens: a vítima, o agressor e o espectador.

O agressor caracteriza-se por possuir uma índole eivada por sentimentos negativos, como a inveja, a covardia, a ira, o instinto violento e o desejo de subjugar o outro. Geralmente é proveniente de um ambiente familiar desestruturado, sem disciplina, sem afeto, com dificuldades de lidar com frustrações. Apresenta-se superior à suas vítimas, é intolerante e não respeita a diversidade. Comporta-se, em alguns casos, como um indivíduo antissocial, avesso ao diálogo ou propenso a más companhias, podendo esconder, no seu íntimo, alguma carência que o leva a chamar a atenção por meio da violência.

A vítima é geralmente uma pessoa tímida, retraída, mais introspectiva e que, em muitos casos, possui uma compleição física diferenciada no que se refere ao peso, altura. Pode ter problemas com o aprendizado ou ter um desempenho destacável no ambiente que frequenta (escola, trabalho). Em decorrência das agressões ou ofensas e da dificuldade em reagir, as vítimas tendem a ficar mais submissas, inseguras e com a estima baixa, permitindo que o agressor continue com as investidas. Consequentemente, o agredido passa a cultivar o medo, a angústia e, na maioria dos casos, a depressão.

Além da vítima típica, existem ainda, duas espécies de vítimas: a provocadora e a agressora. A primeira, "[...] possui um gênio ruim, tenta brigar ou responder quando é atacada ou insultada, mas geralmente, de maneira ineficaz; pode ser imperativa, inquieta, dispersiva e ofensora" (MELO 2011, p. 29). A vítima provocadora dá causa às agressões, atraindo como

ímã o ofensor e, depois, não consegue responder eficazmente, nem se esquivar das *host*ilidades. Falta-lhe inteligência emocional.

Já a vítima agressora faz parte do chamado "efeito cascata", ou seja, ela já foi alvo de violência, de intimidação e, para extravasar o sofrimento, transfere as agressões para indivíduos mais fracos e vulneráveis. É uma forma de propagação do *bullying* convencional ou virtual gerando o crescimento do número de vítimas.

E, por fim, outro personagem importante na trama do *ciberbullying*, é o público (ou telespectadores). Quanto maior a quantidade de pessoas que têm acesso à ofensa (pelas redes sociais, por exemplo), maior é o dano. Muitos indivíduos veem as postagens que afetam o outro, mas ficam inertes, não se posicionam com medo de também sofrerem retaliações ou, em alguns casos, por serem insensíveis à situação. Por outro lado, há aqueles que curtem ou passam as ofensas adiante, podendo, inclusive, se forem identificados, responderem como coautores virtuais.

No Estado de São Paulo, ressalta Koguchi (2015, p.45, v.1):

> [...] 174 ações foram registradas entre 2010 e 2013, sendo que algumas exigiam até R$ 15 mil por danos morais. Além disso, o sindicato dos Estabelecimentos de Ensino do Estado de São Paulo tem orientado as escolas a fazerem seguro de responsabilidade civil para possíveis indenizações em caso de *bullying*.

As Instituições de ensino devem posicionar-se com providências quando o *ciberbullying* ocorrer em suas dependências, pois, do contrário, podem ser corresponsabilizadas no âmbito civil em razão da omissão. Caso o agressor seja menor, os pais ou responsáveis podem também responder pelo dano moral.

No entanto, as ações agressivas praticadas na Internet são consideradas por especialistas como mais nocivas, em razão de algumas características importantes, tais como: podem ser realizadas a qualquer horário, por múltiplos meios e podem chegar ao conhecimento de um número vasto de pessoas, além do que há uma dificuldade considerável em descobrir o verdadeiro agressor em razão da facilidade de anonimato no plano virtual.

Casado (*online*)[34], citando a contribuição do pesquisador Lélio Calhau, salienta que há uma espécie de violência virtual resultante da fusão do *bullying* convencional com o *ciberbullying* denominada de Bofetada Feliz ou *Happy Slapping*, ou seja:

> Prática cruel de *bullying* (real) que se mistura ao *cyberbullying* (virtual). No geral, os agressores atacam uma vítima com bofetadas sendo que um comparsa fica a uma

[34] <http://www.viajus.com.br/viajus.php?pagina=artigos&id=4231&idAreaSel=20&seeArt=yes>.

> pequena distância filmando as agressões com câmera de vídeo de um telefone celular. O vídeo com as agressões são imediatamente postados em redes sociais (ou enviados para telefones celulares) e visualizados por centenas ou milhares de pessoas em pouco tempo, infelizmente, tem se tornado comum no Brasil também.

É mais um tipo abominável de violência que acaba sendo veiculada em forma de vídeo, podendo ser visualizado por milhares de pessoas, especialmente no site do *YouTube*.

Apesar do crescente número de casos do *bullying* cibernético, há também um aparato legal e um judiciário atentos às transformações que ocorrem em razão do uso das tecnologias digitais e dos desvios de conduta que culminam em atos ilícitos.

A Constituição Federal de 1988 dispõe, em alguns incisos do art. 5º, sobre a proteção e salvaguarda de alguns direitos fundamentais, dentre eles, a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. Há a garantia constitucional da liberdade de expressão e de informação, desde que tal direito não seja utilizado de modo exacerbado ferindo outros direitos alheios. Desse modo, divulgar, na Internet, a montagem de uma foto insinuando falsamente que a pessoa é garota de programa não é o exercício legal da liberdade de expressão, nem tampouco de informação, mas uma ofensa à honra, a imagem e à dignidade de outrem.

Além do texto constitucional, há dispositivos legais presentes no Código Penal-CP que tutelam a honra, o decoro, a imagem, a intimidade ou a privacidade das pessoas. A calúnia (imputação falsa de crime) e a difamação, por exemplo, maculam a chamada honra objetiva da vítima (ou seja, sua reputação perante os outros). A injúria ofende a honra subjetiva (aquilo que o indivíduo pensa de si mesmo). Além de ofender a honra, em alguns casos, o *ciberbullying* pode atingir outros bens jurídicos, tais como a paz de espírito, conforme delito de ameaça, descrito no artigo 147 do CP (CASADO, 2015)[35].

Assim, muitos dos delitos tipificados na legislação penal podem ser realizados por meio das tecnologias eletrônicas. Segundo o STJ, "até 2008 foram mais de 17 mil sentenças coibindo diversas práticas criminosas tais como crime de estelionato, injúria, calúnia, difamação, furtos, extorsão, ameaças, fraudes com cartão de crédito, dentre outros".

O *Cyberbullying* é uma violação ao princípio da dignidade da pessoa humana e ao direito à imagem, pois promove atentados à honra e à imagem das pessoas nas redes virtuais. Os *bullies*, ou seja, os sujeitos ativos da prática, se sentem acobertados pelo anonimato da web e possuem a sensação de serem imbatíveis e impuníveis. O *bullying*, em si, já é um fato

[35] http://www.viajus.com.br/viajus.php?pagina=artigos&id=4231&idAreaSel=20&seeArt=yes

grave e que requer atenção, e esse, praticado no meio virtual, traz dificuldades ainda mais sérias por conta da questão da impunidade.

Uma das grandes ameaças no âmbito do *Cyberbullyng* são os chamados *trolls*, indivíduos que se alimentam do sadismo e das frustrações alheias. Apesar de fazerem parte de uma minoria de internautas, eles são altamente perigosos. Pois, além de humilhar, denegrir e ameaçar vítimas vulneráveis, induzem muitas delas ao suicídio. Há muitas indagações a respeito de por que tais indivíduos, com desvio de personalidade deste tipo, têm satisfação em perseguir e aterrorizar pessoas. Gabriela Loureiro (2015, p. 38) ao visitar um site de entretenimento dos *trolls* encontrou o seguinte depoimento do usuário denominado *DelusionalFak*: "Eu me sinto superior. Sei que soa idiota, mas manipular as pessoas para deixá-las furiosas traz alegria ao meu coração, é uma sensação muito boa, parecida com como os serial *killers* se satisfazem matando pessoas: você não os entende até se tornar um deles".

O testemunho acima relaciona-se perfeitamente com a "tétrade obscura" que, segundo pesquisas realizadas pela Universidade de Manitoba, no Canadá, corresponde a quatro desvios ou transtornos de personalidade, quais sejam: psicopatia (falta de remorso e empatia); sadismo (sentir prazer com o sofrimento dos outros); narcisismo (egoísmo e auto-obsessão) e maquiavelismo (tendência a manipular os outros) (LOUREIRO, 2015, p. 39).

O ato de *trollar* pode se dar por meio de uma simples piada ou, até por uma agressão mais violenta. Muitas pessoas não possuem a consciência de que tais atitudes praticadas no âmbito virtual, podem trazer consequências graves na esfera do real. Uma dessas "brincadeiras" sadistas e maldosas levou um garoto à morte em 2010. Tyler Clementi se jogou de uma ponte ao descobrir que virou piada na Internet após seu colega de quarto da Universidade de Rutgers, Dharun Ravi, filmá-lo beijando outro homem e compartilhar o vídeo na rede social do Twitter. Outro caso semelhante, referente à exposição pessoal na rede pública, acabou em tragédia: uma estudante brasileira de 17 anos, do Piauí, chamada Júlia Rebeca, teve seu vídeo íntimo compartilhado no *WhatsApp* e, logo depois, declarou no *Twitter* que iria se matar. Na mesma semana do caso, outra garota gaúcha de 16 anos, Giana Laura, também se suicidou por ter fotos de seus seios expostas nas redes sociais. Outro fato caracterizado por assédio psicológico, perseguição e ameaças recorrentes de um *troll* chamado Lori Drew, de 40 anos, resultou na morte de Megan Meier. Lori criou um perfil falso de um garoto chamado Josh e começou a desestabilizar Megan, induzindo-a, ao final, a cometer suicídio. Disse para a garota: "o mundo ficaria melhor se você se matasse", e, no mesmo dia, Megan se enforcou. (LOUREIRO, 2015, p. 43). Além de instigarem pessoas ao

suicídio, alguns *trolls* também enviam ofensas seguidas de ameaças de estupro e homicídio com a finalidade de aterrorizá-las.

Especialistas recomendam que as vítimas não alimentem os vilões virtuais, de forma a não dar munição para que eles consigam atingir seus objetivos. Elas não devem prosseguir com o diálogo nem retribuir as ofensas. Caso o sujeito passivo seja uma criança ou adolescente, deve-se comunicar o fato aos pais ou responsáveis.

Um outro exemplo, das consequências trágicas que o *Cyberbullying* ou o *bullying* em si pode trazer, é o caso ocorrido em abril de 2011, no Rio de Janeiro, na Escola Municipal Tasso da Silveira (G1, 2015)[36]. Wellington Menezes de Oliveira, de 23 anos, invadiu a escola localizada no bairro de Realengo, e disparou seus revólveres contra os alunos que se encontravam nas salas do local; 12 adolescentes de 13 a 16 anos morreram. Após o crime, o agente foi cercado pela polícia e cometeu suicídio. Pessoas próximas a Wellington e a carta deixada por ele atestaram que o rapaz sofria com o *bullying* durante toda a sua adolescência. A partir desse caso, pode-se ver o forte sentimento de mágoa que algumas vítimas carregam, podendo manifestar um desejo de vingança, não apenas contra o agressor, mas contra a sociedade (inclusive inocentes) e transformando-se de vítima em vilão.

Haja vista essa preocupante situação promovida pelo *cyberbullying*, a sociedade, unida, necessita conscientizar as pessoas, desde sua formação psíquica, por intermédio das instituições escolares e familiares, pregando valores humanos que se encontram subestimados hodiernamente. Além disso, o legislador tem a obrigação legal de fornecer à população uma proteção. Diante disso, surgiram alguns projetos jurídicos e sociais objetivando o combate aos graves problemas que geram a prática do *cyberbullying*.

> O que tem que ser feito é um trabalho educacional nas escolas, ensinando os alunos a terem respeito uns pelos outros. A entender que ninguém tem o direito de ofender o outro quanto mais publicamente como se fosse algo natural e normal. O que tem que ser feito é um trabalho de educação doméstica, ensinar a respeitar o homem, e os tribunais entenderem que dois mil reais não cobrem nem tratamento psicológico que a vítima é submetida a fazer após a agressão. O que tem que ser trabalhado é o respeito e a dignidade ao ser humano. Tratar o homem com respeito e dignidade (ARNOUD, 2014).[37]

O Projeto de Lei registrado no dia 24/03/2014 na Câmara Municipal de Manaus (CMM) defende a promoção de uma campanha formal de conscientização que seja realmente efetiva no combate ao *Cyberbullying*. A autora do projeto é a Professora Therezinha Ruiz

[36] http://g1.globo.com/leiaaintegradacartadoatiradorqueinvadiuescolano-RJ
[37] http://jus.com.br/artigos/32619/cyberbullying-e-responsabilidade-civil-do-provedor-de-Internet-na-lei-do-marco-civil

(DEM), presidente da Comissão de Educação da CMM e vereadora. Ela acredita que o *Cyberbullying* é uma terminologia de uso recente nas instituições de ensino. O fato se inicia principalmente nas redes sociais e, acaba terminando por atingir/prejudicar a vida e o rendimento do alunado. Para ela, a proposta tem a finalidade de alertar o corpo social sobre os danos decorrentes de tal prática e as penalidades para quem insiste em realizá-la (MANAUS, 2014)[38].

4.5.6 O Cyberterrorismo

O *ciberterrorismo* diz respeito aos ataques terroristas realizados por intermédio da Internet, promovendo violação de informação de sistemas e equipamentos do governo, visando danificá-los por questões de cunho político ou religioso.

Não há um conceito uníssono acerca do terrorismo, entretanto essa prática reúne elementos comuns que nos possibilitam construir uma melhor compreensão sobre o termo.

A palavra "terrorismo" deriva do latim terror, que significa medo ou horror. Originalmente, o termo "terrorismo" descrevia a violência exercida pelo Estado contra cidadãos durante a Revolução Francesa. Atualmente, o termo "terrorismo" é comumente utilizado para designar um fenômeno, em geral de natureza política, mas não só isso. Visa, também, obter vantagens de naturezas diversas através do uso de violência e do medo. A vitimologia acerca do terrorismo afirma que, em geral, os agentes do terrorismo utilizam-se de uma estratégia diferenciada de vítimas: a) A **vítima tática**, é a vítima direta, o morto, o esfaqueado, o assassinado, o mutilado, o seqüestrado, aquele que sofre na própria pessoa a violência do atentado; b) A **vítima estratégica,** são todos aqueles que sobrevivem ao atentado, mas que se encontram de alguma maneira dentro do grupo de risco dos vitimados e que, por medo, cedem a vantagens almejadas pelos agentes (WITCKER, 2005)[39].

O Terrorismo se tornou um fenômeno transnacional na década de 1960 com a expansão da aviação comercial, a disponibilidade da transmissão televisiva de notícias, e uma ideia extremista em comum, mas se universalizou com o incremento das mídias digitais e o advento da Internet.

A segurança de um país, atualmente, está altamente relacionada a sistemas de comunicações e *softwares* de computador, e isso constitui uma verdadeira guerra na qual os

[38] http://www.cmm.am.gov.br/camara-aprova-tramitacao-de-projeto-que-preve-campanha-de-combate-ao-cyberbullying/
[39] http://www.cepchile.cl/dms/ lang_1/doc_ 3551.html

alvos são atingidos por meio da rede mundial de computadores. E os ataques que são realizados ameaçam a soberania nacional, a autonomia dos Estados e, até mesmo, geram riscos à segurança do país e às estruturas internas políticas, econômicas e a outros âmbitos. Os terroristas se aproveitam do poder de perpetuação da Internet para disseminar o terrorismo. Alguns grupos espalham seus ideais terroristas em sites para arregimentar membros e desenvolver cada vez mais ataques.

Um episódio com características similares à definição de tal crime ocorreu no começo de 2015, quando a página do *Twitter* do Comando Central Americano foi invadida por um grupo muçulmano ultrarradical influente. Apesar das poucas consequências, o ataque expôs a fragilidade em vista do instrumento digital do Exército mais poderoso do mundo, o dos EUA. O presidente Obama pronunciou-se sobre o caso revelando que pretende criar medidas e uma legislação de *cibersegurança* para evitar que episódios semelhantes continuem acontecendo. O líder norte-americano solicitou, ainda, a participação dos países ocidentais nesta missão. Apesar da dificuldade para impedir este tipo complexo de crime, praticado por meio de uma ferramenta veemente e poderosa, há como tentar evitar, ou pelo menos reduzir, tais investidas: basta investigar, estudar e avaliar formas que conciliem a liberdade digital com a repressão a crimes também neste espaço (G1, 2015)[40].

São utilizadas técnicas específicas e recursos informáticos para invadir computadores, danificar sistemas e roubar dados, aproveitando-se de vulnerabilidades nos *softwares* de computadores. Geralmente são utilizados ataques físicos, uso de energia eletromagnética e/ou códigos maliciosos para desestruturar os computadores e seus processamentos ou deteriorar dados. A característica inerente ao ataque terrorista é a motivação específica do agente que, ao realizar o crime, é movido por fundamentos ideológicos, econômicos ou políticos. Outro exemplo de tal crime aconteceu na Estônia, em 2007, quando houve ataques de *ciberterroristas* que invadiram sites do governo causando danos a serviços no país (DIAS FILHO, 2009).

4.5.7 Fraudes eletrônicas

A Internet tornou-se meio de realização de diversas tarefas na vida cotidiana das pessoas. No campo profissional, ela adquiriu tamanha importância a ponto de existir uma grande dependência de serviços nas corporações mundiais e o fato da possibilidade de este

[40] http://g1.globo.com/mundo/noticia/2015/01/twitter-militar-dos-eua-publica-mensagens-de-cibercalifado.html

sistema falhar pode causar grandes prejuízos. O desenvolvimento de tal tecnologia facilitou a vida das pessoas e proporcionou grandes avanços, mas também fez com que possibilitasse o surgimento das fraudes, perpetradas no meio virtual. Elas são artifícios para alcançar um fim ilícito, obter ganhos pessoais através da ingenuidade de outras pessoas. Um bom exemplo de tal prática é o estelionato, previsto no artigo 171 do Código Penal.

Sobre o art. 171 do Código Penal, Mirabete (2003, p. 1350) comenta:

> A conduta do estelionato consiste no emprego de meio fraudulento para conseguir vantagem econômica ilícita. A fraude pode consistir em artifício, que é a utilização de um aparato que modifica, aparentemente, o aspecto material da coisa ou da situação etc.; em ardil, que é a conversa enganosa, em astúcia, ou mesmo em simples mentira, ou qualquer outro meio de iludir a vítima.

As fraudes eletrônicas não são verdadeiramente novos tipos de fraude, são as mesmas fraudes já cometidas no meio físico que agora estão sendo realizadas por intermédio do meio eletrônico. Os tipos de fraudes são executados com uma lógica similar, entretanto com algumas particularidades. Um dos tipos mais comuns no ambiente virtual é o ocorrido no comércio eletrônico (*e-commerce*). Alguns sites falsos se aproveitam do crescimento das vendas pela Internet, por conta da atratividade, comodidade e facilidade na realização de compras para enganar clientes. Muitos pagam o valor e não recebem sua mercadoria. Outros, os fraudadores, furtam as informações dos cartões de crédito das vítimas e realizam compras em seu nome

.

> Estatísticas divulgadas pelo CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil) mostram que os golpes que utilizam páginas falsas de bancos e sites de comércio eletrônico tiveram aumento de 89% nas notificações recebidas pelo órgão, em relação ao primeiro trimestre de 2012, número cinco vezes maior que no primeiro trimestre de 2011. São justamente esses números, somados ao comportamento dos usuários, que atraem os criminosos para esta modalidade de crime (CASSANTI, 2014, p. 19).

São características comuns neste tipo de fraude: a) O registro de domínios no Brasil e no exterior em nome de pessoas que perdem seu cartão de crédito ou documento, ou os que, os tiveram clonados. As supostas empresas de comércio virtual, que deveriam ser registradas em nome de pessoas jurídicas estão registradas em nome de pessoas físicas. b) Alguns sites também forjam as qualificações positivas (demonstrando satisfação pela compra e pelo tratamento do vendedor) de usuários para inspirar confiança e dar credibilidade ao site. c) Geralmente o site fraudulento abaixa consideravelmente os preços dos produtos para atrair o

consumidor. d) A "política de privacidade" e os Termos de Uso de tais sites são reduzidos, o que mostra a falta de proteção, já que tais políticas são referentes à prestação de informações às autoridades públicas e a própria relação de confiança com o consumidor. e) As formas de contato com a empresa são mínimas, oferecendo, muitas vezes, somente o *e-mail*, sendo este, falso. A empresa geralmente não tem endereço físico e reconhecimento no mercado.

Outra modalidade de fraude bastante frequente é realizada por meio de sites de falsos empréstimos. Estes sites anunciam dinheiro fácil e de forma rápida, sem a comprovação dos documentos, renda e avaliação do perfil do cliente. Tais sites oferecem dados de instituição de empréstimo falsos ou incompletos e não possuem o cadastro nacional de pessoa jurídica (CNPJ). Para enganar o contratante do empréstimo, o site exige que este faça um depósito prévio, como garantia para contratação. Só que o empréstimo não se concretiza, e o valor depositado não é devolvido pelos criminosos. Consiste na já mencionada engenharia social, em que os criminosos manipulam as vítimas para que essas executem as ações desejadas por eles, obtendo assim, ganhos pessoais. Os criminosos burlam o contratante do suposto empréstimo, alegando que precisa de mais uma contraprestação para garantia. Algumas vezes, até simulam o depósito por meio de um envelope vazio. O criminoso orienta a vítima que acesse o extrato bancário e confirme o depósito efetuado, o que efetivamente ocorre. Entretanto o referido depósito é feito em cheque a compensar e, na data aprazada para liberação, ocorre o estorno do valor bloqueado, tendo em vista a devolução do cheque por insuficiência de fundos.

É corriqueira também a ocorrência de fraudes eletrônicas no sistema bancário, por intermédio de cartões de crédito, plataformas de acesso aos dados bancários pela Internet (*home banking),* entre outros. Os criminosos obtêm vantagens financeiras a partir dos dados de outras pessoas. Sacam quantias em caixa eletrônico, realizam transferências, fazem compras virtuais com os dados roubados e clonados, muitas vezes, por meio do envio de *e-mail*s com cavalo de Troia ou *phishing scams*. (Verificar apêndice G, tabela de nº 8, página 100, sobre as principais ameaças virtuais).

Além dos Cibercrimes abordados acima, há muitas outras condutas ilícitas praticadas com o auxílio da ferramenta informática.

4.6 OUTRAS CONDUTAS ILÍCITAS TÍPICAS NO CIBERESPAÇO

Nesta esfera virtual infinda, há também, outras condutas ilícitas típicas do ciberespaço, como por exemplo: danos afetando dados ou programas informáticos,

danificação de informações e/ou programas de computadores, deterioração ou supressão de dados ou de programas informáticos.

Discorremos sobre algumas delas. O parâmetro para a escolha foi o grande número de ocorrências de certos tipos de crimes. Eis os mais comuns:

a) Pichação, que consoante foi visto, significa colocar, de forma indevida, textos ou figuras em sites de terceiros sem a devida autorização. Sobre a referida conduta, Nogueira (2008, p. 62)[41] elucida os objetivos principais dos pichadores virtuais:

> Estes adoram violar algum site, a maioria do poder público, como do FBI, Supremo Tribunal Federal, INSS e lá deixar sua marca, às vezes acontece algum tipo de protesto político ou religioso com esse tipo de invasão, ou podemos chamar de 'manifesto', normalmente não causam danos.

b) Sabotagem informática: significa a entrada, alteração, apagamento ou supressão de dados de programas no intuito de estorvar o funcionamento de um sistema informático ou um sistema de telecomunicações. Pode-se exemplificar como aquela interrupção danosa do sistema central de processamento. Para que se configure o delito de sabotagem, é necessário ocorrência da inviabilidade de dados e/ou o uso do computador para a prática de atos ilícitos.

c) Acesso indevido/ ilegal/ou não autorizado: é o acesso não autorizado/ilegal a um sistema informático ou rede informática pela violação das regras de segurança; concerne especificamente na conduta daquele que ilegalmente penetra em um sistema informático ou telemático protegido por medidas de segurança ou, ainda, ali se mantenha, mesmo contra a vontade expressa ou tácita de quem tem o direito de excluí-lo.

Deve-se ressaltar que a conduta de acesso indevido se torna ilícita quando há a utilização de um sistema informático sem prévia autorização e:

* Provocando o risco de causar prejuízo à pessoa a quem por direito pertence o sistema ou de provocar dano ao sistema ou funcionamento dele;

* Pausando prejuízo à pessoa que tenha autorização de utilizar o sistema ou de provocar danos ao sistema ou o seu funcionamento;

d) Interceptação não autorizada: é a interceptação, não autorizada e por meios técnicos, de comunicação, na origem de ou no seio de um sistema ou rede informática.

e) Utilização não autorizada de um programa informático protegido: é o uso sem autorização de um programa informático protegido pela lei e reproduzido sem autorização, na intenção, seja de obter para si ou para outrem qualquer vantagem, seja de causar prejuízos ao

[41] http://jornalggn.com.br/noticia/assange-snowden-e-ellsberg-por-walnice-nogueira-galvao

titular do direito. Tal conduta também se encontra devidamente tipificada pelo legislador penal pátrio, no art. 12 da Lei nº 9.609, de 19 de fevereiro de 1998, vez que viola o direito de autor de programa de computador.

f) Divulgação de informações sem autorização de autoridade competente ou de pessoa interessada, quando necessária: consiste na conduta daquele que divulga, sem justa causa, informações contidas nos sistemas de informações ou bancos de dados dos computadores.

4.6.1 Denúncias dos cibercrimes

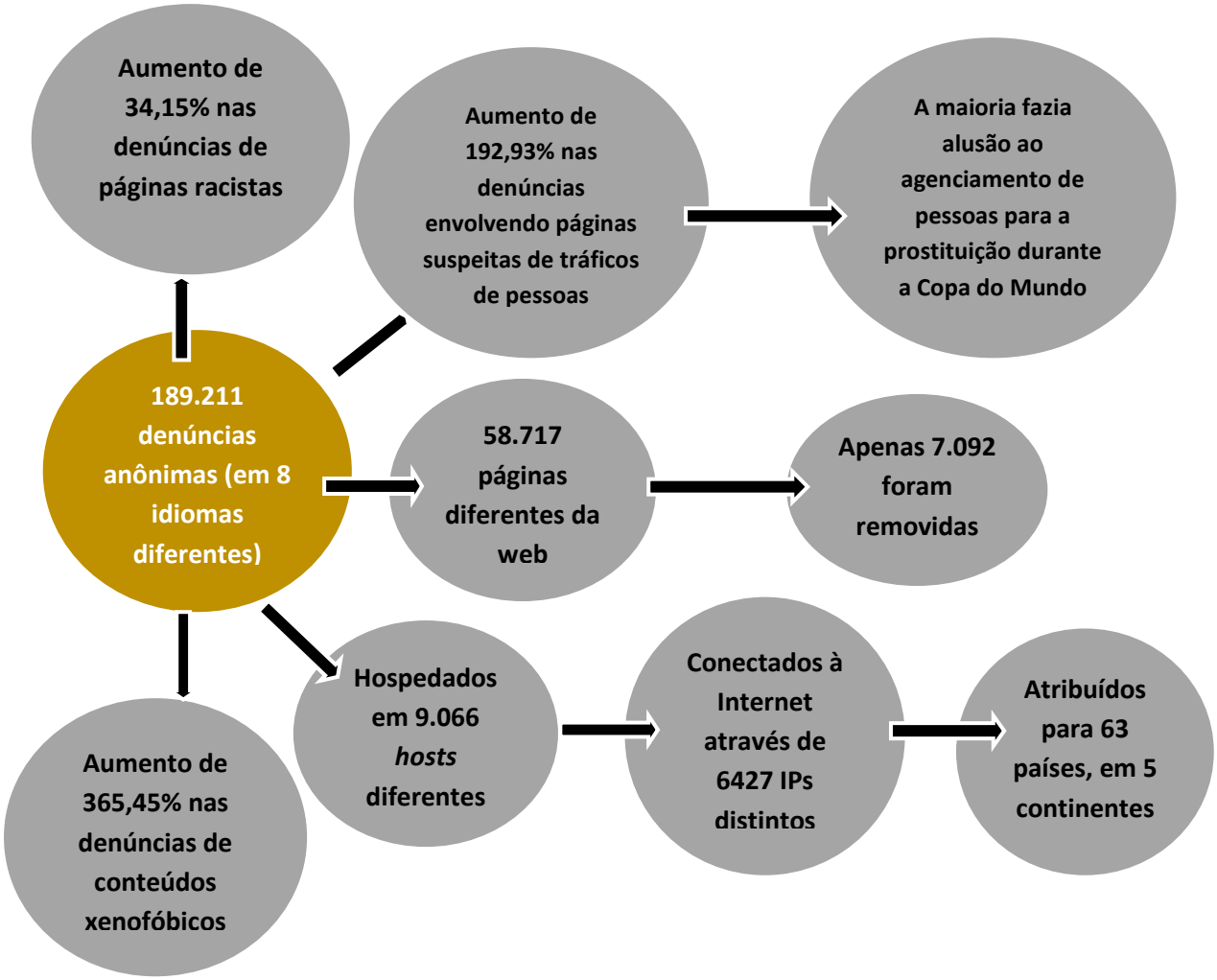
No ano de 2014, a Central Nacional de Denúncias de Crimes Cibernéticos (CND) recebeu milhares de denúncias anônimas de crimes na Internet – cerca de 8,29% a mais, em relação ao ano anterior.

A razão para tal crescimento reside no fato de estas páginas terem sido criadas no período eleitoral, especialmente no dia seguinte ao resultado final da eleição presidencial, quando houve o recorde histórico de denúncias anônimas desde 2006 – de 10.376 contra 6.909 *links* diferentes nas redes sociais.

Segundo Thiago Tavares Nunes de Oliveira, presidente da SaferNet Brasil (CHILDHOOD)[42], "esse grande número de denúncias comprovam que a sociedade brasileira está vigilante e não irá tolerar manifestações de extremismo e preconceito contra as minorias nas redes sociais". Segue um fluxograma relatando esses dados

[42] http://www.childhood.org.br/denuncias-anonimas-de-crimes-na-internet-passam-de-180-mil-em-2014

Figura 3 - Denúncias de crimes na Internet



Fonte: CHILDHOOD.[43] (Adaptada pela autora, 2015).

A SaferNet Brasil esclarece que, dentre os 1225 pedidos de ajuda e orientação psicológica atendidos por ela, em 2014, 222 foram casos de *sexting*, que consiste na prática de enviar fotos e vídeos sexualmente explícitos pelo celular, ocasionando o vazamento desse conteúdo.

Os motivos pelos quais se enviam estas fotos e vídeos são muitos: podendo ser para divertir/descontrair os amigos ou o parceiro; ou após o término do namoro, quando muitos rapazes espalham fotos de ex-namorada nua, como forma de vingança. As consequências são sérias, pois, depois de enviar a imagem, que facilmente se propaga, afetando a reputação da pessoa, a vítima pode perder o controle e até mesmo cometer suicídio.

[43] http://www.childhood.org.br/

Figura 4 - O perfil da vítima de *sexting*

O perfil da vítima de *sexting*			
Sexo	81% do sexo feminino	16% do sexo masculino	3% não identificados
Idade	53% até 25 anos	39% acima de 25 anos	8% não forneceram a idade

Fonte: CHILDHOOD[44] (Adaptada pela autora, 2015).

Outra fonte de denúncia é o ciberbullying. A SaferNet afirma terem sido atendidos 177 casos em 2014. A maioria desses casos envolve situações de humilhação e intimidação através das redes sociais e dispositivos móveis.

A pornografia infantil e pedofilia, apesar de continuarem a liderar o ranking no Brasil (nove anos consecutivo), em 2014, teve uma redução significativa (8,82%) no número de páginas novas denunciadas com relação aos crimes desta natureza.

4.7 A DEEP WEB: o submundo do cibercrime

No decorrer desta pesquisa, vimos que a Internet é integrada por inúmeros computadores que englobam diversos conteúdos, havendo uma conexão entre eles por meio de uma grande rede de cabos espalhados pelo mundo virtual. Por intermédio dessa rede, pode-se chegar a outro computador por meio da identificação da máquina. O protocolo TCP/IP, já descrito anteriormente, representa um endereço, um número único de cada computador (ou roteador), semelhante a um RG ou CEP, através do qual se localiza a máquina em que se veiculou a mensagem.

O avanço e a profusão de conteúdos, a necessidade da utilização da Web para efetuar pesquisas, fizeram com que surgisse a necessidade de se criarem ferramentas que fossem utilizadas para ordenar, orientar a navegação. Assim apareceram os indexadores ou buscadores que facilitaram a execução de pesquisas, tais como Veronica, JumpStation, Aliweb, Yahoo e o gigante Google.

O internauta comum que acessa o Google, por exemplo, acreditando que o referido buscador abarca tão somente a maioria dos dados e informações do planeta (em geral o usuário acredita que o Google é apenas um armazenador de dados), desconhece a amplitude do ciberespaço e suas interconexões. O que costuma ser acessado pelos usuários comuns,

[44] http://www.childhood.org.br/

denominado de *Surface Web* (superfície da Web) corresponde a uma parcela mínima do universo *on-line*.

Ao fazer uma analogia entre a Internet e um *iceberg*, o especialista em cibersegurança Paulo Pagliusi, esclarece que a *Surface Web* é a parcela explícita e visível a todos, a Internet de superfície correspondendo a 4% da Web. No entanto, há uma outra fração que alberga 96% de conteúdo protegido, arquivos desprovidos de metadados e outras informações sigilosas e de difícil acesso que representam a grande parte submersa do *iceberg*, notadamente obscura, densa, batizada de Internet Profunda, Internet Invisível ou Oculta (também chamada de Deep Web, Deep Internet, Undernet) (PAGLIUSI, 2015)[45].

Na Internet convencional, há buscadores como o Google, Bing ou Ask.fm que são ferramentas comuns conhecidas pelos navegadores como Crawlers (motores de busca). Para não ser necessário memorizar o IP de todos os sites desejados, utilizam-se os servidores nominais (servidores de *Domain Name System*- DNS) que transformam os números estranhos em Urls. (exemplificando: www.terra.com.br). Desse modo, os buscadores como Google e Yahoo acessam os servidores de nomes, rastreando os conteúdos permitidos e, assim, o internauta tem acesso a eles. No entanto, os dados que não podem ser identificados com um DNS, nem pelos buscadores tradicionais, encontram-se na Deep Web, mas é necessário um outro meio para se chegar à Internet profunda.

4.7.1 O acesso

Na década de 90, a Marinha dos EUA, por intermédio dos seus matemáticos, criou um protocolo de navegação chamado de The Onion Router-Tor (em português, o Roteador Cebola) que visava a uma navegação mais protegida a serviço da inteligência do país. Tempos depois, o Tor transformou-se numa ONG (Organização não-governamental) com a nomenclatura Tor Project, "[...] com especialistas que trabalham para estimular cada vez mais a navegação confidencial. Para quem deseja circular pela Deep Web, o Tor tornou-se o navegador essencial" (SANTOS, 2015, p.9).

O objetivo do Tor é dificultar a identificação do IP onde o internauta se encontra. A princípio, a navegação seria anônima, mas ela não é criptografada, podendo ser rastreada no retorno. O TOR dificulta o rastreamento, entretanto, não garante a inviolabilidade dos dados nem a identidade da máquina porque não é criptografado. Mas esse instrumento não é a única

[45] https://cryptoid.com.br/destaques/a-Internet-profunda-segredos-riscos-e-ameacas/

forma de acesso às profundezas da Web, havendo opções como o Morphmix / Tarzan, Mixminion / Mixmaster, JAP, MUTE / AntsP2P, Haystack.

Um dos problemas em se rastrear, o que passa pela Deep Web, é justamente a estrutura da rede, em que as páginas são encriptadas e os métodos e as ferramentas comuns não são suficientes para realizar uma busca pela rede profunda.

> As páginas também não estão identificadas pelos servidores DNS, o que facilita seu acesso. Além de dificultar o rastreamento dos sites e dos endereços de IP(o protocolo de Internet que cada computador tem), isso facilita a mudança da página sempre que um criminoso é identificado. Outro fato que dificulta uma investigação é a questão legal, já que as constituições de diversos países garantem o sigilo das comunicações. Os processos de investigação virtual só podem ser levados adiante após uma medida judicial (KOGUCHI, 2015, p. 13).

O escopo maior da Deep Web é fazer com que os dados e as informações possam trafegar de modo anônimo, com mais proteção e sigilo (BORGES apud SANTOS, 2015, p.9). Desse modo, é necessário um tipo diferenciado de navegador que possibilite mais confidencialidade para quem navega.

4.7.2 A moeda eletrônica e alguns Cibercrimes cometidos na Deep Web

No ano de 2008, foi criada a Bitcoin (Moeda digital ou moeda virtual, criptomoeda) desenvolvida por Satochi Nakamoto (pseudônimo japonês, identidade real, até o momento não revelado). Uma criação revolucionária no mundo virtual, pois tal moeda pode ser transferida de um dispositivo eletrônico a outro, computadores, *smartphones*, sem a necessidade de instituições bancárias. A ausência de senhas ou cartões torna muito difícil a localização da origem do dinheiro virtual.

As transações feitas com Bitcoin são realizadas por meio da rede P2P *(peer-to-peer)*, "[...] Esse tipo de arquivo se assemelha a uma rede, cujo "nós" são os próprios usuários. Dessa maneira, cada internauta é, ao mesmo tempo, cliente (que recebe dados) e servidor (que os fornece)", (KOGUCHI, 2015, p. 13).

Assim, há dificuldade para identificar a origem e o destino da moeda, facilitando e deixando mais seguras as compras na Deep Web, incluindo também, as transações ilícitas decorrentes de crimes cibernéticos. Em que pese a criptomoeda ser amplamente utilizada no cerne da Internet profunda, ela não é proibida, pois muitas organizações empresariais utilizam tal moeda eletrônica para fins lícitos e há países que regulamentam sua emissão.

Há um mapa interativo (o BitLegal**)** expondo uma lista dos países que são ou não, amigáveis ao Bitcoin (Bitcoin friendly) (Henrik, 2014)[46].

De acordo com Thiago Tavares, a SaferNet já recebeu denúncias e identificou *links* de crimes na Deep Web.

A organização possui uma parceria com a Polícia Federal e 17 Ministérios Públicos, para quem encaminha todas as denúncias. Contudo, Tavares ressalta que é preciso entender melhor a Deep Web. "Ela foi criada, inclusive, para a defesa dos direitos humanos. Mas, como qualquer ferramenta, pode ser usada para o bem ou para o mal". Sobre os possíveis usos do espaço, ele aponta que ela é "usada também por jornalistas investigativos, militantes de direitos humanos, pessoas que precisam se comunicar sem o risco de serem monitoradas" (TAVARES apud SILVA, M.A.D., 2015).

Conforme elucida Goodman, há inúmeros Cibercrimes cometidos na Deep Web de que são exemplos:

Venda de Drogas- O mais famoso site dessa categoria era o *Silk Road*, descoberto pelo *Federal Bureau of Investigation* –FBI (tradução-Escritório Federal de Investigação) em 2013, mas há inúmeros outros que vendem desde remédios controlados, até cocaína, heroína e demais drogas, inclusive a chamada escopolamina,(" sopro do diabo") um tipo de substância em pó, que soprada na face da pessoa, é capaz de paralisá-la, deixando-a ainda consciente, mas sem livre arbítrio. E, caso seja ingerida, a escopolamina permite o controle total sobre a vítima, inclusive retirando-lhe, da memória, as lembranças do ocorrido.

Cartões e dados bancários- Há sites especializados na comercialização de cartões de débito e crédito, bem como venda de informações constantes nos cartões (Dumps) que possibilitam a confecção de um novo cartão com os referidos dados para serem utilizados nas lojas de modo presencial. O prejuízo é gigantesco, são mais de 11 bilhões de dólares em nível mundial, sendo que, quase a metade, 47%, é concentrada nos EUA.

Tráfico de pessoas e de órgãos- Nos EUA, são 32 bilhões de dólares por ano o lucro com o comércio de seres humanos (Informações do Departamento de Justiça). As vítimas são, em grande parte, crianças, imigrantes e pessoas de baixa renda. Uma criança traficada pode render 200 mil por ano, especialmente se for destinada à exploração sexual. No tocante às mulheres, aproximadamente meio milhão delas chega ao continente europeu por ano, incluindo brasileiras (15%) segundo a ONU.

[46] http://bestbitcoin.com.br/bitlegal-mapa-exibe-lista-de-paises-bitcoin-friendly/

Além de pessoas, na DW são vendidos órgãos humanos: rim, fígado, coração, pulmão, por valores que chegam ao patamar de US$200 mil. Os órgãos extraídos são de refugiados do conflito na Síria, prisioneiros chineses executados, mulheres indianas (coagidas pelos respectivos maridos) e, também, pessoas sequestradas e mortas.

Imagens de Estupro infantil ao vivo- Um relatório apresentado pela Agência de Polícia da União Europeia- Europol constata o crescimento de sites especializados na transmissão, ao vivo, de crianças sofrendo abusos. Muitas dessas organizações criminosas são asiáticas e oferecem, por cem dólares, o repugnante serviço, concedendo ao "cliente", a possibilidade de escolher o tipo de abuso.

Outros ramos ilegais- Na Internet subterrânea, há dinheiro falsificado, especialmente o dólar que passa por um processo de pseudoveracidade dando à cópia uma semelhança altíssima. Pagando o equivalente a 600 dólares, conseguem-se 2.500 dólares falsos. Encontram-se, também, produtos eletrônicos roubados em sites como, Tor Eletronics e Buttery Bootlegging. Existe também o furto de dados pessoais obtido pela invasão de PCs, em redes sociais, sites de compras, etc. Nos EUA, muitas pessoas compram tais informações para fraudar o imposto de renda e o sistema de saúde, causando prejuízos que ultrapassam bilhões de dólares.

Exemplos de alguns serviços ou objetos vendidos na Deep Web (Prints da Deep Web extraídos do blog Noite Sinistra-)

a) **Aluguel de escravo – Site 14yo *Male Skype Slave***

Na página abaixo, um adolescente de 14 anos oferta, pelo Skype, serviços de escravo salientando que "fará tudo o que o mestre ordenar".

Figura 5 - Site de aluguel de escravo

Fonte: <noitesinistra.b*logs*pot.com/2015/.../*links*-da-deep-web-abril-de-2015.htm> (2015).

b) Aluguel de um *Hacker* para qualquer finalidade

Figura 6-Site de aluguel de *Hacker*

Fonte: <noitesinistra.b*logs*pot.com/2015/.../*links*-da-deep-web-abril-de-2015.htm> (2015)

c) Vendas de passaporte falso

Figura 7- Site de venda de passaporte falso

Fonte: <noitesinistra.b*logs*pot.com/2015/.../*links*-da-deep-web-abril-de-2015.htm>(2015).

d) Vendas de livros raros-Bibliotheca Alexandrina

Figura 8-Site de venda de livros raros

Fonte: <noitesinistra.blogspot.com/2015/.../links-da-deep-web-abril-de-2015.htm> (2015).

e) Guia para canibalismo

Figura 9- Site de guia para canibalismo

Fonte: <noitesinistra.b*log*spot.com/2015/.../*link*s-da-deep-web-abril-de-2015.htm> (2015).

4.7.3 O lado bom da Deep Web

Foram abordados até agora, a face obscura da Deep Web, os crimes, a ausência de segurança e os vírus que dela se disseminam, entretanto existe uma face positiva em meio a tanta barbárie virtual.

Apesar dos conteúdos fortes encontrados, quase em sua totalidade, na DW, há também pessoas e organizações (Inteligência policial, Universidades, Ciberativistas) que lutam pela concretização da justiça, dos direitos humanos e de um mundo mais equilibrado e justo. O estudioso Kelton Costa do Instituto de Computação da Universidade de Campinas esclarece que a Internet profunda não oferece realmente qualquer segurança para os internautas, mas é justamente nesta fração da Web que jornalistas, investigadores e ativistas lutam de maneira sigilosa para realizar alguma missão importante. Existem grupos que utilizam o referido espaço virtual para identificar práticas ilícitas. A título de exemplo, ele esclarece: “Wikileaks e o Anonymous fizeram a identificação de uma grande quantidade de pedófilos, além de divulgar documentos governamentais importantes de pessoas que estão no poder e que atuam fora da lei” (COSTA apud ALVES, 2015, p.26).

Nos países em que há censura e o controle da Internet convencional (como na China, Irã e Coreia do Norte), muitos jornalistas e ativistas utilizam a DW, por conta do sigilo e proteção, fazendo fóruns, debatendo, lutando pela liberdade de expressão e outros direitos. As manifestações ocorridas entre 2010 e 2012 no norte da África e no Oriente Médio intitulada de Primavera Árabe foram fruto da disseminação de ideias pelas redes sociais, mas que passaram pela Internet profunda.

O anonimato e a criptografia, consoante visto até agora, foram utilizados para ocultar conteúdos pesados e proibidos (fotos, imagens e vídeos de mortes, assassinatos, canibalismo, pedofilia, pornografia). Excepcionalmente, o anonimato não é utilizado apenas para fazer o mal, usando essa válvula de escape, pessoas se expressam, falam sobre variados assuntos ou conseguem se proteger para exercer uma finalidade lícita. Outra característica da DW é a gratuidade, incluindo pesquisas importantes, artigos científicos, ensaios, etc. Há *download*s disponíveis de filmes e músicas de várias épocas, livros raríssimos disponíveis gratuitamente ou à venda, bem como manuais, tutoriais e guias diversos.

4.7.4 Riscos do acesso à Deep Web

O acesso à Deep Web não é ilegal, mas as ações praticadas no âmago dessa camada ciberespacial podem gerar consequências qualificadas como negativas ou proibidas. Inicialmente, o acesso, conforme já foi demonstrado, é diverso da Internet comum, sendo necessário um navegador específico, como por exemplo, o Tor. Acessar a Internet profunda requer um conhecimento maior na seara computacional, além do domínio razoável da língua inglesa. É uma navegação bastante insegura, há uma variedade de sites desconhecidos, inúmeras páginas repletas de vírus, arquivos maliciosos e pseudo softwares. Os internautas de conhecimento mais restrito sobre informática não devem se aventurar, assim como crianças e adolescentes, pois é um lugar mais complexo e cheio de armadilhas.

4.8 A PERMISSIVIDADE NA REDE

Compartilha-se uma inquietude acerca da gravidade e amplitude de crimes cibernéticos e de certas peculiaridades do ciberespaço que dificultam a identificação e consequente punição do agente criminoso, além da grande extensão de redes e usuários. Já que não existe um eficaz controle sobre sites e redes, discute-se a necessidade de uma legislação efetiva e a aplicação concreta dessa para combater estes tipos de crimes. É

necessária a criação de iniciativas que possam realmente penalizar de forma eficaz os autores, para que a sensação de impunidade e anonimato seja exterminada. Porém essas iniciativas não podem se confundir com censura no vértice da palavra, prática ditatorial e ilegítima.

O risco social dos ciberespaços, em razão da falta de controle público, da crescente dependência tecnológica e da ausência de instrumentos eficazes de proteção e segurança dessas estruturas, tornou-se ainda mais evidente após o caso de espionagem ocorrido nos Estados Unidos (Caso Snowden) fazendo com que essa insegurança tecnológica leve ao inevitável questionamento: há privacidade e segurança nas novas tecnologias da informação?

A formação de um contexto global tecnológico uniformizado, propiciado pela sua constante evolução e ampla utilização da Internet fez com que as barreiras geográficas deixassem de ser empecilho para as ações de seus usuários, passando essas a serem condicionadas pelo tempo de acesso e disponibilidade dos recursos de informações. Associado a isso, com o desenvolvimento econômico e social propiciado pela evolução tecnológica, os Estados passaram a incentivar a criação de novas plataformas tecnológicas que permitem explorar e potencializar as informações e, consequentemente, permitir seu amplo acesso e democratização dos ciberespaços.

Como já foi discutido, com os ciberespaços surgem novas formas de comunicação virtual alterando os processos de interação social e com elas suas consequências. A crescente utilização da Internet constrói pontes praticamente permanentes entre seus usuários o que resulta em uma mudança de paradigmas sociais como, por exemplo, o surgimento de novos atores de intermediação e controle social. O sucesso das redes sociais e a adesão de novos processos de interação, somados a uma possível deficiência na formação tecnológica, geram um pseudo sentimento de confiança que faz com que seus usuários compartilhem dados pessoais, muitas vezes sem restrições, e com isso permitam o surgimento de riscos antes impensados.

A sociedade em rede e a construção dos ciberespaços são características importantes de uma economia em rede, ou seja, a democratização do acesso às informações possibilita uma crescente vantagem competitiva quanto à capacidade de exploração das informações, seja na área econômica ou nas demais atividades do mundo contemporâneo, demonstrando a força de influência que possuem as cadeias de valores das organizações dentro dos espaços virtuais competitivos. Nesse sentido, constatamos que a utilização dessas informações por diferentes atores sociais tanto pode gerar novas oportunidades como ameaças que, inevitavelmente, atingirão a política e estratégia do Estado.

Hoje a utilização da informação está diretamente relacionada à forma como ela é difundida ou apropriada. Nos ciberespaços, elas possuem um alcance global mesmo vindo de uma apropriação local, de um determinado território. Seja através dos espaços geográficos ou da geopolítica, é preciso compreender que o mundo digital se estrutura fisicamente em determinado local para depois produzir seus efeitos e impactos na sociedade virtual globalizada.

Com a desterritorialização, a defesa dos interesses e territórios dos Estados assume outra estruturação, mudança de postura e estratégia dos governantes para lidar com a interdependência dos espaços virtuais. Segundo dados estatísticos (AC, 2010; ISOC, 2010), os ciberespaços podem e devem ser "mapeados" para facilitar sua compreensão evitando assim possíveis problemas decorrentes da sua utilização não criteriosa. Essa análise também pode ser utilizada para efeitos militares na prática dos ciberataques destinados a impedir a utilização da infraestrutura de informação por um adversário, bem como para lançar as bases para o estudo de estratégias militares ou políticas numa perspectiva de alcançar o controle e o poder mundial.

Os Estados ainda precisam lidar com a dificuldade de delimitar os espaços físicos/geográficos das redes de comunicação para estabelecer jurisdição territorial, uma vez que os ambientes de informação possuem escala global sendo difícil estabelecer a forma de sanção e proteção a essas novas tecnologias. A interdependência da economia globalizada com os fluxos de informações estabelecidas através da Internet possibilita o surgimento de novas formas de dominação e controle, assim como crimes digitais, os Cibercrimes.

As mais novas modalidades de práticas criminais, os "Crimes Cibernéticos" ou "Cibercrimes" ocorrem com o uso indevido, nas mais variadas formas, da rede mundial de computadores, tais como: pedofilia, clonagem de cartões de crédito, plágio, calúnia, difamação, uso indevido da imagem, espionagem, entre outras, como já visto nesse estudo.

Uma das questões mais preocupantes quando se aborda o assunto é a não proteção jurídica, ou seja, o despreparo legislativo quanto a tal situação, já que a legislação não evoluiu de forma equitativa com o avanço e desenvolvimento da Internet e sua utilização pelos usuários.

A Internet é um espaço democrático. Seu uso é permitido a indivíduos de todas as faixas etárias, desde crianças a pessoas idosas, e, como já trabalhado, paralelo aos benefícios, facilita a criminalidade virtual por agentes com traquejo nessa área. Além disso, tais condutas, os Cibercrimes, se amparam na fragilidade legislativa sobre o assunto e em uma possível

impunidade, o que faz dessa ferramenta de comunicação interpessoal centro da globalização, uma “terra de ninguém”.

É necessária a criação de iniciativas que possam realmente penalizar de forma eficaz os autores, para que não haja a sensação de impunidade e anonimato. Porém essas iniciativas não podem se confundir com censura no vértice da palavra, prática ditatorial e ilegítima.

> Muitas questões difíceis, relativas à Internet, exigem um consenso internacional: por exemplo, como garantir a privacidade de inúmeros indivíduos e grupos que vivem no respeito da lei, sem impedir que a aplicação da lei e os responsáveis pela segurança exerçam a vigilância sobre os criminosos e os terroristas [...] (FOLEY, 2002, p. 8).

Afinal, se ocorresse censura de fato, estaria sendo prejudicado um dos principais benefícios do ambiente virtual: a formação de uma opinião pública mais autônoma e desprendida da manipulação da informação, o que geralmente ocorre nos regimes de exceção.

Deve-se trabalhar de forma a que se inviabilize qualquer tipo de censura. É necessário que haja averiguação do que realmente é crime cibernético e do que é a expressão de uma opinião. É imprescindível que seja respeitada a multiplicidade de opiniões com defesa de interesses diversos. Isso não descarta, em hipótese nenhuma, a intervenção do Estado com instrumentos normativos que protejam a sociedade por meio de regulamentações eficazes, sem que se resvale para uma censura velada.

Como já discutido, o dinamismo da web, sua "falta" de fronteiras físicas e o anonimato são características do espaço onde o esse tipo de crime ocorre. A identificação do agente, muitas vezes, é realizada por meio do rastreamento do número IP que consiste no endereço da rede do computador do usuário. Os provedores de acesso à Internet, no caso de crime, devem informar, por obrigação legal (conquista proveniente do Marco Civil), os dados cadastrais dos usuários para que a investigação se efetive. Os provedores devem guardar os registros de acesso dos usuários por, pelo menos, um ano. O problema, no entanto, está na identificação da singularidade do criminoso. Afinal, os dados identificam as máquinas através das quais foram cometidos os crimes. Em serviços públicos de acesso à Internet, como *lan houses*, por exemplo, a manipulação das máquinas é realizada por uma série de pessoas e geralmente não se tem controle da identificação de todas aquelas que utilizam o serviço e suas diversas finalidades.

Além disso, a necessária determinação dos locais de realização do crime e a definição de seus componentes principais, discutidos inicialmente, são dificultadas pela globalidade e amplitude da Internet. As informações publicadas na web são acessíveis em todo o mundo. A

Internet é de uma dimensão incalculável. Por conta disso, a delimitação da jurisdição (a competência responsável pela investigação) é uma questão que gera divergência na apuração dos Cibercrimes. O Código Penal Brasileiro considera aspectos geográficos para delimitar a localidade da execução delituosa, o que dificulta a definição da questão no espaço virtual. No Brasil, a aplicação da lei penal no espaço, considera o crime realizado no local da ação ou omissão, assim como onde se produziu o resultado (GRECO, 2014, p. 131). As complicações acontecem no caso do envolvimento de dois países. Um pode tipificar a conduta e o outro, não. Glenny cita um caso que ilustra tal dificuldade:

> Um policial na Colômbia, por exemplo, pode identificar que o endereço IP responsável por coordenar um ataque a um banco colombiano vem do Cazaquistão. Em seguida descobre que essa ação não é considerada crime naquele país, e por isso seus equivalentes cazaques em Astana não terão motivos para investigar o crime (GLENNY, 2011, p.15).

O supramencionado autor, ao investigar sobre a cibercriminalidade e, entrevistando um *carder* sueco (especialista em fraudar cartões), ouve deste que jamais utilizaria cartões de crédito ou de débito americanos, pois: "Isso me colocaria sob a jurisdição legal dos Estados Unidos, onde quer que eu estivesse. Por isso, uso apenas cartões europeus e canadenses, o que me deixa ao mesmo tempo feliz e seguro – eles nunca vão me apanhar" (GLENNY, 2011, p.15).

A definição da competência fica dificultada pela incerteza de onde os dados saíram, foram armazenados e o crime de fato aconteceu. A ausência de legislações específicas sobre tais delitos e a falta de cooperação entre nações revelam-se como sendo grandes obstáculos na luta contra a cibercriminalidade.

Há Estados que regulamentam os delitos, outros não. Assim, há algumas teorias que tratam da regulamentação da Internet. São elas:

- **Teorias anárquicas**

Anarquia é designada como ausência de poder público, os movimentos anarquistas defendiam o fim do poder estatal e do próprio Estado. E esse termo para denominar a teoria, quer dizer que essa é contrária a qualquer tipo de regulação no espaço virtual. Diz respeito à utilização de uma concepção antiga adaptada à realidade hodierna, na qual houve a evolução das tecnologias e o surgimento da "sociedade virtual".

> Sus adeptos no solamente impulsan un espíritu de "libre acción" en Internet, sino también la libre calumnia y el anonimato. Los más extremistas se oponen – inclusive – a la regulación de delitos típicos como el acoso sexual, la pedofilia, la pornografía de menores, entre otros delitos (MIGLIORISI, 2014, p.19).

Entretanto, diante do contexto atual, na civilização presente, com toda sua complexidade, é inviável e utópica a aplicação da descrita teoria no ambiente virtual.

- **Teorias de autorregulação privada**

Tal teoria sugere que, para evitar situações de Cibercrime, as empresas donas das criações interativas no ciberespaço, (como redes sociais - *Facebook, Twitter, Instagram*- e alguns sites - *Youtube, Hotmail, Yahoo, Wordpres*-), estabeleçam leis internas de funcionamento e utilização de tais veículos pelos usuários. Dessa forma, as próprias entidades responsáveis pelos portais irão avaliar e julgar possíveis delitos por meio de seus regulamentos internos.

- **Teoria da regulação governamental**

Determinada teoria acredita que a regulação do ciberespaço deve ser realizada por leis e regras impostas pelo Estado. Destarte, os delitos informáticos serão evitados pelo supervisionamento estatal, qual seja, solucionados pela intervenção governamental.

Os Estados Unidos e a Europa são exemplos favoráveis à atuação de tal teoria, pois tentam combater os delitos informáticos por meio da implementação de legislação nacional. O Brasil também segue essa linha, especialmente agora, com a vigência do Marco Civil.

Existe uma grave preocupação acerca do problema dos Cibercrimes que é a comprovada impunidade existente no ciberespaço. E, em busca do combate a tal situação, foram intensificadas formas de preenchimento das lacunas das leis. Uma delas é o Centro Europeu contra a Delinquência Informática (EC3). A promoção de convênios mundiais para o combate a esse tipo de crime é a melhor forma para uma efetiva solução.

Na visão de Migliorisi (2014, p. 22-23): "Por un lado, un exitoso Estado que regule, controle y persiga al delincuente en forma interna. Pero al no existir un convenio internacional regulatorio del ciberespacio – por lo menos de aplicación mundial -, quedarían impunes los delitos cometidos desde el exterior".

Procurando vencer barreiras investigatórias na luta contra a impunidade no ciberespaço, a citada Convenção sobre o Cibercrime, em Budapeste, organizada pelo Conselho da Europa, em 2001, pretende defender a necessidade de medidas técnicas para

proteger o sistema de informática. Busca-se, também, o respeito aos direitos humanos diante dessa nova sociedade informacional, além de proteger a sociedade contra a criminalidade no ciberespaço, através de uma cooperação internacional e uma legislação adequada aos seus limites.

> [...] a Internet não está mais isenta do que outros meios de comunicação, das leis razoáveis contra a linguagem ofensiva, a difamação, a fraude, a pornografia infantil e a pornografia em geral, assim como outras ofensas. O comportamento criminoso noutros contextos é igualmente um comportamento criminoso no espaço cibernético, e as autoridades civis têm o dever e o direito de fomentar estas leis (FOLEY, 2002, p. 7-8).

Há uma preocupação muito grande em salvaguardar a liberdade de expressão dos internautas, o direito à informação de modo amplo, a intervenção mínima do Estado. Por outro lado, graves delitos vão sendo praticados de forma avassaladora e desmedida. Nenhum direito é absoluto. Sempre houve excepcionalidades em prol de valores maiores como a dignidade humana, a segurança pública, a integridade física e psíquica das pessoas. Estelionato, racismo, xenofobia, pedo-pornografia, terrorismo, incitações ao suicídio, *trollismo*, *ciberbullying*, apologia ao ódio e tantas outras atrocidades cometidas no ciberespaço não podem ser tratadas com sanções leves. Muitos delitos cometidos são exacerbadamente graves e, consequentemente, necessitam de medidas proporcionais à extensão lesiva e danosa.

> O direito penal não é somente um instrumento de violência controlada contra autores de crimes; é também um meio de proteção dos direitos fundamentais das vítimas destes. Criminosos que atuam no ciberespaço não têm o menor respeito pelos direitos individuais dos usuários da Internet. Subtraem informações pessoais, fazem-se passar pelas vítimas, furtam valores, clonam cartões de crédito, cometem *grooming* contra crianças e adolescentes, distribuem vírus de computador, divulgam dados sigilosos (públicos e privados), realizam ataques de negação de serviço, destroem informações vitais para a sociedade ou tentam desestabilizar infraestruturas críticas, como sistemas de controle de tráfego aéreo ou de distribuição de energia elétrica. Infelizmente, a Internet não é um parque de diversões, um mundo idílico onde o mal não viceja (ARAS, 2010)[47].

É notório que o avanço tecnológico trouxe benefícios para a humanidade, em especial a faculdade de se expressar, de se comunicar de um extremo a outro do planeta de modo instantâneo e quase sem custo. Em que pese todas as benesses advindas deste fenômeno, a engenhosidade tecnológica pode ser utilizada indevidamente, possibilitando o ingresso e a configuração de ciberdelitos produzindo efeitos altamente nocivos para a sociedade. Faz-se, outrossim, imprescindível um arcabouço jurídico específico e eficaz para interpretar e aplicar

[47] https://blogdovladimir.files.wordpress.com/2010/01/artigo-marco-civil-da-Internet.pdf

a lei de modo coerente e justo. A seguir, será elencado um rol de leis que, direta ou indiretamente, trata do assunto.

4.9 LEIS BRASILEIRAS E PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO

O Brasil já julgou pelo menos centenas de crimes virtuais, crimes desde espionagem a sabotagem, este considerado como uma espécie de cyberterrorismo, além de outros. Segundo Renato Opice Blum (2011)[48], advogado especializado em Direito Eletrônico, : - "*apesar de não tão divulgadas, essas invasões ocorrem com mais frequência do que se imagina principalmente em empresas, sendo os transgressores identificados. A primeira sentença referente ao assunto aconteceu em 1996*". Ainda, segundo o advogado, algumas instituições nacionais se empenham para evitar esses tipos de crimes, declarando "guerra" aos crimes virtuais.

Diante das caracterizações dos delitos informáticos vistas há pouco (tópico 4.2 deste trabalho), podemos verificar que a legislação brasileira, mesmo ainda não tipificando a conduta criminosa de forma satisfatória, possui inúmeras leis que garantem a proteção aos bens jurídicos afetados por esses atos, podendo se destacar, entre outras, algumas leis e projetos de lei sobre o assunto, levando sempre em consideração que nenhuma legislação infraconstitucional pode deixar de observar os direitos e garantias fundamentais descritos na Constituição Federal de 1988, que destaca em seu artigo art. 5º, XXXIX: "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal", o que impossibilita uma interpretação ampla ou extensiva do tipo penal e sua aplicação em fatos análogos.

As condutas humanas, na norma penal, são classificadas como negativas, incriminando todos os fatos que possam estar desviados de uma conduta aceita socialmente.

A Constituição Federal, em seu artigo 5º, enumera os direitos individuais e coletivos, tais como:

> [...] X- a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação. [...] XXVII – Aos autores, pertence o direito exclusivo de utilização, publicação ou reprodução de suas obras [...] LXXII – Conceder-se-á habeas data: Para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público (BRASIL, 2012)[49].

[48] http://veja.abril.com.br/blog/augusto-nunes/videos-veja-entrevista/renato-opice-blum-advogado-especializado-em-direito-digital-o-conceito-de-privacidade-esta-mudando-talvez-esteja-acabando/

[49] file:///C:/Users/Nots/Downloads/constituicao_federal_35ed.pdf

Na conjuntura atual, têm sido utilizados os princípios constitucionais e legislações infraconstitucionais para sentenciar os crimes virtuais. Entretanto, as legislações penais não evoluíram com a mesma rapidez que a revolução tecnológica e os consequentes crimes. Por isso, houve uma estagnação do Brasil quanto às políticas de proteção ao Cibercrime, ficando o país sendo conhecido como tecnologicamente subdesenvolvido.

Diante desse cenário, alguns projetos de lei tramitaram ou ainda tramitam no Congresso para serem aprovados, aumentando, com isso, a proteção ao bem jurídico lesado. Dentre eles, podemos destacar:

Conforme informa Dullius, Hipller e Franco (2012), o Projeto de Lei nº 76, de 24 de março de 2000, de autoria do Senador Renan Calheiros, enumera, entre as condutas ilícitas mais comuns dos chamados "delitos informáticos", os seguintes tipos de comportamentos: "O acesso não autorizado a computadores e sistemas eletrônicos; A destruição e alteração das informações; A fraude eletrônica, entre outros". O Projeto de Lei do Senado nº 279, de 2003, de autoria do Senador Delcídio Amaral que tem como finalidade coagir os prestadores dos serviços de correio eletrônico a manter o cadastro detalhado. Desse cadastro constarão: "[...] se pessoa física: número do Cadastro de Pessoa Física (CPF), nome completo, endereço residencial, número da carteira de identidade (RG), data e órgão expedidor; [...] se pessoa jurídica: razão social, o endereço completo e o número do Cadastro de Pessoa Jurídica (CNPJ)".

Já o projeto de Lei nº 508, de 2003, institui a vedação da divulgação de informações privadas, como origem racial, opinião política, vida sexual, registros policiais, entre outros. Além desses projetos de lei, existem, no ordenamento jurídico, algumas leis específicas para tratar sobre o ciberespaço, dentre elas: A Lei 7.232, de 29 de outubro de 1984, que estabeleceu princípios a respeito do tema de Política Nacional de Informática, e criou também o Conselho Nacional de Informática. Tal lei representou a legitimação da política adotada pela SEI- Secretaria Especial de Informática, que consiste no ato de afunilar a entrada no mercado nacional de tecnologia de empresas brasileiras de capital estrangeiro. Observando o art. 171 da Constituição Federal instituiu proteção extra às empresas brasileiras de capital nacional.

Já a Lei 8.741, de 3 de dezembro de 1993, promoveu novas regras estruturais do CONIN. Órgão que faz parte do Ministério da Ciência e Tecnologia.

Com a proveniente discussão sobre a má utilização dos recursos tecnológicos e informáticos, o poder legislativo atentou-se e criou a Lei 7.646/87, que faz uma regulamentação da proteção da propriedade intelectual sobre programas de computador e sua

comercialização na nação. Faz previsão a dois tipos penais: a violação do direito do autor do programa de computador, com pena máxima de dois anos de detenção, e o ato de comercializar programas de origem estrangeira não cadastrada, com pena máxima de quatro anos de detenção.

O Código de Defesa do Consumidor, promulgado pela Lei 8.078/90, também criou tipos penais referentes ao tema, o de impedir o acesso de informações pessoais dos consumidores constantes em bancos de dados, com pena máxima de detenção de um ano ou multa; e o de falta de retificação imediata de informação inexata no banco de dados, com pena máxima de um ano também.

Lei 9.100, de 29 de setembro de 1995, estabeleceu normas para a realização das eleições de 1996, quanto à votação e apuração de votos no sistema eletrônico. Tal lei criou os primeiros tipos penais praticados por meio da informática. Dentre os crimes eleitorais, estão aqueles previstos no art. 67 da Lei, como o de "obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizados; tentar desenvolver ou introduzir comando, instrução ou programa de computador capaz de destruir , apagar, eliminar, alterar, gravar ou transmitir dados, dentre outros atos."

Em 1996, a Lei 9.296, de 24 de julho, veio regulamentar o inciso XII, parte final do art. 5º da Constituição Federal que dispõe sobre o sigilo de correspondência e das comunicações telefônicas. O texto legal, em seu art. 10, tipifica a interceptação de comunicações de informática e telemática. A Lei nº 9.609, de 19 de fevereiro de 1998 também dispõe sobre a proteção da propriedade intelectual de programa de computador e sua comercialização no País. E a Lei nº 9.983, de 14 de julho de 2000 alterou alguns artigos da Parte Especial do Código Penal, acrescentando dispositivos que tratam concernentes à criminalidade informática:

Como já discutido (no tópico 4.5.3 deste trabalho sobre pedofilia e pornografia infantil), o Estatuto da Criança e do Adolescente (com redação dada pela Lei n° 10.764, de 12 de novembro de 2003) tipifica a divulgação, por qualquer meio de comunicação, inclusive pela Internet, de imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente. Artigo 241: Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou Internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente.

4.9.1 Lei Carolina Dieckmann e Lei Azeredo

No tocante à legislação nacional sobre crimes na seara digital, há duas leis específicas, a 12.735 e a 12.737 que vigoram desde 2012. É uma legislação voltada especificamente para os chamados crimes digitais próprios, ou seja, crimes cometidos contra dados, informações ou sistemas de informação, diferentemente dos crimes digitais impróprios, em que os sistemas de informação são utilizados como instrumentos, como um meio para a prática ou execução de outros crimes.

Tais leis buscam uma dupla finalidade: responsabilizar os invasores de dispositivos alheios que furtam dados e, concomitantemente, convida o usuário a proteger suas informações, procurando, assim, dificultar a ação do cibercriminoso.

A Lei 12.737, intitulada Lei Carolina Dieckmann, tipificou a invasão de dispositivo informático alheio (Art.154-A do Código Penal), mas desde que tal invasão obedeça alguns requisitos: que a invasão seja indevida ocorrendo com rompimento de sistema de segurança e com o fim de obter, adulterar ou destruir os dados sem a devida autorização. Incorre nas mesmas penas quem instala alguma vulnerabilidade no dispositivo informático para alcançar a vantagem indevida.

Houve também, a ampliação do delito de interrupção ou perturbação de serviço de utilidade pública quando for por meio informático (Art. 266 do Código Penal) além de ter equiparado a documento particular, o cartão magnético, buscando punir a ação de falsificar cartões de débito e crédito.

Caso a invasão tenha por finalidade a obtenção de informações e segredos comerciais ou industriais, também será punida, configurando mais um dispositivo jurídico contra a espionagem digital.

As penas ainda são baixas, variando de 3 meses de detenção a 2 anos de reclusão, podendo serem agravadas havendo prejuízo econômico, divulgação ou vazamento dos dados na Internet ou se resultar na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou o controle remoto não autorizado do dispositivo invadido. O fato das penas serem menores é um ponto negativo no entendimento dos advogados especialistas em Direito Digital Pinheiro e Haikal, pois:

> ”[...] permite o enquadramento dos crimes como pequeno potencial ofensivo, o que não se coaduna com a proteção dos ativos intangíveis, a pedra angular da sociedade da informação. Muitas vezes uma apropriação indevida de dados pode ser mais prejudicial que um furto comum e, por isso, não deveria ter pena mais baixa;

> sobretudo em casos de espionagem que podem levar à concorrência desleal" (PINHEIRO; HAIKAL, 2015)[50].

A Lei 12.735, conhecida como Lei Azeredo, por conta dos protestos da época de sua elaboração (sendo o projeto taxado como uma espécie de AI-5 da Internet) trouxe apenas dois dispositivos jurídicos: o primeiro indicando que as Polícias Judiciárias mediante regulamentação, deverão se preparar para o combate a crimes digitais e o segundo que, em casos de crime de discriminação (Lei 7.716 de 1989), o juiz poderá solicitar a retirada de conteúdo discriminatório não somente de rádio, tevê ou Internet, mas de qualquer meio possível.

Ainda observando a análise de Pinheiro e Haikal,

> 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 (PINHEIRO; HAIKAL, 2015)[51].

Por fim, constatamos que a legislação brasileira ampara a privacidade, visando, ao mesmo tempo, coibir as condutas mal intencionadas no âmbito virtual, entretanto, ainda necessita de medidas que abordem, de forma mais eficaz e particular os Cibercrimes.

4.9.2 Uma análise do processo de inclusão do Marco Civil da Internet na agenda governamental à luz da teoria de múltiplos fluxos de John Kingdon

Este tópico procura identificar as razões que levaram o Marco Civil a ocupar prioridade na agenda governamental do país, sendo aprovado, de modo muito rápido, especialmente após as denúncias de espionagem norte-americana. A análise da questão será feita à luz da teoria de Kingdon, verificando a presença dos elementos constitutivos do modelo de múltiplos fluxos. Serão destacados os indicadores importantes nesse processo.

---

[50] http://www.gazetadopovo.com.br/vida-publica/justica-direito/artigos/a-nova-lei-de-crimes-digitais-evf935c0vqjw7rh9b4cq75tfy

[51] http://www.gazetadopovo.com.br/vida-publica/justica-direito/artigos/a-nova-lei-de-crimes-digitais-evf935c0vqjw7rh9b4cq75tfy

- **Histórico**

A concepção e desenho do Modelo de Múltiplos Fluxos são de John Wells Kingdon, americano, professor emérito da Universidade de Michigan e Presidente da Academia Americana de Artes e Ciências.

Tal modelo foi elaborado, a princípio, para alimentar/formular políticas públicas do governo federal norte-americano atinentes à área de saúde e transporte públicos. Posteriormente, tornou-se ferramenta basilar para a análise e elaboração de políticas públicas governamentais.

Capella (2005, p.3) assegura que "Baseado em um corpo extenso de dados empíricos, obtidos, em sua maior parte, por meio de entrevistas com altos funcionários públicos, o modelo preocupa-se com estágios pré-decisórios da formulação de políticas". Para se adentrar nos conceitos e estudo propriamente ditos dos Múltiplos Fluxos, faz-se necessário atentar para o que KINGDON (1995, apud Pereira e Teixeira) aponta como processos pré-decisórios para incluir pontos importantes na construção de uma política governamental, que são: a agenda e as alternativas. Frisa também o autor que há uma evidente distinção entre eles. Para compreensão do processo em si, convém fazer uma abordagem mais analítica desses dois aspectos.

- **Agenda**

É impossível desvincular as tratativas para se estabelecerem políticas públicas da ferramenta que contribui para a consecução de tal objetivo, ou seja, a agenda governamental e suas divisões.

Kingdon (2003 apud CAPELLA, 2005, p. 03)[52], define agenda como "[...] conjunto de assuntos sobre os quais o governo e pessoas ligadas a ele concentram sua atenção num determinado momento". O pronome indefinido "determinado" já aponta que as agendas sofrem ação direta dos assuntos que ocupam a atenção dos atores, podendo deixar de ser prioridade ou voltando a sê-lo em outras ocasiões.

Outro aspecto requer registro, ao se abordar o tema agenda, que é a questão dos tipos. O primeiro, conhecido como Agenda Sistêmica, que nada mais é senão um conjunto de assuntos que constituem o alvo da atenção de um povo, embora não se tenham tornado, ainda, objeto de conhecimento ou atenção do governo. Esses assuntos formam um leque incômodo de temas situados num horizonte externo ao poder central, sem que este esboce qualquer

[52] http://www.anpocs.org/portal/index.php?option=com_docman&task=doc_view&gid=3789&Itemid=318

atitude para inserção nas suas políticas de governo. O segundo, a Agenda Governamental, consiste numa panorâmica de temas que merecem do governo e seus assessores um foco de atenção, contudo, nem sempre chega às vias da prática. E o terceiro, A agenda Decisória, que "[...] constitui-se da lista de temas dentro da agenda de governo que são encaminhados para deliberação" (KINGDON, 1995; VIANA, 1996, apud PEREIRA e TEIXEIRA, 2011).

Em determinado momento, o próprio Kingdon classifica a Agenda Decisória, ou Decisional, não como um tipo distinto, entretanto sendo um componente da Agenda governamental. Deste modo, Kingdon (apud CAPELLA, 2005, p. 03) define este terceiro tipo de agenda como "um subconjunto da agenda governamental que contempla questões prontas para uma decisão ativa dos formuladores de políticas, ou seja, prestes a se tornarem políticas (polices)". Sendo assim, a Agenda Decisória engloba um elenco de temas, pinçado da Agenda Governamental, então escolhido para deliberação, pela importância e urgência, através de uma dinâmica similar ao *brainstorming.* Vale fazer uma analogia desse processo com o poema "Catar Feijão" de João Cabral de Mello Neto: "Catar feijão se limita com escrever/ jogam-se os grãos na água do alguidar/ e as palavras na folha de papel/ e depois joga-se fora o que boiar". É uma metáfora muito apropriada à Agenda Decisória, em que os atores envolvidos no processo têm de fazer uma escolha entre as alternativas apresentadas, implementando-se as que se mostram mais exequíveis.

- **Alternativas**

Diferentemente da Agenda, as alternativas constituem uma segunda etapa do processo pré-decisório. Como o próprio vocábulo quer dizer, são o cardápio de possibilidades em que se farão as escolhas para a implementação da agenda.

Antes de se discutirem os três fluxos estabelecidos por Kingdon, é importante registrar a existência dos atores, figuras importantes que desempenham papel crucial e permeiam todo o processo de escolhas para agendamento governamental de itens relevantes e sua consequente transformação em PL – Projeto de Lei, ou Leis propriamente ditas. Compondo este elenco, destacam-se dois tipos de atores: o visível e o invisível.

No rol de atores visíveis, ou seja, aqueles que merecem da mídia em geral o brilho dos holofotes, estão os que compõem a esfera administrativa, como o Presidente da República, que é considerado por Kingdon "o ator mais forte na definição da agenda" (CAPELLA, 2005)[53]. Além do Presidente, há Secretários-Executivos, figuras do Poder Legislativo

[53] http://www.anpocs.org/portal/index.php?option=com_docman&task=doc_view&gid=3789&Itemid=318

(Deputados, Senadores, etc). É interessante assinalar que, no cenário hodierno brasileiro, o Presidente da Câmara tem exercido um poder significativo na seleção ou descarte de temas propostos.

O universo de atores invisíveis é composto por servidores públicos, assessores de parlamentares, lobistas, acadêmicos, pesquisadores e consultores. Não se pode desprezar, neste cômputo, a opinião pública, bem como os atores sociais, fortemente atuantes nas redes, a mobilizarem milhares e até milhões de pessoas para elaboração de abaixo-assinados que, não raro, chegam ao Congresso e têm conseguido a inserção nas agendas.

Caso bem recente é o de uma moradora de Santo Antônio da Platina, no Paraná, que encabeçou um protesto, cujo desfecho fez a Câmara de Vereadores local não apenas rever um pedido de aumento exorbitante em seus salários, mas reduzir o que até então vigorava. Aqui, convém citar o que observa Capella (2005, p. 17): "Uma opinião pública negativa, por exemplo, pode fazer com que os atores do Poder Legislativo deixem de defender uma questão". É a população no papel de atores sociais.

- **Os três fluxos e seus mecanismos**

Para se chegar ao objetivo desta análise, que é entender como o tema "regulação da Internet" ganhou *status* de Agenda Governamental, e que dinâmica permeou todo o processo é importante que se faça uma breve consideração a respeito do Modelo de Múltiplos Fluxos, de John Kingdon, vez que se amolda, perfeitamente, como matriz e indicadores para referida análise.

Frise-se que este modelo tem sido sobejamente utilizado no Brasil em formulação de políticas públicas, como na "Montagem de agenda no Comitê Itajaí", (Bacia Hidrográfica), "A Inclusão de Catadores em Programas de Coleta Seletiva: da agenda local à nacional", "Avaliação da implementação das condicionalidades de Saúde do Programa Bolsa Família e seu papel no Cuidado à Saúde: estudo de caso no município do Rio de Janeiro," "O modelo dos múltiplos fluxos de Kingdon na análise de políticas de saúde: aplicabilidades, contribuições e limites", entre outros (CORRUPTECA)[54].

- **Problema**

Compondo o primeiro fluxo do Modelo está o "Problema", com que se

[54] http://corrupteca.nupps.usp.br/publicacoes/?q=modelo+de+m%C3%BAltiplos+fluxos

> [...]busca analisar de que forma as questões são reconhecidas como problemas e por que determinados problemas passam a ocupar a agenda governamental. Considerando que as pessoas não podem prestar atenção a todos os problemas durante todo tempo, Kingdon parte do pressuposto de que esses indivíduos concentrarão sua atenção em alguns problemas potenciais e tenderão a ignorar outros (CAPELLA, 2005)[55].

O que se pode depreender dessa afirmação é que o processo é seletivo: priorizam-se alguns problemas em detrimento de outros. Tudo vai depender de como os elaboradores de políticas fazem a leitura do cenário apresentado e o que eles vão pinçar, ante um vasto repertório de situações, aquelas que consideram cruciais e urgentes para serem definidas e apresentadas como problemas.

Para nortear referida seleção, três meios são basilares para que as situações apresentadas sejam alçadas a problema e este mereça de quem pode fazê-lo uma atenção especial. São eles:

a) Indicadores, que funcionam como um sinal amarelo de que há uma situação anormal, inclusive mensurando seu grau de magnitude;

b) Eventos, que são ocorrências como: acontecimentos marcantes, crises, etc. Exemplificando situações ocorridas na esteira histórica recente do Brasil, pode-se citar o caso do *impeachment* do ex-presidente Fernando Collor de Mello em 1992. Especificamente neste caso, a crise de credibilidade estartou o processo do impedimento. Ora, aquilo não constava da agenda do Congresso até que acontecimentos marcantes (aparição dos caras-pintadas na mídia, descoberta de corrupção envolvendo tesoureiro da campanha, etc.) começaram a fazer parte do cenário e da preocupação brasileiros. Outro exemplo é a situação de crise em que a nação brasileira mergulhou recentemente. Ela vem dando munição para levantamentos especulativos na esfera política. Numa análise à luz do objeto tratado neste capítulo, qual seja, o modelo de Múltiplos Fluxos de Kingdon no processo de regulamentação do Marco Civil Regulatório da Internet no Brasil, contribuíram sobremaneira para a inclusão do assunto na agenda governamental dois acontecimentos: primeiro, o vazamento e veiculação, na Internet, de fotos de uma atriz muito conhecida no cenário artístico brasileiro – Carolina Dieckmann (Nome da Lei já comentada); e, posteriormente, o "caso Snowden". Como será detalhado neste trabalho, as revelações daquele jovem americano a respeito do intrometimento do Serviço Secreto Americano em assuntos privados de outras nações, acabaram por concluir que ligações telefônicas e *e-mail* particulares da Presidente Dilma haviam sido rastreados pelos

[55] http://www.anpocs.org/portal/index.php?option=com_docman&task=doc_view&gid=3789&Itemid=318

Estados Unidos. Isso foi o suficiente para acelerar o processo de discussão a respeito dos limites do uso da Internet e priorizar a regulação de leis neste sentido.

c) Retroalimentação (*feedback*): frente de tarefas, projetos e programas podem denunciar problemas que, inicialmente, nem eram vislumbrados. O cenário brasileiro recente apresentou algo dentro deste contexto. Investigações que começaram timidamente e localizadas num caso apenas- tomaram desdobramentos de grandes proporções. Como o fio de uma meada, os fatos investigados têm-se desdobrado em progressão geométrica, retroalimentando outros.

- **Propostas e soluções**

Este segundo fluxo contempla o processo de identificação e seleção de alternativas viáveis para a solução do (s) problema (s) detectado (s). Não há como desconsiderar a importância dos atores, já tratados anteriormente, na elaboração de propostas e soluções.

Capella (2005)[56] estabelece uma interessante analogia entre este segundo fluxo e o "processo biológico de seleção natural", ao asseverar que

> A geração de alternativas e soluções é explicada pelo modelo de multiplestreams em analogia ao processo biológico de seleção natural. Da mesma forma como moléculas flutuam no que os biólogos chamam de "caldo primordial", o autor entende que as idéias a respeito de soluções são geradas em comunidades (policycommunities) e flutuam em um "caldo primordial de políticas" (policyprimevalsoup). Neste "caldo", algumas idéias sobrevivem intactas, outras se confrontam e se combinam em novas propostas, outras ainda são descartadas. Neste processo competitivo de seleção, as idéias que se mostram viáveis do ponto de vista técnico e as que têm custos toleráveis geralmente sobrevivem, assim como aquelas que representam valores compartilhados, contam com a aceitação do público em geral e com a receptividade dos formuladores de políticas. Como resultado final, partindo de um grande número de idéias possíveis, um pequeno conjunto de propostas é levado ao topo do "caldo primordial de políticas", alternativas que emergem para a efetiva consideração dos participantes do processo decisório (CAPELA, 2005, p. 06).

Compõem o elenco de atores atuantes, neste segundo fluxo, aqueles que partilham uma mesma preocupação, difundindo ideias como multiplicadores e de formadores de opinião. Foram citados anteriormente, tais como: assessores parlamentares, professores acadêmicos, pesquisadores, funcionários públicos, lobistas, etc.

- **Política**

Finalmente, no outro extremo dos fluxos, contribuindo para a eleição de um problema para compor uma agenda, está a questão política. É nessa esfera em que estão as assinaturas,

[56] http://www.anpocs.org/portal/index.php?option=com_docman&task=doc_view&gid=3789&Itemid=318

os carimbos, capazes de fazer valer aquilo que começou, vezes muitas, de um anseio da população, de uma prioridade estabelecida em mudança de governo, ou mesmo na retroalimentação, ferramenta que pode trazer à tona problemas graves e urgentes de solução.

Ferreira (2014, p. 25) afirma, taxativamente, que

> [...] não é a existência de uma solução que faz com que um problema seja inserido na agenda, transformando-se numa política; é necessário um contexto político favorável no qual ele seja reconhecido. Além disso, não é apenas o contexto político favorável que faz com que uma política seja decidida; é preciso que o problema seja bem definido, com suas relações causais bem estabelecidas, para sensibilizar os tomadores de decisão, e que existam soluções viáveis e aceitáveis para ele. Portanto, é a conjunção dos três fluxos (problems, policies, andpolitics) que abre uma "janela de oportunidade política" (policywindow) para que uma questão entre na agenda de decisão (do mesmo modo, uma "janela" se fecha quando um dos fluxos se desconjunta dos demais).

A questão da "janela de oportunidades" é muito bem apropriada para a análise do trâmite do Marco Regulatório da Internet no Brasil. Em que pese já ter sido objeto de referência neste trabalho, não custa lembrar que passou por movimento de sístoles e diástoles, de recrudescência e arrefecimento, desde que se delineou a primeira "janela", expressa em fatos que fizeram o Senador Eduardo Azeredo propor, em 2008, substitutivo ao PL 84/1999, de autoria do deputado Luiz Piauhylino e passou a tramitar em regime de urgência no Congresso; depois, mesmo que embrionariamente, com a participação do Presidente Lula no Fórum Internacional de Software Livre; posteriormente, houve acirrada discussão a respeito do tênue limiar entre regulação e censura, até ser encaminhado ao Congresso Nacional, em 2011. Outra "janela de oportunidades" foi o vazamento de fotos da atriz Carolina Dieckmann na web, em 2012, que alcançou grande repercussão nacional, além do caso da Presidente Dilma, (alvo, como dito, de espionagem americana denunciada por Snowden). Finalmente, o Marco Regulatório foi aprovado, em março de 2014, pela Câmara dos Deputados e, passados os trâmites de praxe, tornou-se lei.

O processo conceptivo do Marco Civil Regulatório da Internet trouxe desdobramentos de interpretação quanto aos mecanismos velados de censura no seu conteúdo, opiniões que se divergiam a respeito de uma visão regulatória que não palmilhasse um viés restritivo, mas libertário; que não enxergasse apenas a via penal, mas uma legislação que primasse pelo direito e liberdade de expressão, que possibilitasse malhas digitais com novas dinâmicas nas redes, onde privacidade, autonomia e neutralidade tivessem espaço. Ao esboço inicial do texto, houve reações, como a do ativista digital João Caribé com seu blog "Mega Não".

Referido processo, aqui discutido, nos remete a uma conclusão irrefutável: a Ciberdemocracia, através da ambiência do ciberespaço, expôs uma dinâmica nova do cenário hodierno. Fica bem claro que as novas tecnologias trazem, em seu bojo, o dilema entre o arcabouço legal obsoleto, com leis em descompasso com a celeridade das novas conquistas tecnológicas, e uma realidade digital nova, ainda não incorporada ao universo jurídico, ou por este não absorvida completamente, o que foi muito bem explorado por Ferreira (2014, p. 94):

> [...] se, por um lado, formuladores de política e sociedade debatem criação de normas para lidar com as novas questões trazidas pela Internet, muitas vezes, por outro lado, legisladores e tribunais parecem desconhecer o funcionamento do mundo virtual. Como consequência disso, vive-se o paradoxo entre a tentativa de proteção ultrarrestritiva e a liberação generalizada.

Finalmente, depreende-se do que foi exposto que, de uma forma articulada ou independente, o modelo de Múltiplos Fluxos proposto por Kingdon para estabelecimento de agendas, permeou todo o processo de regulamentação do Marco Civil Regulatório da Internet no Brasil, valendo-se de cada um deles, qual seja: problema, propostas/alternativas e política.

4.9.3 O Marco Civil da Internet

A Lei 12.965, de 23 de abril de 2014, sancionada pela Presidente Dilma Rousseff, "estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil" (BRASIL, 2014, art. 1). É o que se chamou de Marco Civil da Internet. Alvo de críticas por alguns, que chegam a questionar se se trata de uma solução ou um problema, a lei, no seu Artigo 2º, aponta para o reconhecimento da escala mundial da rede, finalidade social, pluralidade e diversidade, entre outros pontos.

Há, inegavelmente, um certo conflito entre privacidade da rede e os deveres elencados pela lei supracitada, para alguns considerados como se fossem um certo cerceamento de liberdade. Essa dicotomia será estudada a seguir.

O Marco civil da Internet, vigorando desde o dia 23 de junho de 2014, revela-se como sendo uma espécie de Constituição digital, pois conforme já foi dito, estabelece princípios, garantias, deveres e direitos para a utilização da rede no Brasil. O Marco regulatório tramitou por dois anos na Câmara dos Deputados. Foi apresentado, inicialmente, não como um texto de lei, mas com uma indagação à sociedade, a respeito do que se desejaria no tocante à regulação da Internet.

É oportuno esclarecer que a resposta não seria apenas sobre os malefícios gerados por ela, mas também sobre todo potencial positivo no que se refere:

> à cultura, à educação, ao desenvolvimento tecnológico e regional, ao infinito potencial de arranjos produtivos e mercadológicos que ela permite alcançar pela superação da necessidade de intermediários e consequente ganho de escala. Por fim, a geração de riqueza, conhecimento, produção e identidade regional (PEIXOTO, 2014, p. 29).

O texto regulatório da Internet no Brasil, mesmo apresentando algumas falhas legislativas, é um exemplo de Ciberdemocracia, da utilização da "ágora digital" em favor da população virtual, pois o processo de construção do projeto de lei contou com a participação de vários segmentos da sociedade. No ano de 2009, houve uma destacada mobilização com consultas públicas e a contribuição de organizações não governamentais, de setores públicos, internautas, instituições de ensino, empresas, dentre outros colaboradores.

O projeto foi dividido em dois períodos, cada um totalizando 45 dias. A fase primeira foi marcada por uma consulta aberta à sociedade (por meio de *blog* oficial, um grupo de discussão e um perfil na rede social - Twitter). Duração de 29/10/2009 a 17/12/2009. Foram realizados debates sobre princípios gerais que serviriam de fundamentação e referência para a elaboração do texto legal. Os princípios foram divididos em três grupos: (1) direitos individuais e coletivos (privacidade, liberdade de expressão e direito de acesso); (2) princípios e deveres relacionados aos intermediários (neutralidade de rede e responsabilidade por publicação de terceiro); e (3) diretrizes governamentais (abertura, infraestrutura e capacitação). Ao fim dessa fase, foi redigido um texto incluindo as questões mais importantes sobre a temática realizada.

A segunda fase, iniciada em 08/04/2010 e finalizada no dia 30/05/2010, submeteu à apreciação uma minuta de um anteprojeto de lei. Nessa fase foram permitidas diversas postagens (inclusive *e-mail*s), divulgação de notícias e comentários dos comentários.

Os assuntos tratados nesses debates foram: a) a guarda de registros de conexão, que havia sido um dos pontos principais de críticas ao projeto de lei dos Cibercrimes; b) a remoção e responsabilização dos intermediários por conteúdo publicado por terceiro; c) a liberdade de expressão e o anonimato; d) a requisição judicial para registros, as diretrizes comuns para o desenvolvimento na Internet em todas as esferas do governo, os parâmetros para os sítios públicos e a capacitação para o uso da Internet.

O projeto de cunho experimental transformou-se num ponto democrático, numa esfera pública destinada a debates. Uma plataforma digital foi estruturada para servir como local de

diálogo entre os interessados sobre a regulação da Internet. O *blog*, construído pelo Ministério da Justiça em parceria com o Ministério da Cultura tornou-se o instrumento virtual para o encontro.

O Marco regulatório é dividido em cinco capítulos, sendo reservado o primeiro a disposições preliminares englobando alguns fundamentos e princípios importantes que devem ser observados no uso da Internet por todos os agentes envolvidos, como a garantia de liberdade de expressão, a proteção da privacidade, a preservação e garantia da neutralidade da rede, entre outros.

O segundo capítulo contempla os direitos e garantias dos usuários, tais como o direito à inviolabilidade da intimidade e ao sigilo das comunicações privadas, o direito à indenização pelo uso indevido, o direito a acessibilidade e outros.

A provisão de conexão e a aplicação de Internet encontram-se no terceiro capítulo, que apresenta quatro relevantes seções, que abordando a neutralidade da rede, a proteção aos registros, aos dados pessoais e às comunicações privadas, a responsabilidade pelos danos decorrentes de conteúdo gerado por terceiros, bem como a requisição judicial de registros.

O quarto capítulo tratou da atuação do poder público, com a aplicação de diretrizes, deveres e iniciativas públicas. O quinto e derradeiro capítulo traçou as disposições finais, tais como o controle parental de conteúdo, a inclusão digital, a forma de exercício em juízo dos direitos e interesses estabelecidos nessa lei, além da *vacatio legis*, fixada em sessenta dias após sua publicação.

O Marco Civil, inicialmente, traz como fundamento, em seu art. 2º, a liberdade de expressão. Um direito consagrado previsto no art. 5º da Constituição Federal. No entanto, tal direito não é absoluto, pois o próprio texto constitucional proíbe o anonimato. Desse modo, trazendo a questão para o ciberespaço, caso a manifestação do usuário atente contra o direito de outrem, haverá um ilícito e, consequentemente, a responsabilização. Para tanto, há a necessidade da identificação do infrator. Além disso, caso o conteúdo divulgado fira direito alheio, é necessário, segundo a nova lei, em seu art.7º, II, de uma ordem judicial direcionada ao provedor para a retirada do conteúdo do ar.

Muitos juristas criticam essa exigência legal, pois antes do Marco Civil, o provedor poderia retirar divulgações que maculassem a integridade de alguém sem intervenção judicial. Em alguns casos, pelo requerimento da vítima ou por meio de acordo, fruto de mediações ou de soluções extrajudiciais.

De acordo com a nova lei, a única hipótese em que é obrigatória a retirada do conteúdo, sem ordem judicial, é no caso de conteúdo com nudez e atos sexuais, especialmente

na chamada “pornografia de Vingança”. Algo realmente justo. Mas existem outros casos que apesar de não envolver fotos e filmes de cunho muito íntimo ou com conotação sexual, são igualmente graves e devastadores.

O grande problema é que, no espaço virtual, a publicação de um conteúdo ofensivo tem uma repercussão vasta, pois o meio de divulgação é altamente veloz e amplo. A notícia ou informação chega muito rápida e acaba também sendo reproduzida quase que instantaneamente para inúmeras pessoas. Assim, a lesão à honra, à imagem ou à privacidade pode ser devastadora. Por isso, o tempo é uma questão preciosa quando o assunto é dano moral na Internet. Conforme Paulo de Sá, sobre as considerações realizadas em sua entrevista ao Desembargador Santarelli Zuliani (2014): “Muitas vezes, a demora faz com que o direito da parte seja prejudicado eternamente, tornando impossível evitar a propagação de conteúdo ilícito pela Internet”.

Sendo assim, a dependência de uma ordem judicial para a retirada de conteúdos evidentemente ilícitos, pode trazer a própria ineficácia da lei, pois cria um entrave à questão da celeridade, tão imprescindíveis em determinadas situações.

Uma das temáticas mais polêmicas do Marco Civil, prevista no Art. 9º, foi a denominada “neutralidade de rede”. O dispositivo prevê que: “O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação” (BRASIL, 2014)[57].

Em outros termos, a lei, ao dispor sobre o tratamento igualitário dos usuários na rede, objetivou impedir a oferta diferenciada de conexões pelos provedores ou, seja, não pode haver pacotes de preços distintos para o acesso exclusivo a determinados locais virtuais. Os provedores não poderão fazer distinção do fluxo de tráfego para determinados conteúdos ou acessos em detrimento de outros. “Portanto, substancialmente com a neutralidade de rede o consumidor ao contratar um plano de Internet pagará apenas pela velocidade contratada, não podendo haver limitação ao acesso a determinados sites” (MACHADO, R.C., 2015, p. 2)[58].

A garantia da neutralidade de rede pode ser um entrave à inclusão digital? Ainda não se sabe, mas no mundo globalizado e regido por uma estrutura capitalista, talvez a adoção dessa garantia implique num repasse aos usuários dos valores para a manutenção dessa neutralidade, podendo dificultar, cada vez mais, a acessibilidade com isonomia.

[57] http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
[58] http://jus.com.br/artigos/30162

O princípio da neutralidade da rede pode sofrer exceções, conforme o disposto no §1º do art. 9º da Lei nº 12.965/2014:

"§ 1o A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de: I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e II - priorização de serviços de emergência".

As exceções serão regulamentadas por meio de decreto presidencial, após consulta prévia ao Comitê Gestor da Internet (CGI.br) e a Agência Nacional de Telecomunicações – ANATEL" (BRASIL, 2014).

No entendimento de Machado (2014, p. 2):

> O único receio que se tem quanto a esta previsão de exceções à regra é em relação a um possível abuso à discricionariedade dada ao Presidente da República, uma vez que os pareceres da CGI.br e ANATEL não serão vinculativos, podendo o Presidente estabelecer regulamentações distintas às orientações. Ou seja, há um sério risco do chefe do executivo utilizar-se da roupagem da busca pela "finalidade social da rede" (art. 2º, inc. IV, do Marco Civil) e impor medidas restritivas de aplicações de protesto e organização sociais, tendo em vista que as recentes manifestações no Brasil e no mundo nasceram nas redes sociais.

O Marco Civil contempla também a guarda de registros eletrônicos para fins de investigação exigindo que os provedores de conexão guardem os dados de usuários por um ano. Já os provedores de aplicação devem guardar os dados por um prazo de seis meses.

Os provedores responsáveis pela guarda (sites e afins) deverão proteger os registros, dados pessoais e as comunicações privadas dos usuários, conforme o previsto no Art. a 10, da presente lei. O legislador buscou salvaguardar a intimidade, a privacidade, a honra e a imagem dos internautas. E, conforme já foi mencionado, os provedores somente disponibilizarão tais dados por ordem judicial, ressalvada a possibilidade, pelas autoridades administrativas (polícia, Ministério Público, Receita Federal etc), de obtenção dos dados cadastrais, na forma da lei. O prazo de um ano da referida guarda pode ser superior caso as autoridades mencionadas requeiram, Art. 13, § 3º (OLIVEIRA, 2014).

As regras constantes nos artigos 10 e 11 valem inclusive para empresas estrangeiras que operam no Brasil. Dessa forma, havendo descumprimento, tais organizações serão punidas com sanções que poderão ser aplicadas isolada ou cumulativamente, como: advertência; multa de até 10% do faturamento do grupo econômico no Brasil; suspensão

temporária ou proibição do exercício das atividades. Assim, qualquer empresa que preste serviços no Brasil, mesmo que seja uma filial, tem o dever de cumprir a legislação brasileira.

Simbolicamente, a lei aprovada expressa a representação democrática no campo da comunicação, uma barreira difícil de ser quebrada em razão da longa tradição do autoritarismo legal que sempre buscou beneficiar as empresas de radiodifusão e de telecomunicações no Brasil.

Foram mais de duas mil intervenções participativas. No Congresso Nacional, deputados e senadores debateram, partidos dialogaram e, ao término do processo, por meio de redes sociais e de outras mobilizações, houve a aprovação da lei. Em que pese as posições contrárias e algumas imperfeições legais, o Marco Civil foi fruto de um processo democrático, uma vitória do povo brasileiro.

4.9.4 A Convenção de Budapeste

A Convenção de Budapeste, conhecida como Convenção sobre o Cibercrime, é um tratado internacional do Conselho da Europa que engloba mais de 20 países e foi criado em 2001, na Hungria, pelo Conselho da Europa (e está em vigor desde 2004). Países como Canadá, Japão, África do Sul, Espanha e Estados Unidos ratificaram o tratado. A Convenção de Budapeste nasce com grande participação e influência da União Europeia, a partir de estudos e pesquisas do OCDE (Organização para a Cooperação e Desenvolvimento Econômico) e G8 que discutiram, há bastante tempo, a necessidade latente de mudança e cooperação internacional para uma renovação em matéria Penal e combate ao crime transnacional.

Já assinada por 46 países, a Convenção tipifica os principais crimes cometidos na Internet (como conteúdo de pornografia infantil e ofensa aos direitos autorais), definindo-os como infrações contra sistemas e dados informáticos ou relacionadas com computadores. Dessa maneira, a convenção cumpre a função de auxiliar na proteção efetiva da sociedade no ciberespaço a partir da cooperação entre os Estados e da tentativa de harmonizar as legislações nacionais (SOUZA; PEREIRA, 2015)[59].

O progresso de novas tecnologias deflagrou uma profunda mudança nos conceitos tradicionais sobre uma série de questões como espaço e tempo. Essa transformação na sociedade fez com que novos fenômenos e condutas sociais surgissem em meio ao corpo

[59] http://www.academia.edu/786458/A_CONVEN_DE_BUDAPESTE_E_AS_LEIS_BRASILEIRAS

público. E, dessa forma, revelou-se necessário que outras searas do conhecimento humano também acompanhassem a mutação para que pudesse haver uma adequação social. Nessa conjuntura, surge a discussão sobre o Cibercrime, a contravenção realizada por intermédio das redes virtuais. Novos instrumentos jurídicos foram aparecendo através da cooperação penal internacional, visando à aplicação da lei em escala global e não em território específico, sujeitando a legislação à inefetividade.

> As novas tecnologias existentes irão desafiar os conceitos jurídicos. Informação e comunicação fluir mais facilmente em todo o mundo. Fronteiras não são mais limites para este fluxo. Os criminosos estão cada vez mais localizadas em locais diferentes do que os seus actos produzir os seus efeitos. No entanto, as leis são geralmente confinado a um território específico. Assim, soluções para os problemas devem ser abordados pela legislação internacional, que requeiram a adopção de adequados instrumentos jurídicos internacionais. A presente Convenção visa enfrentar este desafio, com o devido respeito aos direitos humanos na nova sociedade da informação (CONVENÇÃO DE BUDAPESTE apud MORAIS NETO, 2009, p. 124).

Neste sentido, depreende-se que a legislação penal sobre o Cibercrime encontrou grande progresso na Convenção de Budapeste, criada a partir de uma discussão global sobre as mutações ocorridas nos últimos anos sobre a eficácia da lei em casos de crimes virtuais. Tese essa confirmada pelos próprios termos do preâmbulo da Convenção de Budapeste:

> Convictos de que a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e confiável; [...]de modo a tornar mais eficazes as investigações e as acções penais relativas a infracções penais relacionadas com sistemas e dados informáticos, bem como permitir a recolha de provas em forma electrónica de uma infracção penal (MORAIS NETO, 2009, p. 125)

A Convenção possui quatro capítulos e 48 artigos em sua estrutura normativa, que destacam seus pontos jurídicos fulcrais. O capítulo I possui apenas um artigo que trata de nomenclaturas. Já o II, estabelece medidas a respeito de direito penal e processual e o III trata de princípios referentes à cooperação internacional. O capítulo VI contém disposições a respeito da aplicação territorial, procedimento de adesão, entre outros princípios práticos. Visando à grande importância da cooperação internacional, o artigo sobre a questão da adesão à Convenção, deixa claro que está aberta à adesão de outros países que não participaram de sua elaboração contanto que convidados pelo Comitê de Ministros do Conselho da Europa

(após declaração de acordo unânime e consulta aos Estados signatários). Conforme o artigo 37 da referida Convenção de Budapeste sobre a adesão: "[...] é possível se constatar o sobredito: "[...] O Comitê de Ministros do Conselho da Europa pode [...] convidar qualquer Estado não membro do Conselho e que não tenha participado na sua elaboração, a aderir à presente Convenção".

A maioria dos países que adotaram o texto já se organizou quanto à regulamentação da Internet para se adequar aos parâmetros criminais de aplicação do tratado. A estrutura para investigação dos crimes cibernéticos é complexa possuindo acervos direcionados para cada campo específico, como crimes de pedofilia, xenofobia, fraude, organizações criminosas e terrorismo. Para garantir efetividade no combate aos Cibercrimes, a adoção ao tratado deve estar aliada a mudanças concretas. Alguns de seus países membros, Itália e Portugal, por exemplo, só começaram a agir anos após a assinatura. (VICENTE, 2014)[60].

Apesar dos vários elogios ao pioneirismo da Convenção, muitos países ainda possuem receio do fato de o tratado dispor de um artigo que prevê o uso de interceptação de comunicações, além da vigilância de redes internacionalmente. As críticas direcionam-se no sentido de uma possível ofensa a direitos fundamentais como privacidade e liberdade de expressão. Conforme o relatório explicativo da Convenção:

> [...] o uso, incluindo um eventual uso de caráter transfronteiriço, e a aplicabilidade de poderes coercitivos num meio tecnológico, a saber, a intercepção de telecomunicações e a vigilância eletrônica das redes de informação, por exemplo, através da Internet, a investigação e apreensão no que se refere a sistemas de tratamento da informação (incluindo os sites da Internet), tornando inacessível o material ilegal e exigindo dos fornecedores de serviços o cumprimento de obrigações especiais, tendo em consideração os problemas resultantes de medidas específicas de segurança da informação, como por exemplo, a encriptação (CONVENÇÃO... apud FERREIRA, 2014, p. 42).

Ainda que se percebam inclinações visíveis do Congresso Brasileiro (a partir de projetos de lei e da aprovação do Marco Civil) a disposições semelhantes à legislação internacional sobre o Cibercrime, o país ainda não aderiu ao tratado. Há grande expectativa sobre a adesão do Brasil ao texto da Convenção, porém, além do convite do Comitê de Ministros do Conselho da Europa (que não parece um problema já que o país tem boas relações internacionais podendo obter aceitação unânime dos países membros da Convenção) tem que haver manifestação de interesse do Estado, o que parece não ser uma prioridade. Como já comentado, deve haver uma preparação técnica e civil de regulamentação para que

[60] http://pt.slideshare.net/AymeVicente/monografia-a-arte-da-computao-em-polticas-pblicas-legislao-preveno-e-combate-aos-Cibercrimes

possa ser possível a aplicação dos parâmetros criminais. Além disso, também, precisa-se fazer um preparativo com adequações preliminares para que possa existir a compatibilização das leis nacionais com o texto do tratado e, talvez, o Brasil não esteja preparado para promover estas organizações (VICENTE, 2014)[61].

Este e outros motivos, como por exemplo, o conflito já discutido entre os direitos fundamentais (estabelecidos na Constituição Federal) e medidas processuais de investigação consideradas como vigilância adiam a adesão do Brasil. O fato é que apesar de diversos órgãos do governo já terem analisado o texto da Convenção, este nunca foi aprovado. Isso, acontece, apesar da necessidade crescente que o país tem em combater as milhares de ocorrências de Cibercrimes de diversos tipos cada vez mais frequentes. O que, não impede, entretanto, que a nação brasileira crie sua própria legislação de combate a tais crimes.

À luz do exposto, contata-se que, a despeito de a legislação penal comum abarcar ainda grande parte dos crimes ocorridos mesmo no meio virtual (como dano, racismo e crimes contra a honra), sente-se a necessidade da legislação específica, pois, questões procedimentais jurídicas, como jurisdição e competência, além de investigação policial encontram obstáculos pelo rompimento de fronteiras que o ciberespaço ocasiona. Destaca-se a importância da cooperação internacional, apesar das dificuldades de adequação das jurisdições (o conflito entre soberanias) e de instrumentos jurídicos hábeis na luta pelo combate eficaz a essas novas estirpes criminais.

[61] http://pt.slideshare.net/AymeVicente/monografia-a-arte-da-computao-em-polticas-pblicas-legislao-preveno-e-combate-aos-Cibercrimes

5 O CASO SNOWDEN: a necessidade de criação de diretrizes para fortalecer a Cibersegurança brasileira

Neste capítulo, será estudado de modo abrangente, o caso Snowden e sua repercussão no Brasil e no mundo. Importante ressaltar, também, que se fará uma breve análise sobre a questão da Cibersegurança no contexto brasileiro.

5.1 O CASO SNOWDEN: Prolegômenos

> Não quero viver em um mundo onde tudo que digo, tudo que faço, todos com quem converso, toda expressão de criatividade, amor ou amizade estejam sendo gravados.
>
> (SNOWDEN apud HARDING, 2014, p. 9)

Em 1948, uma obra secular, com laivos premonitórios, quiçá proféticos e notadamente futurista, lançada por George Orwell, fazia referência a um ser nunca visto, mas abstratamente presente, que ceifava a privacidade de todos em função das teletelas espalhadas em diversos lugares. Em grandes letreiros, uma expressão recorrente: “O Grande Irmão está de olho em você" (ORWELL, 2009). E assim, o povo ia vivendo em meio à submissão, monitoramento, ausência de liberdade e totalitarismo, até que Winston, protagonista da história, resolve transgredir o sistema e se rebelar contra o regime. Essa ficção, criada no final da década de quarenta, do século passado, surpreendentemente, espelha uma realidade vivida no cotidiano do século XXI. A avançada era tecnológica, com suas microcâmeras, satélites, interceptações telefônicas, celulares hackeados, *dronies* expõe todos a uma nociva devastação da intimidade. Em que pese as suspeitas, ou, até mesmo, o conhecimento de que se está sendo espionado, há uma anuência tácita, um silêncio hibernado, uma acomodação apática. Assim como no romance orwelliano, foi necessário, nos dias de hoje, que alguém corajoso reagisse para despertar os demais contra o cerco de vigilância e monitoramento. Foi o que fez Edward Snowden.

Na história jornalística mundial, indubitavelmente, nunca alguém havia revelado um acervo tão grandioso e ultrassecreto, com arquivos de conteúdo altamente comprometedores vindos do maior organismo global de segurança e inteligência. As razões que motivaram tão perigosa e audaciosa delação foram: a desilusão perante o governo e o sistema estatal; a

violação à Constituição americana e a invasão abusiva à liberdade de expressão humana no tocante ao agir, pensar, criar e viver.

Impulsionado pela lisura, pela ética e pela cidadania, Eduard Snowden expôs ao mundo, a verdadeira face da Agência de Segurança Nacional dos Estados Unidos, bem como, dos chamados aliados. Ele poderia ter leiloado toda carga de documentos secretos aos quais teve acesso, poderia ter comercializado todo conteúdo a países, organizações estrangeiras e ter se tornado um milionário, mas não o fez. As razões que moveram Snowden eram caracterizadas por um cunho ético, ideológico e humanista.

A revelação contida nos arquivos publicados demonstrava que as agências de inteligência dos EUA e do Reino Unido, por meio de uma espionagem exacerbada, tiveram acesso à inúmeras informações eletrônicas justificadas pelos ataques pós 11 de setembro que geraram pânico e desordem em solo norte-americano.

Os documentos ultrassecretos mais notáveis da atual conjuntura mundial não foram expostos de uma só vez, nem de modo instantâneo e irresponsável. Foi necessário um longo e gradativo trajeto estratégico para revelar ao mundo a ausência de limites e o desrespeito à privacidade e à liberdade humanas.

Por muitos meses, Snowden estudou, analisou e pesou os desafios, as consequências e repercussões de sua delação. As revelações não poderiam ser compartilhadas antes de serem transmitidas a pessoas erradas. Era necessário encontrar cidadãos confiantes e responsáveis.

O alvo da espionagem realizada pela Casa Branca incluía terroristas, russos, iranianos, chineses, a AL-Qaeda, latino-americanos, dentre outros. Além de prováveis inimigos, supostos aliados também foram espionados, tais como a França, Alemanha, Itália, México, Brasil, bem como os próprios cidadãos norte-americanos (G1, 2015)[62].

Em parceria com a National Security Agency - NSA e localizada na área interiorana da Inglaterra, estava a Agência de Inteligência do Reino Unido, o GCHQ (Govermente Comunications Headquarters). As duas organizações agiam em conjunto na execução de programas de alta espionagem, trocando e compartilhando inúmeras informações. A referida parceria já existe desde a década de 40 do século passado, no auge da segunda Grande Guerra.

Um dos nomes de confiança do jovem analista era Glenn Greenwald, jornalista do The Guardian (jornal inglês) que à época estava trabalhando na cidade do Rio de Janeiro, no Brasil. A outra pessoa era a documentarista americana Laura Poitras. A NSA perdera o seu

[62] http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html

verdadeiro foco, sua missão genuína de recolher inteligência sobre o exterior, transformando numa grande observadora eletrônica em massa.

Snowden tinha 29 anos quando relatou o fato, era um contratado terceirizado da Agência de Segurança Nacional. Trabalhou em Kunia, no Havaí, no centro regional de operações da NSA. O jovem que estava hospedado no Mira Mar hotel em Hong Kong portava uma mochila, poucas roupas, mas detinha um arsenal de informações em *laptops* cuidadosamente criptografados. Eram documentos extraídos dos servidores da NSA e do GCHQ:

> Dezenas de milhares de documentos, na verdade. A maioria estava marcada como "Top Secret" (altamente sigiloso). Alguns, como "Top Secret Strap 1" — o maior nível britânico de confidencialidade para material interceptado — ou mesmo "Strap 2", que era o mais secreto possível. Ninguém — fora um restrito círculo de agentes de segurança — jamais tinha visto documentos deste tipo antes. O que carregava, segundo Snowden, era o maior vazamento de inteligência da História (HARDING, 2014, p.13).

A Internet tornou-se alvo de manipulação do governo estadunidense, pois era facilmente possível, por meio de uma megacoleta de dados, saber amplamente sobre pessoas, instituições, lugares, numa espécie de sequestro da privacidade. Um estado de extrema vigilância ou panóptico (expressão utilizada por Snowden, mas utilizada também por Jeremy Bentham, filósofo inglês, ao descrever uma prisão em que os soldados tinham visão integral de todos os presos, sem que estes notassem, em razão do formato circular do estabelecimento) (HAILER, 2014)[63].

Por meio de registros telefônicos, *e-mail*s, ligações de interceptadores de dados aos cabos de fibra ótica, os EUA e seu aliado britânico tiveram acesso a grande parte das comunicações mundiais. Além disso, a NSA acessava direto os grandes servidores, tais como: Google, Microsoft, Facebook, Apple, entre outros. Visando o enfraquecimento do sistema, a NSA dos EUA introduziu Backdoors (recurso que possibilita o acesso remoto a uma rede) secretas em softwares de criptografia *on-line*, utilizadas para proteção e segurança das transações bancárias (G1, 2015)[64].

A revelação de Snowden causou um grande impacto nos EUA e na Europa, pois abriu uma acirrada discussão acerca de antagônicos direitos: de um lado, a segurança, do outro, as liberdades civis; de um lado, a liberdade de expressão, do outro, a privacidade. Em que pese

[63] http://revistaforum.com.br/digital/138/criptografia-e-distopia-da-sociedade-controle/
[64] http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html

toda a discussão entre políticos, civis, instituições, órgãos de imprensa, nada foi capaz de impedir que Snowden fosse acusado de crime de espionagem e da cassação de seu passaporte. Além disso, os jornalistas que se dispuseram a narrar e noticiar toda a trama de espionagem revelada foram também vítimas de dilemas e de possíveis implicações nas searas jurídica, política e profissional.

5.1.1 The True Hooha: um jovem da Carolina do Sul

Snowden nasceu em 21 de junho de 1983, nos Estados Unidos, em Elizabeth City (Carolina do Norte), porém foi criado em Wilmington, no mesmo estado. Sua mãe, Elizabeth (mais conhecida como Wendy) nasceu no estado de Maryland, em Baltimore e é uma funcionária do Tribunal Federal de Maryland. O pai de Snowden, Lonnie Snowden (nascido em Pennsylvania) era um virtuoso oficial da Guarda Costeira dos Estados Unidos. Snowden tinha um pseudônimo na Internet, The true Hooha, pois era colaborador assíduo do ARS Technica (site especializado em tecnologia). No decorrer de oito anos, participou de quase oitocentos comentários, demonstrando um vasto conhecimento sobre computadores, programas, além de expor opiniões políticas expressando fortes convicções no campo da liberdade pessoal. Entre o final de 2009, prenúncio de 2010, The true Hooha foi esboçando um pouco de descrença e dando os primeiros sinais de preocupação acerca da sociedade e do Estado.

O senso libertário e a visão patriota foram herdados de seu pai, Lonnie Snowden, um membro das Forças Armadas Americanas. Desejando servir ao seu país e seguir a carreira paterna, Snowden resolveu se alistar na Geórgia na época em que os EUA invadiram o Iraque (2003-2004), no entanto após um acidente em que fraturou as pernas, foi dispensado. Retornando, em 2005, empregou-se no Centro de Estudos Linguísticos Avançados, na Universidade de Maryland, no cargo de "especialista em segurança". Era um posto da NSA, no campus da universidade (WIKIPÉDIA, 2014)[65].

Edward não ingressou na faculdade. Preferiu utilizar sua inteligência e desenvoltura no meio digital, tornando-se um *expert* na área da computação, assim, em 2006 começou a trabalhar para a CIA no setor de tecnologia da informação. Em pouco tempo, conheceu os meandros que envolviam a segurança da rede de computadores do órgão mais importante da inteligência norte-americana.

[65] https://pt.wikipedia.org/wiki/Edward_Snowden

O trabalho, num órgão de grande relevância estatal, proporcionou ao jovem, uma rica visão do mundo, pois passou a viajar e conhecer outros países, com culturas, ideologias e contextos sociopolíticos distintos. Em Genebra, na Suíça, zelou pela segurança dos diplomatas norte americanos operando no setor de tecnologia da informação e sistemas. Ele teve acesso a um feixe de opiniões políticas, sociais e econômicas, conhecendo intelectuais de esquerda. Nesse período viajou para Sarayevo, Bósnia, Romênia e Espanha.

Nessa época, era um crítico rígido dos jornais e do *website dos Wikileaks*, discordando da maneira como as publicações de vazamento de informações eram realizadas por Assange, podendo expor pessoas ao perigo. No entanto, a Suíça foi uma grande escola para Snowden, pois, estando muito próximo dos funcionários da CIA e de todo o aparato sigiloso e invasivo da espionagem, passou a rever seu posicionamento.

> Muito do que vi em Genebra realmente me desiludiu quanto à forma como meu governo funciona e qual o seu impacto no mundo. Percebi que eu fazia parte de algo que estava causando muito mais danos do que benefícios (SNOWDEN apud HARDING, 2014, p. 34).

No auge da campanha de Obama e pouco depois de sua posse, Snowden tinha uma expectativa de mudança, especialmente no tocante aos abusos ocorridos na baía de Guantánamo, em que homens eram presos e torturados, sem uma acusação plausível, sem o devido processo legal, aguardando anos sem julgamento, sendo que alguns não tinham comprovação de envolvimento com extremistas, nem terroristas. Decepcionou-se com o novo Presidente, que, em sua visão, manteve os resquícios da era Bush que afrontava a liberdade civil e a dignidade humana.

A função que desempenhava no cargo de administrador de sistemas possibilitou a Snowden compreender o raro e extraordinário poder de vigilância da NSA, e como a referida agência ultrapassou os limites legais previstos na própria legislação pátria, bem como em tratados internacionais. Ele passou a questionar sua própria função e a verificar que não estava de acordo com a devastação abusiva das informações realizadas pelo governo.

Demitiu-se da CIA e passou a trabalhar na Dell como terceirizado numa das unidades da NSA no Japão, passando a ter acesso a material altamente secreto, devido as suas habilidades em TI. Gradativamente ele foi tendo acesso a ampla fonte de dados espionados pela NSA. Em 2012, saiu do território japonês e foi trabalhar no Centro Regional de Criptografia da NSA no Havaí, ainda como contratado da Dell. Na função de administrador de sistemas, acessou uma vasta rede de informações secretas, especialmente sobre a China,

alvo estratégico da inteligência americana. Foi assim, que o jovem da Carolina do Norte, tornou-se um prodígio especialista em TI, conhecendo o vasto sistema de espionagem e deparando-se com dilemas inquietantes.

> A NSA podia colocar uma escuta em "qualquer um", do presidente para baixo, disse Snowden. Na teoria, a agência de espionagem deveria coletar informação de inteligência apenas de alvos estrangeiros, conhecidos como SIGINT. Na prática, aquilo era uma piada, disse Snowden a Greenwald: a NSA já estava capturando metadados de milhões de norte-americanos. Registros telefônicos, cabeçalhos de *e-mail*, as linhas de assunto, tudo levantado sem autorização ou consentimento. A partir dessas informações era possível construir uma narrativa eletrônica completa da vida de um indivíduo — seus amigos, seus romances, suas alegrias, suas tristezas. Em conjunto com o GCHQ**,** a NSA tinha ligado secretamente interceptadores de dados aos cabos de fibra ótica submarinos que circundam o globo. Isso permitiu que os EUA e o Reino Unido tivessem acesso à maior parte das comunicações mundiais. Tribunais secretos convenciam empresas de telecomunicações a entregar seus dados. Mais que isso: praticamente todo o Vale do Silício estava envolvido com a NSA, disse Snowden. Google, Microsoft, Facebook, até mesmo a Apple, de Steve Jobs. A NSA alegava ter "acesso direto" aos servidores das gigantes da tecnologia (HARDING, 2014, p. 13-14).

Havia o grande receio de ser preso e de ter toda a aparelhagem confiscada pela CIA, porém Snowden já estava muito imerso no que seria a missão de sua vida. Ele repugnava as atitudes antilibertárias do governo dos EUA, que ofendiam o direito à privacidade e a própria dignidade humana de milhões de pessoas. Era um abuso de poder, e ele estava certo de que, apesar de prever consequências pela sua ousadia, tudo valeria a pena.

5.1.2 Os jornalistas aliados de Snowden

Glenn Greenwald é um comentarista político, de 46 anos de idade, bastante expressivo em sua geração. Profissionalmente, é bastante retórico, pratica o sarcasmo em suas construções e comentários, e é incisivamente crítico, especialmente quando se trata da política americana. Nesta conjectura, os seus temas mais recorrentes são: os direitos dos cidadãos, os ataques por mísseis guiados, a "intervenção" conveniente dos EUA no mundo muçulmano, a administração de Obama, guerras estrangeiras e o regime norte-americano de tortura mundial.

Em comentários extensos, Greenwald se tornou afamado por discorrer sobre sua opinião a respeito da violação da privacidade, da soberania de modo geral, e da vigilância praticada pelo governo. Nesse contexto, ele até apontou os possíveis crimes cometidos pelo governo americano em vários países pelo mundo. Greenwald escreveu para o site Salon.com no qual postava suas opiniões políticas como fazia anteriormente em seu blog pessoal "Unclaimed Territory". Em agosto de 2002, saiu do Salon e começou a estabelecer parceria

com o “The Guardian”, contribuindo como colunista *freelance*. O Guardian é um jornal americano vanguardista, que transformou a maneira de se executar o jornalismo com diversos novos recursos tecnológicos. Glenn parece se identificar bastante com esse perfil, o que garantiu uma parceria de sucesso. Com essa abertura, Greenwald empreende uma discussão sobre o significado de exercer o jornalismo no século XXI, com as transformações que o mundo virtual traz.

Em dezembro de 2002, um *e-mail* recebido que mudaria sua vida passou despercebido entre tantos que se aglomeravam em sua caixa de entrada diariamente. Nele, o remetente escrevera que tinha informações que poderiam interessá-lo. Mas, foi muito genérico em sua expressão e não chamou atenção, fazendo com que Glenn não o tratasse como prioridade. Alguns meses depois, em um encontro em Hong Kong, Greenwald descobriu que os *e-mail*s a que ele não deu tanta importância eram de Edward Snowden, que admirava seu trabalho. A grande oportunidade desperdiçada por Greenwald de angariar graves e essenciais informações gerou frustração no delator.

Após isso, buscando uma outra maneira de contatar Green, em janeiro de 2013 Snowden enviou um *e-mail* para a documentarista Laura Poitras (próxima de Greeenwald) que também fazia críticas a vigilância dos EUA. Por conta do seu ousado jornalismo, Poitras foi perseguida durante cerca de seis anos (a partir de 2006), toda vez que ela entrava nos EUA, os agentes do Departamento de Segurança de Estado confiscavam seus objetos, prendiam-na diversas vezes e a interrogavam, sem sucesso, já que nunca conseguiam provas que a incriminassem. Em 2011, foi ameaçada de invasão em seus aparelhos eletrônicos, pois não queria falar sobre seu trabalho. O repúdio à tamanha invasão de privacidade fez com que ela se tornasse especialista em criptografia para que suas informações ficassem protegidas.

Quando se mudou para Berlim, Poitras recebeu um *e-mail* de Snowden dizendo que era um membro da comunidade de espionagem. Na época, ele era analista de infraestrutura, há pouco tempo, e o título que se deu no *e-mail* parecia ser para chamar atenção de Poitras. Eles começaram a se comunicar com a proteção da criptografia, mesmo que ela tivesse dúvidas sobre a legitimidade do bom intento de Snowden, ainda desconhecido (poderia ser uma armadilha do governo). Ele disse que continha informações importantes que queria revelar. Snowden continuava contatando com Poitras por redes alternativas, cuidadosamente, para não ser descoberto.

Em um dos seus *e-mail*s, Snowden mandou uma informação reveladora, disse ter posse de um documento de sigilo absoluto, a Política Presidencial com a Diretiva 20, de outubro de 2012. Tal documento delatava um pedido secreto de Obama aos seus funcionários

(sêniores da segurança nacional e da inteligência) de que fizessem uma lista de alvos potenciais para ataques cibernéticos. Poitras se assustou ao receber o relato de Snowden de que ele tinha como provar que os americanos estavam promovendo ataques no exterior. A agência NSA estava colocando escuta em cabos de fibra ótica, grampeando e interceptando pontos de telefonia em todo o mundo. A partir disso, Poitras buscou averiguar a veracidade das informações através de contatos com especialistas confiáveis no assunto.

Devido ao perigo que corria, cercada pela vigilância das forças americanas, precisou encontrar um meio seguro de comunicação para entrar em contato com o seu parceiro Greenwald. Poitras conseguiu marcar um encontro com ele, em uma de suas viagens aos EUA, em um local improvável para que não fossem descobertos. Eles se encontraram para que pudessem conversar sobre o correspondente misterioso de Poitras. Ela ainda não se dava conta de que estava em um momento importante, a um passo do vazamento mais significativo da história da espionagem americana (o qual Snowden propiciou com toda coragem mesmo tendo consciência de que aquilo traria consequências imensuráveis). Glenn e Poitras perceberam a autenticidade dos *e-mail*s. Eles notaram que, de fato, aquele correspondente era possuidor de inteligência, visão crítica e, dizia coisas que faziam todo sentido - parecia planejar uma astuta revolução calculada, dada a riqueza de detalhes.

A cada tempo que se passava, a fonte dos jornalistas parecia revelar coisas mais sérias e intrigantes, e eles sabiam que a maneira mais segura de provar a ilegalidade das ações da NSA seria obter os documentos de segurança nacional. Em abril de 2013, Greenwald recebeu um pacote de Poitras: eram dois *pen drives*, neles continham um kit de segurança para instalação de um programa de bate-papo criptografado. Nesse estágio, Snowden estava destinado a divulgar um documento que revelaria o envolvimento entre a NSA e uma influente corporação de Internet na produção de um programa secreto intitulado PRISM. Ele mandou um arquivo criptografado para Poitras, que era o PowerPoint do PRISM e um mapa com um conjunto de informações de como eles se encontrariam, dizendo que o ponto de destino seria Hong Kong. Neste momento, Snowden já havia revelado seu nome à jornalista. Aproveitando o canal criptografado de Greenwald, Snowden também começou finalmente a conversar com ele. Snowden enviou 20 documentos secretos dos santuários internos da NSA, como os slides do PRISM e alguns que preenchiam informações sobre o caso de impunidade do STELLAR WIND, tão estudado por Glenn. Dessa forma, Glenn foi para Nova York e conversou com Gibson na sede do Guardian, convencendo-a de que uma viagem até Hong Kong possibilitaria uma descoberta mais aprofundada sobre todo o assunto e a fonte

misteriosa. Já que muitos documentos eram técnicos, só Snowden, que conhecia os métodos e especificações da NSA, podia ajudar a interpretá-los.

Apesar da seriedade da questão, já que despertar a ira da NSA, do FBI, da Casa Branca e de outros poderosos envolvidos parecia uma missão suicida, o Guardian mandou Glenn e outro membro da equipe (Ewen MacAskill, um dos mais respeitados jornalistas do Guardian) para Hong Kong. MacAskill tinha grandes experiências, fez uma cobertura sobre a vitória nas eleições de Tony Blair, em 1997 e em 2000 se tornou editor diplomático ao cobrir o Iraque e a Intifada antes de se mudar para Washington em 2007.

Na viagem, Poitras mostrou a Glenn um outro *pen drive* que recebera de Snowden, em que também continha documentos secretos da NSA, mas, para a surpresa dos dois, eram quatro mil itens. Entusiasmados e eufóricos com o imensurável tesouro que tinham em mãos, eles chegaram a Hong Kong sem mais dúvidas sobre a legitimidade de Snowden. Aquilo tudo era real.

Diante de toda essa realidade, questiona-se em que momento se iniciou o processo de vigilância de usuários em massa. O que motivou essa prática foi o episódio do dia 11 de setembro de 2001 (dia em que ocorreu o maior ataque terrorista que mobilizou todo os EUA) e a conjuntura que se formou a partir daí. Foi criada uma cultura de invasão de privacidade, além de que a tecnologia alcançou grandes avanços que tornaram escutas e ferramentas semelhantes mais viáveis e comuns. A Internet se tornaria, como afirmou Julian Assange, "a maior máquina de espionagem que o mundo já viu". A falha da NSA – maior agência de inteligência dos EUA – em repreender de maneira proativa o esquema da Al-Qaeda (para realização do ataque surpresa contra as Torres Gêmeas) criou um certo trauma e desejo de compensação. A partir disso, parece que a agência iniciou um processo de atividades de espionagem mais rigoroso como forma de compensação pelo acontecido. A NSA foi criada com a proposta de coletar sinais de inteligência pelo mundo, tecnologias como satélites e Internet.

Quando os três jornalistas, Glenn, Poitras e MacAskill chegaram no local onde se encontrava o delator da NSA pelo Guardian, Snowden sabia da gravidade e amplitude da espionagem que estava a um passo de ser revelada e tomava precauções das mais inimagináveis. Os jornalistas perceberam que Snowden se sentia vulnerável, pois até a publicação dos documentos todos eles corriam sérios riscos se fossem pegos com material secreto de uma agência tão poderosa. MacAskill começou a entrevistar Snowden, perguntas básicas sobre como ele havia se envolvido com o trabalho de inteligência, o ano que entrou para o CIA, sua identificação no CIA, a sua missão no Havaí, seu salário e, finalmente, por

que estava em Hong Kong. Snowden explicou sobre esse último ponto que apesar de ser completamente oposta da cultura americana, já que a cidade fazia parte da República Popular da China, ela pregava a liberdade de expressão amplamente.

O relato da vida de Snowden comoveu MacAskill, ele teria chegado à conclusão de que aquilo com certeza era verdadeiro, apesar de muito aventuroso. Assim, Mac estava se questionando sobre a coragem absurda de um rapaz tão jovem como Snowden. Snowden disse que sabia que poderia acontecer coisas terríveis com ele, porém não se arrependeria de nada, pois não queria viver em um mundo onde tudo que se faz e se diz é gravado. MacAskill percebeu então que Snowden era um patriota, acreditava no idealismo. Snowden dizia que o ataque secreto do governo americano era uma ofensa à Constituição, era uma verdadeira ocupação territorial. O maior medo de Snowden era que sua família, que não sabia nada do que estava acontecendo, fosse perseguida, além de seus amigos e sua namorada.

5.1.3 O teor das reportagens e os principais arquivos revelados

A primeira reportagem sobre os programas de espionagem foi realizada pelo americano Glenn Greenwald (quando ele ainda trabalhava no jornal britânico "The Guardian") e publicada no dia 5 de junho. Foi revelado que a Agência Nacional de Segurança monitora ligações telefônicas de milhares de americanos. Além disso, a NSA acessa informações pessoais de aparelhos eletrônicos, como fotos e *e-mail*s, por intermédio de empresas americanas como Facebook e Skype. Havia um mandado secreto da justiça americana que obrigava a empresa de telefonia Verizon a entregar à NSA dados de seus clientes como número e duração de chamadas realizadas dentro dos EUA (para o território nacional ou para outros países) entre os meses de abril e julho de 2013 (PRESSE, 2015)[66].

> As implicações eram enormes. A ordem judicial secreta da Verizon datava de 25 de abril de 2013 e forçava uma das maiores empresas de telecomunicação dos EUA a entregar à NSA os registros telefônicos de milhões de seus clientes norte-americanos. A Verizon estava fornecendo detalhes privados em uma "base diária, recorrente". Estava dando à NSA informações sobre todas as chamadas em seus sistemas, tanto em território americano quanto entre os EUA e outros países. Era uma evidência sensacional de que a NSA praticava uma "pesca de arrasto", recolhendo registros de milhões de cidadãos norte-americanos independentemente de terem cometido ou não algum crime ou de estarem envolvidos com terrorismo. O documento vinha do tribunal da FISA. Assinado pelo juiz Roger Vinson, dava autoridade ilimitada ao governo dos EUA para coletar metadados de telefone por um prazo de 90 dias (HARDING, 2014, p. 103).

[66] http://g1.globo.com/mundo/noticia/2013/07/as-principais-revelacoes-de-edward-snowden.html

Outras fontes também publicaram sobre o vazamento de programas de espionagem nos EUA, como o jornal americano "The Washington Post", em 07 de junho. Tal jornal publicou uma relação de arquivos divulgados por Snowden que expunham um programa de vigilância desenvolvido por grupos de inteligência da Microsoft, Google, Facebook, entre outras empresas do Vale do Silício (G1, 2015)[67].

No dia 08 de junho, o Guardian e o Washington publicaram mais notícias. Surgiram mais revelações. A NSA e o FBI estariam recebendo informações de nove empresas americanas renomadas em serviço de Internet, sobre comunicações de internautas estrangeiros em países de todo o mundo. Snowden havia contatado o Washington Post para entregar documentos, entre eles o PowerPoint que expõe a parceira da NSA com empresas de Internet (como Skype, YouTube, Apple e PalTalk). A NSA estabelecia conexão com servidores dessas empresas através de um portal, e isso foi possibilitado pelo programa secreto PRISM, desenvolvido em 2007. A agência, então, descumpria a lei americana que protege os cidadãos dos EUA contra a violação de dados privados em território nacional. Sem desenvolver as pesquisas devidas, a NSA vigiava pessoas que presumiam estar no exterior sem ordem judicial (PRESSE, 2015)[68].

Quarenta e um slides explicavam toda a sistemática do PRISM, um programa sigiloso que possibilitava à NSA, a coleta de dados diretamente dos servidores de grandes empresas como Google, Facebook, Yahoo, Microsoft, Apple, entre outras. Assim, *e-mail*s, postagens, e demais informações digitais, eram vazados sem a necessidade de mandados judiciais específicos oriundos de um devido processo legal, imbuído de qualquer acusação legítima, apenas com carimbos e aprovações internas sigilosas baseada na Lei de Vigilância. A *Foreign Intelligence Surveillance Act* of 1978 – FISA, revisada em 2008 com a finalidade de reger a vigilância da NSA na missão de identificar atividades terroristas.

> Um slide enfatizava as datas em que empresas de tecnologia do Vale do Silício haviam assumido o compromisso de se tornar parceiras corporativas da agência de espionagem. A primeira a fornecer material ao PRISM foi a Microsoft. A data era 11 de setembro de 2007. Exatos seis anos após o 11 de setembro. Em seguida, vieram Yahoo (março de 2008) e Google (janeiro de 2009). Depois, Facebook (junho de 2009), PalTalk (dezembro de 2009), YouTube (setembro de 2010), Skype (fevereiro de 2011) e AOL (março de 2011). Por razões desconhecidas, a Apple resistiu por cinco anos. Foi a última grande empresa de tecnologia a se inscrever. Ela se juntou em outubro de 2012 – exatamente um ano após a morte de Jobs (HARDING, 2014, p. 163-164).

[67] http://g1.globo.com/mundo/noticia/2015/01/programa-de-espionagem-vazado-por-snowden-esta-ligado-muitos-paises.html

[68] http://g1.globo.com/mundo/noticia/2013/07/as-principais-revelacoes-de-edward-snowden.html

Segundo tal lei, em sua seção 702, a NSA poderia investigar as ligações e *e-mail*s de um cidadão americano por intermédio de um mandato específico. Além disso, tem a obrigação de fornecer ao tribunal FISA seus procedimentos gerais quanto às investigações uma vez ao ano. Os critérios de aprovação da lei eram mínimos e havia a exigência, um tanto subjetiva, de que a vigilância ajudasse a arrecadação legítima de inteligência estrangeira. Realizada a aprovação dos procedimentos fornecidos pela NSA, a agência poderia empreender a vigilância de cidadãos estrangeiros e "intimar" qualquer empresa de telefonia ou Internet a fornecer dados de comunicações de estrangeiros, interceptações de Facebook, *e-mail,* Google etc. Tais operações seriam realizadas sem apresentação de motivos ou uma averiguação de que o alvo poderia ser de fato culpado de algum delito, ou a cautela de selecionar os cidadãos para que norte-americanos não fossem vigiados "por acaso" no processo (BASTOS, 2014, p. 28)[69].

Depois da revelação em escala mundial do escândalo de espionagem, as pessoas finalmente ficaram sabendo a identidade do revelador dos documentos e arquivos que provaram o esquema. Edward Snowden declarou, em entrevista ao "The Guardian" em 09 de junho que não iria se esconder, pois suas ações não tinham nada de errado, muito pelo contrário, ele havia se arriscado por uma causa maior: defender a sociedade americana e ser honesto com o resto do mundo. "Não tenho nenhuma intenção de me esconder porque sei que não fiz nada de errado", disse Snowden. (G1, 2015)[70].

Dias depois, 22 de junho, o jornal China Morning Post, de Hong Kong, publicou uma matéria anunciando que o governo americano pirateava empresas de telefonia chinesas, a fim de apanhar milhares de mensagens de texto. Snowden compartilhou com os jornais que a Universidade Tsinghua de Pequim havia sido pirateada pelos EUA e também a empresa Pacnet (operadora asiática de fibras óticas). Em 31 de julho, uma nova reportagem do "Guardian" revelava o sistema XKeyscore de vigilância, o maior desenvolvido pela NSA, que permitia a agência supervisionar secretamente praticamente todas as ações dos internautas na Internet. A revista alemã N Der Spiegel, informou a partir de documentos entregues por Snowden, que os EUA teriam espionado escritórios da Missão Diplomática da Union European - EU em Washington e nas Nações Unidas, e também da União Europeia em Bruxelas. A revista relatou que o programa era constituído por um sistema infiltrado na rede de informática que possibilitava a espionagem através do acesso a *e-mail*s e outros

[69] http://webcache.googleusercontent.com/search?q=cache:ugj2WpuAUgcJ:https://repositorio.ufsc.br/
[70] ttp://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html

documentos pessoais. Além disso, microfones eram instalados no prédio da UE em Washington. Snowden confirmou que o mesmo perfil de programa era utilizado na América Latina e até mesmo no Brasil (PRESSE, 2015).

O "Washington Post" fez outra revelação sobre a NSA, no fim de outubro, que espalhou mais revolta pelo mundo. A agência de inteligência americana teria invadido secretamente *links* de comunicação que estabelecem conexão com *data centers* do Yahoo e do Google internacionalmente. Com essa ação, a NSA obteve acesso à dados de milhares de usuários. Com a notícia, Eric Schmidt, o chairman do Google se pronunciou dizendo que o fato é ilegal e afrontador se for comprovada sua legitimidade. O jornal voltou a noticiar em dezembro sobre o caso de espionagem informando que até mesmo a geolocalização de celulares ao redor do planeta era monitorada diariamente pelos EUA.

Em meio ao escândalo, vários jornais, de toda parte do mundo (Alemanha, França, Brasil), publicaram notícias e reportagens sobre os vazamentos realizados por Snowden. No começo do ano de 2014, o "The New York Times" defendeu a posição corajosa do jovem Snowden, pedindo clemência pela sua situação em uma publicação de editorial. Logo depois, veio à tona a informação de que instrumentos foram desenvolvidos a fim de burlar proteção de aplicativos para celulares (como o jogo Angry Birds, popular na época) pela NSA e GCHQ (do Reino Unido). Com as ferramentas, os dados dos usuários que possuíam os aplicativos em seus aparelhos eram transmitidos através da Internet. Quando a notícia saiu, os criadores do aplicativo esclareceram não ter qualquer envolvimento no caso. No mesmo período, outra descoberta foi realizada por um novo documento de Snowden divulgado pelo "The Huffington Post". A revelação que deixou as relações diplomáticas dos EUA afetadas foi a de que NSA teria monitorado comunicações de outros governos (antes e durante a Conferência sobre Mudanças Climáticas das Nações Unidas em 2009), violando o princípio da soberania (G1, 2015)[71].

5.1.4 Os precursores de Snowden: Assange, Ellsberg e Manning

O grande poder emanado pelos Estados Unidos reflete segredos em toda sua história. Diante disso, nada mais natural que Snowden não tenha sido o primeiro a vivenciar e delatar vazamentos a respeito da nação americana. Snowden teve precursores que também marcaram a história da manipulação de informações e espionagem estadunidense. Um deles foi Daniel

[71] ttp://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html

Ellsberg, economista formado em Harvard, e, também, marine com estágio no Vietnã. Ellsberg realizou um trabalho no Pentágono durante a Guerra do Vietnã durante o qual se indignou com as visíveis distorções entre o que o governo declarava e os dados a que ele tinha acesso pelo seu ofício. Na época, o governo dizia que estava desacelerando o investimento em recursos bélicos para pôr fim ao conflito e, em vez disso, estava dobrando os investimentos para conter as derrotas. Ellsberg desejava divulgar suas descobertas à população, porém tinha medo da reação dessa sobre a veracidade das informações e do poder dos órgãos do Estado que poderiam agir contra ele. Resolveu, então, copiar cerca de 7 mil documentos e divulgar clandestinamente aos jornais mais importantes como o New York Times. Este travou uma guerra com o governo após as publicações, mas conseguiu a liberdade de expressar as notícias à população. Logo depois, o analista foi descoberto e respondeu um processo sobre sua traição, conseguindo ser absolvido com o apoio de progressistas e vários críticos do seu país. Sua alma ativista e sua história (que inclusive inspirou alguns filmes) de luta pela paz, conquistou pessoas de todo o mundo, e ele continua a se envolver na luta por um mundo mais justo e honesto até os dias atuais (GALVÃO, 2015)[72].

Julian Assange foi outro delator memorável na história americana. O jornalista e ciberativista australiano é um dos nove membros do conselho do WikiLeaks (site de denúncias e vazamento de informações sigilosas), seu fundador e porta-voz. Ganhou vários prêmios pela habilidade informática e seu trabalho no *website*. Em 2010, houve um grande vazamento através do WikiLeaks de documentos que declaravam crimes de guerra cometidos na Guerra do Afeganistão e na do Iraque pelo Exército norte-americano e outras informações secretas dos EUA. Um mês depois desse episódio, a Justiça da Suécia expediu dois mandatos de prisão contra Assange por estupro e por agressão sexual sem apresentação de acusações formais. Com isso, corria o risco de ser extraditado para a Suécia e depois para os EUA e, assim, processado nos EUA por espionagem e fraude, por conta dos 250 mil documentos publicados a respeito de informações diplomáticas norte-americanas. Investigadores acreditam que o delator tenha sido vítima de armadilha provocada por serviços de inteligência do Governo. Tempos depois, em 2012, a corte suprema do Reino Unido anunciou decisão a favor da extradição de Assange para a Suécia. Em julho do mesmo ano, ele se refugiou na embaixada do Equador em Londres, a fim de obter asilo político. O Equador deu o asilo, porém o Reino Unido negou a concessão do visto para que ele pudesse sair do país. Temendo

[72] http://jornalggn.com.br/noticia/assange-snowden-e-ellsberg-por-walnice-nogueira-galvao

ser extraditado para a Suécia vive há três anos na embaixada sem poder sair em nenhuma hipótese (GOODMAN, 2015).

Outro importante delator, o jovem Bradley Manning, nascido em Crescent e soldado que trabalhava como analista de inteligência no Iraque e por isso possuindo contato com informações sigilosas, entregou documentos secretos dos EUA (cerca de 700 mil, envolvendo comunicações diplomáticas) para o site de vazamentos WikiLeaks. Esse vazamento ocasionou um forte tumulto na diplomacia mundial e a revolta das autoridades estadunidenses. Acusado em 2010 por uma série de crimes como espionagem e roubo, Manning foi sentenciado a 35 anos de prisão (G1, 2013)[73].

5.1.5 Repercussões do caso no Brasil e no mundo

A espionagem praticada pela agência de inteligência norte americana, com o aval do governo, tinha como premissa maior o combate ao terrorismo, fundamento que dava legitimidade a tal função. Não obstante, é necessário salientar que a utilização das tecnologias de coleta de dados, para fins de segurança e defesa das nações é, sim, relevante, mas é necessário que haja fundamento jurídico, sensatez e equilíbrio para que não se transforme numa afronta aos direitos mais básicos da personalidade.

A invasão e violação da privacidade, em seus mais variados níveis, pela NSA, tornaram-se uma constante. Por isso, Snowden passou a questionar o que seria ou não justo, quais ações eram certas, quais eram fruto do erro, qual melhor decisão tomar. Ele se deparou com dilemas de cunho ético. Um Estado pode executar determinadas medidas para se salvaguardar de investidas terroristas? Até que ponto? De qualquer modo, tal compromisso com a pátria não pode ter uma conotação que visa, também, proteger e assegurar a hegemonia política e econômica?

A publicação da coleta de dados em massa que resultou no maior vazamento de informações das Agências de Segurança Nacional norte-americana e britânica deu início a um recorrente debate mundial acerca dos limites e das novas formas de violação a um dos principais direitos fundamentais da personalidade que é a privacidade (GLENN; MACASKILL; POITRAS, 2013)[74]. Nesse raciocínio, houve importantes repercussões das revelações feitas por Snowden em várias partes do globo, que implicaram discussões e desdobramentos políticos, sociais, econômicos e jurídicos.

[73] http://g1.globo.com/mundo/noticia/2013/08/entenda-o-caso-de-bradley-manning-condenado-por-vazar-segredos.html
[74] http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Edward Snowden foi responsável pela revelação do programa de coleta de dados executado pela Agência de Segurança Nacional norte-americana, fato que provocou o debate acerca das novas formas de violação ao direito fundamental à privacidade, que demonstra a necessidade de adequação do Direito às novidades aportadas pelas constantes inovações tecnológicas.

Foram iniciadas discussões no Congresso norte-americano para limitar o poder de vigilância e monitoramento da NSA, além disso, muitos cidadãos de várias partes do mundo começaram a pressionar as grandes empresas de tecnologia de informação para que deem mais garantia e segurança aos consumidores, oferecendo produtos criptografados e serviços mais seguros.

O ex-analista da NSA também revelou que as comunicações pessoais da presidente Dilma Rousseff, seus assessores, as tratativas da empresa brasileira Petrobrás, além de outras organizações e cidadãos que utilizam a rede mundial de Internet foram alvo de espionagem. Os EUA ao espionar o sistema brasileiro visava obter informações de países não aliados como a China e o Irã (GREENWALD; KAZ; CASADO, 2013)[75].

Em relação ao Brasil, inicialmente houve um posicionamento de indignação frente ao governo dos EUA. A Presidente Dilma Roussef pediu explicações, os Estados Unidos negaram as denúncias de espionagem, e tal fato acelerou a aprovação do Marco Civil da Internet. Roussef também suspendeu uma visita de Estado a Washington agendada para outubro de 2013 (G1, 2015). Foram realizadas algumas investigações iniciais pelo Ministério da Defesa e pelas Forças Armadas para averiguar se o sistema de criptografia relativo a assuntos estratégicos do país havia sofrido invasão, mas os Estados Unidos negaram as denúncias de espionagem.

No Congresso, foi aberta uma Comissão Parlamentar de Inquérito, criada para proceder à investigação do monitoramento, solicitando, inclusive, o depoimento do jornalista Glenn Greenwald (DINIZ, 2013)[76]. Alguns debates envolveram jornalistas, professores, políticos. O Ministro das Comunicações, Paulo Bernardo ressaltou a possibilidade de ter havido vazamento de algumas conversas realizadas cotidianamente pelo governo brasileiro:

> O governo tem redes corporativas seguras, redes onde nós transitamos as nossas informações, documentos, atos que precisam ser tomados pelo governo e nós não temos problema. Agora, aquilo que nós colocamos na rede e a forma pela qual nós nos comunicamos, por exemplo, a presidenta Dilma me liga seguidamente e liga no meu celular. Ela, nesse momento, está se comunicando com a mesma condição de

[75] http://oglobo.globo.com/mundo/eua-espionaram-milhoes-d*e-mail*s-ligacoes-de-brasileiros-8940934
[76] http://observatoriodaimprensa.com.br/caderno-da-cidadania/o_caso_snowden_e_a_espionagem_que_chegou_ao_brasil/

> qualquer cidadão. Se todo esse rastreamento está acontecendo, então, é evidente que essa ligação também vai ser abrangida (DINIZ, 2013).

Apesar disso, atualmente, a relação entre o governo brasileiro e norte-americano está estável. Entretanto, para evitar a espionagem do governo americano, a nação brasileira está planejando junto à União Europeia a instalação de um "cabo submarino" exclusivo de comunicação entre as cidades de Fortaleza e Lisboa. A presidente Dilma Rousseff objetiva reduzir a dependência entre o Brasil e os EUA nas relações internacionais. Segundo ela, o investimento de quase 185 milhões seria necessário para garantir a neutralidade da rede, além da democracia e liberdade de expressão e o respeito à privacidade e à soberania (CANALTECH, 2015,)[77].

Além da urgência na tramitação do Marco Civil, alguns juristas e especialistas na área de Direito Digital, como Luiz Moncau, expressaram a necessidade de trabalhar outros projetos de lei que tratam sobre o assunto, a exemplo do que se refere à proteção dos dados pessoais. Considerável número de nações já tem leis específicas sobre a matéria, além de organismos e agências que desempenham funções protetoras dos dados, salvaguardando, em especial, os consumidores de instituições que possam praticar abusos.

Os Estados Unidos são o protagonista do esquema revelado por Edward Snowden. No entanto, em menor potencialidade, outros governos também praticam a espionagem. E, como foi delatado, com o auxílio de grandes empresas privadas que recebem pela colaboração. O jornalista Caio Túlio, em entrevista, esclareceu que empresas do Vale do Silício, como o Facebook e o Google, por meio do histórico, têm capacidade para construir perfis dos vários internautas e direcionar projetos publicitários destinados aos interesses dos usuários. Há o armazenamento dos dados dos usuários que viram objeto de negociação. Tal fato é uma espécie de invasão de privacidade, mas como o internauta aceita o disposto pelos ditames do facebook, torna-se legal, mas o monitoramento ocorre.

As informações de Snowden revelaram que os Estados Unidos tiveram acesso às comunicações pessoais de alguns líderes aliados, dentre eles a chanceler alemã, Angela Merkel. Em janeiro de 2014, o presidente Obama ordenou o fim da espionagem a lideranças de nações aliadas, mas informou que a agência de inteligência ainda estaria coletando informações sobre alguns os governos estrangeiros, por questão de segurança. Em março, do mesmo ano, o Presidente divulgou um plano formal de diminuição do controle governamental dos dados telefônicos que passariam a ser monitorados pelas companhias telefônicas por um período máximo de 18 meses.

[77] http://canaltech.com.br/noticia/espionagem/Brasil-e-Europa-terao-cabo-de-comunicacao-para-fugir-da-espionagem-dos-EUA/

Tais dados só poderiam ser objeto de acesso pela NSA quando houvesse suspeitas plausíveis de que o número observado tivesse alguma relação com terroristas e por meio de autorização específica da The Foreign Intelligence Surveillance - FISA (Lei de Vigilância de Inteligência Estrangeira).

Depois das revelações muitos usuários começaram a utilizar a criptografia para proteger dados. A criptografia é um conjunto de técnicas que tem o objetivo de codificar uma certa informação sigilosa. Sua nomenclatura é originária do grego e significa "escrita oculta". Com a codificação realizada por ela, somente o emissor e o receptor podem acessar tal informação, impedindo que um terceiro "intruso" consiga decifrá-la. Conforme há a renovação e o aperfeiçoamento das tecnologias, as técnicas de criptografia vão tornando cada vez mais seguras. No meio virtual, a técnica mais conhecida é a chave criptográfica (ROMAGNOLO, 2015)[78].

Por meio da criptografia, os internautas podem ter uma navegação mais segura. O remetente envia ao destinatário a mensagem de um modo que só este tem a chave, decodifica e consegue ler, entretanto a grande maioria dos usuários não tem costume de usar, desconhece ou não se interessa pela proteção, deixando os dados desprovidos de codificação.

A intensidade dos debates impulsionou o governo dos EUA a limitar o poderio dos serviços de espionagem realizados pela NSA. Muitas instituições europeias foram contrárias a atividades de espionagem consideradas ilegais e buscaram restringir as funções de inteligência que violassem direitos civis básicos. No entanto, muitos ataques cibernéticos continuam sendo feitos contra os Estados Unidos, possivelmente vindos da China e da Rússia, mas é premente que se busque um equilíbrio entre segurança e privacidade (NAÍM, 2015).

Em vista da grande repercussão causada pela ofensiva invasão de privacidade cometida pela NSA dos EUA contra milhares de cidadãos, o presidente Barack Obama promulgou uma lei que representa um vitorioso avanço quanto à questão do direito à privacidade. A USA Freedom Act (como é conhecido o novo dispositivo legal) determina que as agências do Governo dos Estados Unidos não podem reter informações de todas as comunicações dos cidadãos do país sem a devida justificação legal. O próprio Snowden alerta que, apesar de ser um progresso e um marco na história do direito à privacidade do país, necessita-se de uma reforma mais profunda para que a segurança seja retomada concretamente (MARTINS, 2015)[79].

[78] https://www.oficinadanet.com.br/artigo/443/o_que_e_criptografia
[79] Disponível em: <http://www.publico.pt/mundo/noticia/nova-lei-sobre-espionagem-nos-eua-e-um-primeiro-passo-para-reformas-profundas-1697825

Todo o aparato prévio de espionagem, segundo pesquisa realizada pela própria Casa Branca, não impediu a ocorrência de ataques terroristas. As Nações Unidas reconheceram e proclamaram que a vigilância em massa constitui uma afronta aos direitos humanos e o Conselho da Europa solicitou a promulgação de novos diplomas legais que proíbam a perseguição àqueles que denunciam as ilegalidades. Na seara técnica, novos programas e dispositivos estão sendo criados, outros revistos e a criptografia começa a ser utilizada com mais intensidade. Os usuários da rede mundial, por meio dessas transformações de cunho tecnológico, buscam a proteção contra as arbitrariedades que violam o direito sagrado à privacidade.

Numa espécie de carta para o mundo, Edward Snowden revela:

> [...] Em meu foro íntimo, houve momentos em que me preocupei com a possibilidade de que tivéssemos posto em perigo, por nada, as nossas vidas privilegiadas, de que a opinião pública reagiria com indiferença ou adotasse uma atitude de cinismo ante as revelações. Nunca agradeci o suficiente por ter me enganado tanto. Eis que dois anos depois a diferença é profunda. (...) Embora tenhamos percorrido um longo caminho, o direito à privacidade –fundamento das liberdades consagradas na Carta dos Direitos dos Estados Unidos – continua sob ameaça por parte de outros programas e autoridades. Alguns dos serviços online mais populares do mundo foram recrutados como colaboradores dos programas de vigilância maciça da Agência Nacional de Segurança e as empresas de tecnologia recebem pressões de Governos de todo o mundo para que trabalhem contra seus clientes, em vez de agirem em seu favor. [...] Nós ficamos cientes de que nosso Governo enfraquece de modo intencional a segurança fundamental da Internet por "portas traseiras" que transformam as vidas privadas em livros abertos. [...] Fora dos Estados Unidos, os encarregados da espionagem da Austrália, Canadá e França aproveitaram tragédias recentes para tentar obter novos poderes invasivos, apesar dos esmagadores indícios de que tais autoridades não teriam impedido de modo algum os ataques. [...] Ao iniciar o novo milênio, poucos imaginavam que os cidadãos das democracias desenvolvidas não tardariam em ver a necessidade de defender o conceito de sociedade aberta contra seus próprios dirigentes. Mas o equilíbrio de poder está começando a mudar. Estamos presenciando o aparecimento de uma geração posterior ao terror, uma geração que rejeita uma visão de mundo definida por uma tragédia singular. Pela primeira vez desde os atentados de 11 de setembro de 2001 é possível vislumbrar uma política que se afasta da reação e do medo em favor da resiliência e da razão. Com cada vitória nos tribunais, com cada mudança na lei, estamos demonstrando de novo que o valor de um direito não reside no que ele esconde, mas no que protege (SNOWDEN, 2015)[80].

Dentro desse novo contexto jurídico-tecnológico, é necessário procurar uma equilibrada adequação do Direito ao uso das inovações tecnológicas por parte dos Estados para que haja um maior respeito e garantia à vida privada dos cidadãos, instituições e nações.

Após os escândalos de espionagem delatados por Snowden, ele se tornou um dos homens mais procurados do mundo e ficou na zona de trânsito do aeroporto Sheremetyevo,

[80] http://g1.globo.com/mundo/noticia/2015/01/programa-de-espionagem-vazado-por-snowden-esta-ligado-muitos-paises.html

em Moscou. Porém, em agosto de 2013, Snowden recebeu asilo temporário de 1 ano da Rússia com a condição de que parasse de vazar os segredos dos EUA, proposta que foi aceita por ele. Na época, o governo norte-americano se revelou indignado com a decisão russa e considerou desmarcar uma reunião com o governo (IG, 2014)[81]. Todavia, a lei internacional protegeu Snowden que vive na Rússia até os dias atuais, e o asilo foi renovado por mais três anos em agosto de 2014.

Após o relato descritivo do caso Snowden e toda a gama de repercussões no mundo, e especialmente no Brasil, serão delineadas algumas iniciativas do governo no tocante à Cibersegurança brasileira.

5.2 CIBERSEGURANÇA

O termo Cibersegurança ganhou visibilidade e motivou debates em 1990 nos Estados Unidos, e em outras potências mundiais, movidos pela Revolução da informação. Verificou-se a necessidade de políticas de segurança e ferramentas similares para combater a criminalidade no meio virtual que surgia com o avanço tecnológico e a crescente utilização da Internet.

Segundo a Comissão Europeia, o vocábulo em questão abrange:

> [...] as precauções e ações que podem ser utilizadas para proteger o ciberespaço, tanto nos domínios civil como militar, contra as ameaças decorrentes da interdependência das suas redes e infraestruturas informáticas ou que as possam danificar. A cibersegurança procura manter a disponibilidade e a integridade das redes e infraestruturas e a confidencialidade das informações nelas contidas (COMISSÃO EUROPEIA, 2013 apud SANTOS).[82]

A palavra Cibersegurança significa a reunião de tecnologias de defesa de computadores redes, programas, softwares e dados, potenciais alvos de invasão danosa, dos ciberataques. Visando a essa proteção, e analisando a gravidade dos impactos que os ciberataques podem ocasionar à economia e à política de um Estado, às empresas e aos indivíduos de forma geral, os governos estão incentivando as pesquisas na área da Cibersegurança e implantação de medidas técnicas e políticas de proteção ao ciberespaço.

> As políticas de segurança são compostas de um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações e serviços importantes para

[81] http://g1.globo.com/mundo/noticia/2015/01/programa-de-espionagem-vazado-por-snowden-esta-ligado-muitos-paises.html
[82] http://segurancaecienciasforenses.com/2013/10/28/ciberdefesa/

> uma determinada empresa recebam a proteção conveniente, de modo a garantir a sua confidencialidade, integridade e disponibilidade. Uma política de segurança de informação tem como propósito, fornecer orientação e apoio às ações de gestão de segurança (CARVALHO, 2005, p. 55).

O objetivo da Cibersegurança reside, então, na proteção dos Sistemas de Informação e Comunicações da Defesa Nacional contra ciberataques, no apoio à atuação proativa do Estado (conforme seu interesse geral e o bem comum) e no ciberespaço quando se verifica que esse foi utilizado de maneira inadequada/com destinações criminosas (SANTOS, 2013).

Desse modo, medidas protetivas no âmbito da cibersegurança são, na atualidade, urgentes e necessárias, pois os sistemas prioritários de um país dependem da manutenção da segurança tecnológica, uma vez que as instituições e os principais serviços estatais estão ligados e interconectados à grande rede mundial.

5.2.1 Ciberespionagem e Cibersegurança

O Diretor-redator da Revista Linux, ao falar sobre a temática Segurança da Informação, equiparou os profissionais de TI a alguns profissionais da área de saúde, que, muitas vezes, são omissos, deixam de seguir protocolos importantes e acabam pondo em risco a saúde de muitos. No caso do Ebola, por exemplo, ele explica que o primeiro surto ocorreu em 1976, mas só agora, depois que saiu da África e veio para os Estados Unidos, é que resolveram providenciar o medicamento adequado. Dois projetos importantes (plataformas Unix- Linux) Heartbleed (no projeto OpenSSL) e Shellshock, (Bash) interpretadores de comandos mais utilizados no mundo Linux foram alvo de vulnerabilidades, de falhas em sua implementação e viraram notícia. Segundo Silva:

> Essas falhas de implementação serviram para levantar novamente paralelos entre ciência médica e tecnologia. A falha no projeto OpenSSL foi introduzida no código fonte da biblioteca no último dia de 2011 por um de seus principais desenvolvedores, tendo sido descoberta apenas mais de três anos depois, em abril de 2014. A falha no código do Bash está disponível desde a sua versão 1.03, lançada em setembro de 1989 – i.e., há 25 anos! Assim, da mesma forma que patógenos podem ficar anos esperando por condições adequadas para se alastrar, com certeza há um sem-número de falhas de implementação "escondidas" em programas, esperando para ser descobertas e devidamente exploradas. [...] Tanto na biologia quanto na tecnologia, é questão de tempo para aparecer um organismo com altíssimo poder de alastramento e altíssima taxa de letalidade. Na biologia, a Gripe Espanhola de 1918 é um exemplo recente de que isso até já ocorreu, matando entre 3% e 5% da população mundial à época! Ainda teremos desastres similares na TI, mas que podem ser minimizados com o uso de ferramentas adequadas – SELinux (MAC), AppArmor (DAC), IPS/IDS, firewalls etc. – e melhores práticas de segurança da informação – controle do ciclo de vida de pessoal, uso e auditoria de sistemas, Open

> Source, testes de invasão, programação segura etc. Previna-se! (SILVA, S.M.L., 2014)[83].

Desse modo, pode-se concluir que a segurança cibernética, assim como os assuntos relacionados à saúde e vigilância sanitária, são temáticas a exigirem uma atenção urgente, não podem ser preteridas em razão da grave lesão que pode afetar várias nações, especialmente por meio da ciberespionagem, de ciberataques a grandes instituições (com segredos industriais), quais sejam: sistemas e redes de dados dos órgãos, militares e civis, que compõem a defesa nacional, e a população como um todo. Para a proteção e defesa das nações, imperioso se faz a adoção de diretrizes estratégicas em cibersegurança, investindo nesta nova área, já que a possibilidade da existência de uma ciberguerra, não é tema apenas de filmes na modalidade ficção. Trata-se de uma possibilidade real, especialmente em tempos de ciberespionagem.

A ciberespionagem e a espionagem possuem características muito similares. Apenas aspectos ínfimos as diferenciam. A ciberespionagem pode ser considera como uma subcategoria da espionagem. Ela teve seu surgimento atrelado à adaptação às transformações dos últimos anos (em decorrência da globalização e do avanço contínuo da tecnologia). Apesar de possuírem finalidades análogas (obter proveito nas relações comerciais, políticas, militares, etc), a particularidade da ciberespionagem diz respeito ao espaço onde ela se constitui. Esse é o ciberespaço, a rede virtual, que proporciona oportunidades inúmeras nesse aspecto, já que rompe as barreiras geográficas e possibilita um acesso, instantâneo e de amplo alcance, à informação. Trata-se de uma espionagem aprimorada, que dispõe de técnicas e ferramentas mais evoluídas.

Todas estas preocupações têm fomentado esforços no sentido de se elaborarem estratégias de cibersegurança e de mobilizar a cooperação internacional, pois é neste sentido que se julga também estar boa parte das soluções, especificamente no que concerne ao combate à ciberespionagem.

A legislação nacional brasileira, no que se refere à espionagem, é defasada, além de ter sido criada num contexto político de exceção. A Lei de Segurança Nacional (lei nº 7.170/83) tutelava a política interna do país na era da guerra fria e da bilateralidade entre comunismo e capitalismo.

---

[83] http://comum.rcaap.pt/bitstream/123456789/8750/1/Ciberespionagem%20no%20Contexto%20Portugu%Silva.pdf

> A derradeira tentativa conhecida de aplicação da Lei de Segurança Nacional ocorreu há cerca de sete anos, quando mais de cem integrantes do Movimento de Libertação dos Sem Terra (MLST) depredaram dependências da Câmara e foram presos acusados de crime político. Entretanto, a defesa da integridade de um Estado democrático não pode se limitar à repressão de ações ilegais de grupos nacionais que atingem somente a chamada segurança interna, como a danificação de bens públicos e privados (ZAMPRONHA, 2013, p. 2)[84].

O mundo globalizado alcançou características próprias como a interdependência, que necessita de uma preparação para prevenir as novas ameaças que vêm com as transformações. Diante dessa conjuntura, é imprescindível o fortalecimento do sistema de segurança (contra inteligência). É necessário que o país seja proativo para evitar as ameaças e desenvolver ações eficazes para salvaguardar as informações particulares das pessoas, empresas e agências, muitas vezes, alvos de interesses externos por executarem importantes funções associadas a política, economia, etc. Além disso, é primordial expandir políticas corporativas internas (como treinamentos e conscientização da equipe), e dar a devida importância às medidas de segurança (CORRÊA, 2013).

Na atual era tecnológica, em tempos de ciberataques, um país necessita defender sua segurança interna e externa, protegendo as informações de instituições nacionais públicas e privadas, além de seus cidadãos, de modo geral. Até mesmo porque a tendência é o progressivo agravo do problema, já que no contexto atual, todos estão conectados através das numerosas tecnologias, telefones, *smartphones*, redes, laptops, *tablets*, etc. Esses ambientes virtuais podem se tornar facilmente ferramentas dos cibercriminosos. Em 2020, 50 bilhões de dispositivos estarão conectados à Internet, alvos potenciais crescentes, que demonstram que "A aterrorizante vulnerabilidade de segurança de uma pessoa é a arma secreta de outra" (ELAZARI, 2015, p. 58).

A nação brasileira necessita de um aparato jurídico estratégico que proporcione maior proteção às informações e dados de empresas, do Estado e dos indivíduos. É necessário também, um arcabouço legal atualizado e condizente com os novos crimes virtuais para proteger o país da violação de segredo industrial ou de qualquer ameaça à soberania nacional.

5.2.2 Novas Diretrizes em Cibersegurança no Brasil

A espionagem norte-americana praticada pela "National Security Agency" e pela correspondente britânica "Government Communications Headquarters" (GCHQ) representou

[84] http://www.conjur.com.br/2013-set-08/luis-flavio-zampronha-brasil-adotar-leis-espionagem-internacional1

simbolicamente uma violação explícita da soberania de nações e da privacidade de instituições e cidadãos em várias partes do mundo.

A presidente Dilma, na 68ª Assembleia Geral da ONU, em 2013, explicitou em seu discurso de abertura, que:

> [...] imiscuir-se dessa forma na vida de outros países fere o Direito Internacional e afronta os princípios que devem reger as relações entre eles, sobretudo, entre nações amigas. Jamais pode uma soberania firmar- se em detrimento de outra soberania. Jamais pode o direito à segurança dos cidadãos de um país ser garantido mediante a violação de direitos humanos e civis fundamentais dos cidadãos de outro país (PORTAL BRASIL, 2013)[85].

Após o vazamento das informações de espionagem, algumas medidas começaram a ser tomadas pelo governo brasileiro sobre o assunto. Uma visita oficial aos EUA foi adiada, o Brasil e a Alemanha (ambos vítimas da espionagem dos EUA) apresentaram a ONU uma proposta da "criação de nova arquitetura de controle da Internet". A proposta gerou a aprovação de uma resolução sobre direito à privacidade e temas afins, inclusive na Internet, na chamada Terceira Comissão da ONU. Foi uma vitória expressiva no cenário internacional. A partir dessa situação, a Rússia declarou apoio ao Brasil e à Alemanha pela proposta apresentada, e o ministro Celso Amorim destacou a importância da união das nações sul-americanas (como Argentina e Brasil) para o estabelecimento de uma estratégia conjunta e forte na defesa cibernética. Isso, apesar da posição contrária dos EUA e aliados, que tentam destituir a iniciativa de proposta discutida anteriormente.

Internamente, o governo reconheceu a seriedade da questão de segurança cibernética e promoveu algumas ações concretas a respeito do tema. Nota-se um avanço gradual desde 2000, quando foi instituído o Comitê Gestor de Segurança da Informação (CGSI) – atrelado ao Conselho de Defesa Nacional, a Estratégia Nacional de Defesa (2008), em seguida, a fundação do Centro de Defesa Cibernética do Exército (CD Ciber, 2010/2011), depois o Plano Nacional de Defesa Cibernética (2012) instaurando especificamente para as operações realizadas nos chamados "Grandes eventos", com (Rio+20), seguida da Copa das Confederações (Copa Conf 2013), da Jornada Mundial da Juventude (JMJ 2013) e da Copa do Mundo de Futebol (FIFA 2014). Tal ciclo finaliza-se em 2016, com a realização dos Jogos Olímpicos e Paralímpicos. Em razão de o país ter sediado eventos de grande repercussão mundial, pela primeira vez, um planejamento operacional militar foi realizado, levando em consideração as ameaças advindas do espaço cibernético.

[85] http://www.brasil.gov.br/governo/2013/09/brasil-mantem-tradicao-e-abre-a-68a-assembleia-geral-da-onu

No entanto, foi após as denúncias de espionagem norte-americana anunciadas em 2013, por Edward Snowden, sendo alvo vários países, dentre eles o Brasil, que a segurança virtual e defesa cibernética foram sendo discutidas com bastante ênfase, tanto na esfera civil quanto na esfera militar. Após tais revelações, a Administração Federal Brasileira promoveu algumas ações concretas (em 2015) a respeito do tema, dentre elas: a criação da Portaria de número 2.777 do Ministério da Defesa, do dia 27 de outubro de 2014, que define diretrizes a serem seguidas para defender o ciberespaço; a criação do Comando de Defesa Cibernética (ComDCiber) e da Escola Nacional de Defesa Cibernética (ENaDCiber). Conforme o texto da portaria: "Esta diretriz tem como objetivo definir responsabilidades sobre a implantação das medidas que visam a potencialização da defesa cibernética nacional, de acordo com os seguintes encargos [...]". A portaria define uma série de especificidades, atribuições de órgãos como Secretaria Geral, o Exército Brasileiro quanto às providências de aplicação, propostas, implantações, organizações, etc. Quando implementadas tais disposições, espera-se a redução das vulnerabilidades do ciberespaço, tornando-o menos sujeito aos ataques de espionagens cibernéticas (CONCEIÇÃO, 2015)[86].

Outra tentativa de defesa cibernética é a do "Mapa Estratégico da Segurança da Informação e da Segurança Cibernética 2015-2018", lançado este ano pelo Gabinete da Presidência da República. Constitui um documento detalhado sobre atribuições de órgãos de Estado, e exposição de possíveis contribuições sociais para a elaboração dessas políticas. O mapa reflete a visão crítica de gestão para o setor de segurança e defesa que o Brasil vem adquirindo, e um rigor do poder público quanto ao tratamento da questão. Ele vai ajudar a destrinchar as políticas corretas e integradas para os casos (bastante complexos) a serem resolvidos, disseminando-as na estrutura da organização social. Na elaboração do Mapa, o CGSI abordou indicadores coletados pelo Tribunal de Contas da União-TCU para alertar a população. Esses são bastante alarmantes, como o fato de que 80% das redes apresentam falhas em mecanismos de continuidade dos negócios, 70% exibem falhas no controle do acesso, entre outros. A iniciativa é válida e certamente eficiente, apresentando práticas estratégicas (como desenvolvimento do algoritmo criptográfico proprietário, identificação de população de Empresas Estratégicas de Defesa), porém precisa-se rever as vulnerabilidades de gestão de empresas e órgão públicos (retratados pelo próprio mapa) (FRANGOLA, 2015).

Verifica-se que o sistema de inteligência brasileiro, apesar de muitos avanços na área, ainda precisa adequar-se, de fato, ao novo mundo globalizado e ultra tecnológico, aplicando-

[86] http://dgei.ufrj.br/images/Monografias/TCC-LUIZ-FELIPE-CONCEICAO.pdf

se e investindo-se em pesquisas, além de ampliar o conhecimento e trabalhar de modo estratégico no cerne da cibersegurança. É necessário um plano multilateral que possa preparar a nação contra as ameaças, ataques e invasões virtuais. Assim, a implementação concreta de diretrizes estratégicas que defendam os ativos de organizações, pessoas e a própria administração pública brasileira é imprescindível, uma questão de urgência estatal. No entanto, antes de qualquer ação específica no tocante à cibersegurança, faz-se necessário um processo reeducativo que envolva escolas, pequenas, médias e grandes empresas, municípios, estados e a capital federal, seus organismos como um todo. Medidas eficazes de segurança dependem, antes de mais nada, de informação, educação e conscientização. Somente agindo dessa forma, a segurança informacional e cibernética poderão ser defendidas e protegidas com mais estratégia e eficácia, ou seja, de modo complexo e conglobante.

6 DA GESTÃO JURÍDICO-ESTRATÉGICA NO COMBATE AOS CIBERCRIMES

Esta parte inicial do capítulo apresenta, alguns pontos importantes sobre a utilização da Internet na atualidade, um panorama englobando dados em nível mundial e nacional. Em seguida, alguns comentários pertinentes acerca do Direito na atualidade, em razão da globalização e de como isso se reflete no conceito de soberania, especialmente no momento de definir a competência e a jurisdição dos crimes cibernéticos. Depois, de modo breve, alguns exemplos de ciberataques no mundo e sua nocividade. Serão abordados também, alguns aspectos referentes ao processo investigatório dos crimes cibernéticos, seus procedimentos, suas dificuldades e avanços. E, por fim, serão trabalhadas as diretrizes da gestão jurídico-estratégica no enfrentamento dos Cibercrimes, os desafios e perspectivas

6.1 A AMPLIAÇÃO DAS INTERCONEXÕES E O CRESCIMENTO DOS CIBERATAQUES

Segundo a União Internacional de Telecomunicações (UIT), 57,6% da população brasileira já tem acesso à Internet. O país evoluiu significativamente nos últimos anos e tem sido elogiado por suas políticas de popularização do acesso, mas ainda permanece abaixo dos padrões de países desenvolvidos. A Internet móvel foi o que fez com que o país subisse no *ranking*, alcançando a 27ª posição. Já a conexão fixa não conseguiu acompanhar o ritmo mundial, fazendo-o cair (AMARAL, 2015)[87].

Na região Norte, predomina o uso de celular para acesso à Internet (75,4%). Isso se dá pelo fato de que lá é a única região do Brasil em que a conexão via banda larga móvel (3G e 4G) ultrapassou a rede fixa. O paradoxo vem através de Rondônia, que foi o estado que registrou a maior proporção de acesso exclusivo por meio do computador (61,1%). No Sul, Santa Catarina teve o menor percentual de acesso exclusivo por celular ou tablet (5%). No resto do Brasil, ainda predomina o uso do computador. (BARRUCHO, 2015).

Uma iniciativa brasileira que vem sido elogiada é a pretensão de implementar o Plano Nacional de Banda Larga 2.0 (também chamado de "Banda Larga para Todos" até 2018. A proposta planeja instalar, em todo o país, uma conexão que alcance a velocidade de 25 mbps.

[87] http://exame.abril.com.br/tecnologia/noticias/seis-em-cada-dez-pessoas-ainda-estao-offline-no-mundo

Tabela 1 - Acesso por celular e *tablet*

Estados em que o acesso feito exclusivamente por celular ou tablet superou o feito por computador		
Estado	**Feito por celular ou tablet**	**Computador**
Sergipe	28%	19,3%
Pará	41,2%	17,3%
Roraima	32%	17,2%
Amapá	43%	11,9%
Amazonas	39,6%	11,1%

Fonte: Barrucho, 2015[88] (adaptação da autora, 2015).

A forma de acesso, porém, apresenta variações, como mostrado na TAB. 2:

Tabela 2 - Formas de acesso e suas variações

Formas de acesso à Internet (Fonte: IBGE)	
Banda larga móvel	78,1
Banda larga fixa	11,5
Outros/não possuem nenhum	10,4

Fonte: Barrucho, 2015 (adaptação da autora, 2015).

Os dispositivos móveis vêm conquistando o público brasileiro, causando uma pequena queda na parcela da população que utilizou o computador para navegar, como mostrado abaixo:

Tabela 3 - Uso do computador para navegar na Internet

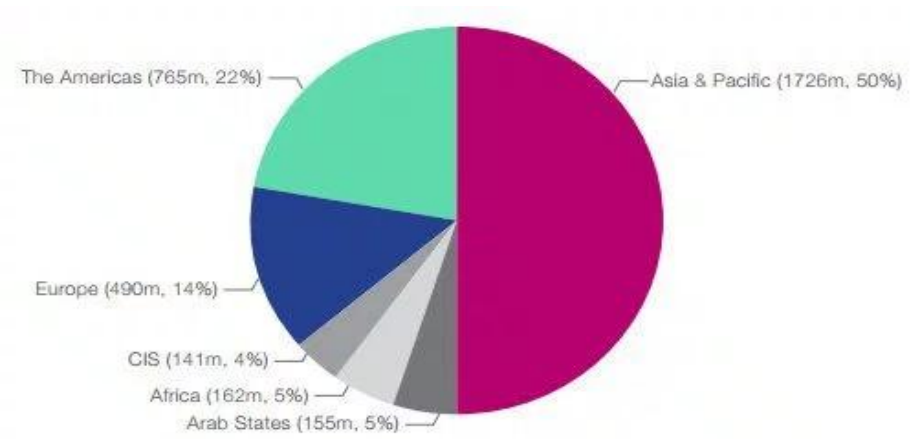
Uso do computador para navegar na Internet	
2011	46,5%
2013	45,3%

Fonte: Barrucho, 2015 (adaptação da autora, 2015).

[88] http://www.bbc.com/portuguese/noticias/2015/04/150429_divulgacao_pnad_ibge_lgb

Em relação aos acessos de banda larga móvel no mundo, a União Internacional das Telecomunicações - UIT estima que metade deles é feita na região da Ásia/Pacífico – cerca de 1.726 bilhões. As Américas vêm em seguida, com 765 milhões. Por último, estão os Estados Árabes, com 155 milhões, como vemos abaixo:

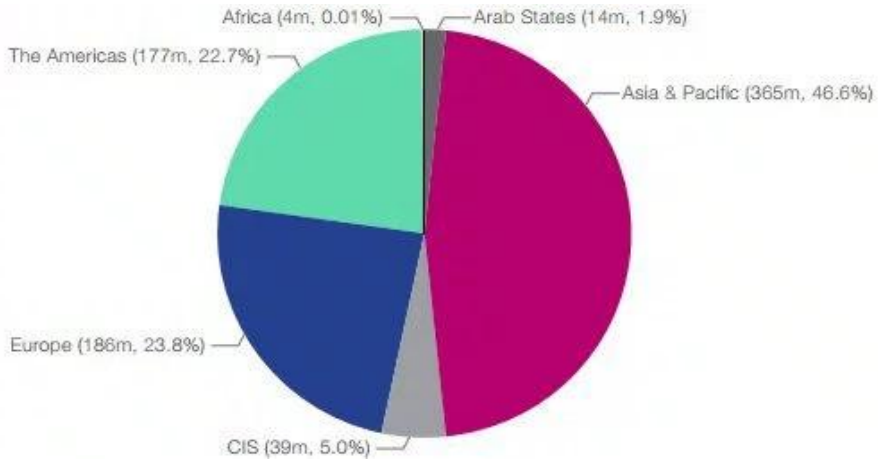
Figura 10 – Acesso de banda larga móvel no mundo



Fonte: Amaral, 2015[89].

Quando se trata do acesso à rede fixa, a UIT estima um total de 794 milhões de acessos. A quantidade de usuários avançou 7,82%, alcançando a marca de 3,17 bilhões. A maior parte desses acessos fixos também é feita na Ásia/Pacífico (46,6%) e as Américas novamente vêm em seguida, com 22,7%, como mostra o gráfico:

Figura 11 – Acesso de banda larga fixa no mundo



Fonte: Amaral, 2015.

[89] http://exame.abril.com.br/tecnologia/noticias/seis-em-cada-dez-pessoas-ainda-estao-offline-no-mundo

Algo que também influencia bastante é a velocidade da Internet banda larga, onde, segundo a UIT, há uma diferença brusca entre a velocidade dos países ricos e a das nações em desenvolvimento.

A utilização da Internet e das Tecnologias de Informação e Comunicação (TIC) continua em ascendência, com números cada vez maiores e um destaque especial para o crescente uso de dispositivos móveis, da chamada computação em nuvem, bem como o avanço da chamada "Internet das coisas". Movimentando aproximadamente cerca de US$ 170 bilhões, o Brasil está ocupando o quarto lugar no mercado mundial do setor de TIC.

O país vive a era da Sociedade da Informação acompanhada de características específicas, tais como:

a) Elevada convergência tecnológica;

b) Aumento significativo de sistemas e redes de informação, bem como da interconexão e interdependência dos mesmos;

c) Aumento crescente e bastante substantivo de acesso à Internet e das redes sociais;

d) Avanços das tecnologias de informação e comunicação (TIC);

e) Aumento das ameaças e das vulnerabilidades de segurança cibernética;

f) Ambientes complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças. (GSI/PR, 2010, p.14)

Os dados trabalhados acima refletem o grau de interconectividade do Brasil e, consequentemente, toda essa interconexão traz grandes desafios e riscos traduzidos em ataques a redes e infraestruturas críticas da informação; o crescimento dos ataques cibernéticos; além das fraudes e furto de dados. Todos estes acontecimentos vêm crescendo em consonância com a ampliação da interconectividade.

De acordo com o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança – CERT, os números de registros de incidentes no período de 1999 até 2014, no Brasil são os seguintes:

Gráfico 1 – Incidentes no período de 1999 até 2014

Fonte: CERT.br, 2014.

Ao analisar os dados acima, verifica-se que houve um aumento gradativo do ano de 1999 até 2004, quando, a partir daí, apesar de ocorrerem significativos aumentos, também houve algumas reduções de incidentes, como em 2005, 2007, 2010 e 2013. O que chama atenção é o fato de que, no ano de 2014, o total de incidentes quase triplicou, passando de um milhão. Neste ano, as notificações de tentativas de fraude constituíram-se a maior parte desse total (44%) – número cinco vezes maior do que o de 2013. Dentre essas tentativas, as que mais se repetem são os casos de páginas falsas de bancos e sítios de comércio eletrônico – que cresceram 80% - e os casos de páginas falsas como as de serviços de webmail e redes sociais – que tiveram um aumento de 73% em relação ao ano anterior.

Outro aumento significativo foi dos ataques a servidores Web – que aumentaram 54%, ultrapassando a marca de 28 mil notificações recebidas. Nesses casos, os atacantes exploram vulnerabilidades em aplicações Web para hospedar nesses sites páginas falsas de instituições financeiras e Cavalos de Tróia – ferramentas utilizadas em ataques a outros servidores e scripts para envio de spam ou scam.

Nos últimos anos, o CERT.br verificou uma grande quantidade de notificações de ataques de força bruta contra sistemas de gerenciamento de conteúdo, sendo em sua maioria, tentativas de adivinhação das senhas das contas de administração destes sistemas. O

aconselhável para prevenir este tipo de fraude é utilizar boas senhas em conjunto com o uso de verificação ou autenticidade em duas etapas.

Reforçando os dados analisados, a TAB. 4 demonstra a diversidade e o crescimento de vários tipos de ataques ocorridos no ano de 2014.

Tabela 4 – Total de ataques ocorridos no ano de 2014

Total mensal e trimestral classificado por tipo de ataque															
Mês	**Total**	**Worm**	**(%)**	**Dos**	**(%)**	**invasão**	**(%)**	**Web**	**(%)**	**scan**	**(%)**	**fraude**	**(%)**	**outros**	**(%)**
jan	33959	2853	8	6539	19	590	1	1267	3	13916	40	7248	21	1546	4
fev	43227	4163	9	6190	14	764	1	1434	3	19862	45	9616	22	1198	2
mar	45808	9238	20	2829	6	780	1	1253	2	22471	49	7780	16	1457	3
abr	41533	3513	8	1505	3	1559	3	1900	4	23320	56	8562	20	1174	2
mai	48565	2857	5	8383	17	293	0	1997	4	20756	42	12962	26	1317	2
jun	54057	2274	4	10345	19	612	1	2171	4	17477	32	20149	37	1029	1
jul	58662	3294	5	10218	17	210	0	2225	3	20292	34	21265	36	1158	1
ago	134156	3327	2	38822	28	187	0	1828	1	21500	16	67480	50	1012	0
set	214954	3312	1	56184	26	290	0	2347	1	21498	10	130108	60	1215	0
out	206148	2563	1	50195	24	296	0	3029	1	23763	11	125060	60	1242	0
nov	107219	2571	2	29566	27	201	0	3416	3	28053	26	42420	39	992	0
dez	58743	2226	3	3159	5	727	1	5941	10	30751	52	14971	25	968	1
Total	1047031	42191	4	223935	21	6509	0	28808	2	263659	25	467621	44		1

Fonte: CERT.br, 2014.

- Incidentes ocorridos de **janeiro a dezembro de 2014.**
- Incidentes reportados ao CERT.br - **janeiro a dezembro de 2014**
- **worm**: notificações de atividades maliciosas relacionadas ao processo automatizado de propagação de códigos maliciosos na rede.

- **dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **invasão**: um ataque bem-sucedido que resulte no acesso não autorizado a um computador ou rede.
- **web**: um caso particular de ataque visando especificamente ao comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

Obs.: Vale lembrar que **não se deve confundir scan com scam**. Scams (com "m") são quaisquer esquemas para enganar um usuário, geralmente, com a finalidade de obter vantagens financeiras. Ataques deste tipo são enquadrados na categoria fraude.

6.1.1 Ciberataques importantes no mundo

Um episódio de ciberataque bastante repercutido pelo mundo aconteceu em 2003, conhecido como “Titan Rain”, englobou uma série de ciberataques nas redes computacionais de várias agências (inclusive no Departamento de Defesa dos Estados Unidos da América). Os ataques tinham a finalidade de furtar informações de empresas e organismos governamentais. Na investigação para constatar a origem desses ataques, conseguiu-se descobrir apenas que eles vinham de computadores da China, não encontrando precisamente a localização deles nem, consequentemente, a identidade de seus dirigentes. Prevalece o entendimento de que os ataques tinham relação com uma Ameaça Persistente Avançada (Advanced Persistent Threat – APT 38) – referente a um ataque com alvo específico, e este alvo foi o governo dos E.U.A. Redes de *proxy*s e computadores infectados por alguns vírus. Esses ataques geraram apreensão, pois os milhares de dados furtados, reunidos, poderiam propiciar informação conveniente aos adversários. Preocupou tal situação, ainda que tenha

sido declarado que os sistemas não foram comprometidos, e as informações acessadas aparentemente inócuas (SILVA, M.A.D., 2014)[90].

Outra vez, voltou a ser amplamente discutida a questão explanada por conta do intenso ciberataque empreendido contra a Estônia em abril e maio de 2007. Houve sérias consequências para o país inteiro, vários servidores, agências, instituições, mídias, foram sobrecarregados por uma série de solicitações de serviços, causando impossibilidade de resposta (ataque do tipo DoS - denial of service -2 41) e outros prejuízos.

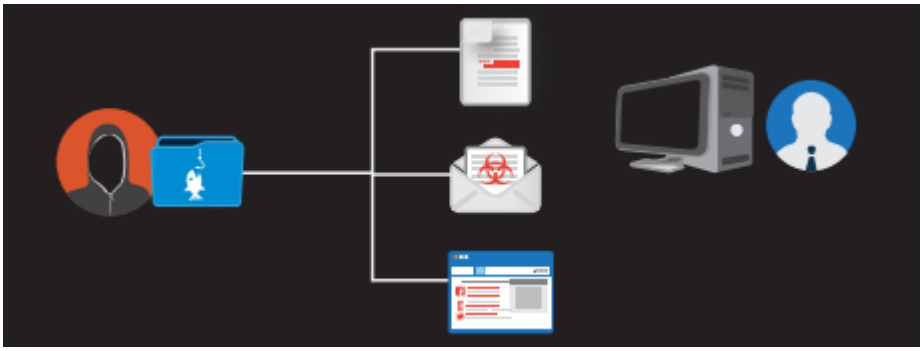
> O ataque coordenado que colocou fora de serviço parte dos sítios governamentais e comerciais parece ter tido origem na Rússia, motivado por disputas políticas entre os dois países (iniciadas pela mudança do local de um memorial russo na capital de Estónia erguido em homenagem ao soldado russo - era da dominação soviética sobre aquele país) e um eventual teste à resposta da NATO (SILVA, S.M.L., 2014).

As ilustrações na FIG. 12 exemplificam os sete estágios das ameaças avançadas na Internet, fazendo uma compreensão da cadeia de destruição do ataque cibernético.

Figura 12 – Sete estágios das ameaças avançadas na Internet

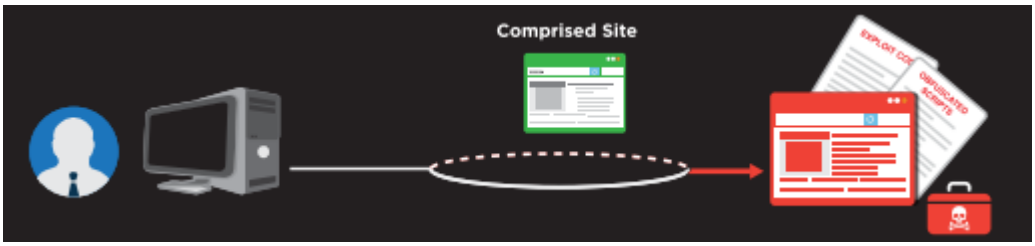
Estágio nº 1 – Reconhecimento: Quando os cibercriminosos investigam vítimas em potencial, utilizando-se de sites pessoais, profissionais e de mídias sociais. Eles procuram informações para ajudá-los a criar "iscas" aparentemente de confiança, que contêm *links* para sites comprometidos, sob o controle do cibercriminoso.

Estágio nº 2 – Iscas: Usando as informações coletadas na fase do Reconhecimento, os cibercriminosos criam mensagens de *e-mail*s, mensagens de mídia sociais ou outros conteúdos que parecem vir de fontes confiáveis para se tornarem "iscas", que podem fazer os usuários clicarem em *links* de sites comprometidos. No Twitter, há uma média de 91 tweets “maliciosos” por segundo.

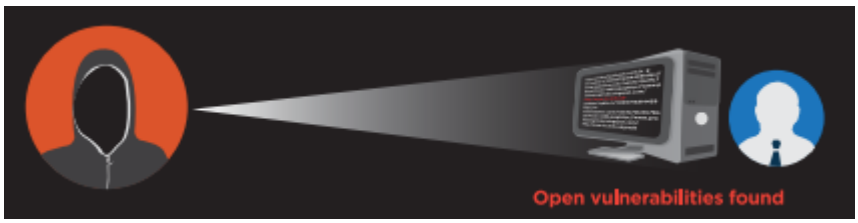


[90] http://www.jurisway.org.br/v2/dhall.asp?id_dh=15329

Estágio nº 3 – Redirecionamento: Em suas iscas, os cibercriminosos podem usar *links* que redirecionam os usuários a páginas de aspecto seguro, mas que ocultam o conteúdo malicioso, e contêm *kits* de exploração, códigos de exploração ou dados ofuscados. 85% de *links* maliciosos são encontrados em *hosts* comprometidos.

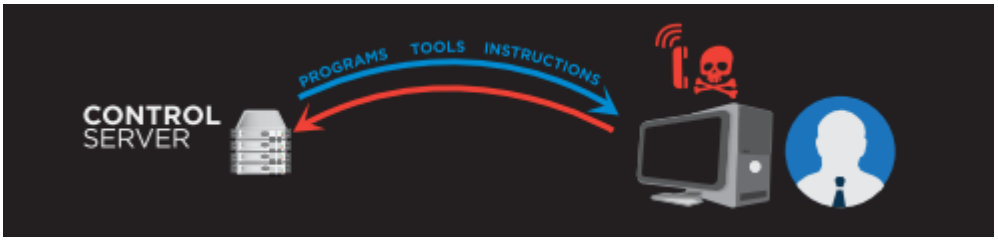


Estágio nº 4 – Kits de exploração: Uma vez que um usuário clicou em um *link* de um site comprometido, o kit de exploração verifica o sistema da vítima para encontrar vulnerabilidades abertas ou ameaças *zeroday*- o primeiro passo em direção a novas invasões.



Estágio nº 5 – Arquivos conta-gotas - Uma vez que o kit de exploração já encontrou um caminho para a entrada de *malwares*, o cibercriminoso oferece um "arquivo conta-gotas ", normalmente a partir de outro servidor comprometido, para infectar o sistema da vítima.

Estágio nº 6 - *Call Home*: Uma vez que o arquivo conta-gotas infecta o sistema alvo, são realizadas atualizações por um servidor de comando e controle para baixar programas adicionais, ferramentas ou instruções.



Estágio nº 7 – Roubo de dados: O golpe final da maioria dos ataques cibernéticos modernos. O estágio de roubo de dados completa a cadeia de destruição do ataque. Os cibercriminosos roubam propriedade intelectual, informações pessoais e de identificação dos usuários, ou outros dados valiosos.

Fonte: Websense (Tradução, explicação e adaptação do gráfico realizada pela autora), 2015.

6.1.2 Cibercriminalidade, Globalização e Soberania

Conforme as explanações acima, nota-se que, na contemporaneidade, há uma evolução tecnológica que interfere, positiva ou negativamente, em todas as áreas da sociedade, fazendo com que conceitos, que até então pareciam incontestáveis, recebam novas leituras e entendimentos. Hoje, denominações como informação, direito à privacidade e intimidade, passaram a ter, nacional e internacionalmente, valores e referências distintas, já que o mundo deixou de ser, apenas real, para tornar-se virtual.

Toda essa tecnologia possibilitou uma difusão do conhecimento nunca antes presenciado. O fácil acesso às informações, o acompanhamento, em tempo real, do mundo globalizado, o controle social e cultural, ou ainda a possibilidade de romper os limites territoriais trouxeram não só benefícios, mas também um campo fértil e favorável para a criminalidade moderna mundial, deixando vulneráveis muitos sistemas tecnológicos e desrespeitando os acordos internacionais estabelecidos entre os Estados.

Nesse sentido, devido à necessidade de normatização das relações internacionais, o Direito Internacional Público está passando por profundas mudanças, sejam elas oriundas do processo de globalização, das relações políticas e econômicas, sejam pelos avanços da criminalidade, advindos do sistema tecnológico que alcança mundialmente questões da vida pública e privada.

Assim, o Cibercrime faz com que surjam novas reflexões sobre o Direito, sua aplicabilidade, proteção e eficiência em um mundo onde as informações e comunicações são totalmente globalizadas e onde não há mais espaços territoriais delimitados.

A questão que merece análise, no atual cenário contemporâneo mundializado e tecnológico, é a necessidade de grande parte dos países rever dois pilares básicos que fundamentam um Estado: a autonomia política e a soberania. Esta última é entendida como “a atividade realizada pelo Estado, objetivando a aplicação do direito objetivo ao caso concreto trazido a juízo, resolvendo-se com caráter de definitividade uma situação de crise jurídica, de modo a alcançar a pacificação social” (SANTOS, 2014).

Dessa forma, a jurisdição nos Estados modernos é uma das expressões da sua soberania e é exercida em nome do povo (CALAMANDREI, 1999). Fazendo uma correlação entre os termos jurisdição e competência, depreende-se que:

> A jurisdição é um amplo poder de dizer o direito, já a competência seria uma delimitação da jurisdição. A função jurisdicional, como uma das expressões do poder soberano, encerra-se normalmente nos mesmos limites da soberania. Em algumas situações, o próprio exercício da jurisdição executiva sobre conflito localizado no território de outro Estado será, *per se*, uma agressão à soberania alheia (MADRUGA, 2011)[91].

O Estado passa a ser soberano quando exerce a jurisdição geral e exclusiva:

> [...] geral enquanto exerce em seu domínio territorial todas as competências de ordem legislativa, administrativa e jurisdicional, ou seja, a tricotomia tradicional; exclusiva, porque permite que, no exercício de tais competências, o Estado local não enfrente a concorrência de qualquer outra soberania (FERREIRA, 2006).

Atualmente, com o célere avanço dos aparatos tecnológicos, o processo de globalização e a vasta conexão da Internet, conceituações e afirmações em torno de elementos da Ciência política, tais como território, soberania, Estado mudaram, ocasionando também, transformações na seara jurídica.

Diante deste cenário, faz-se necessário também o questionamento de como a Internet está interferindo nas relações jurídicas e estabelecendo limites comportamentais entre o indivíduo e a preservação dos seus direitos à privacidade e às liberdades pública e privada. Por outro lado, os Estados, nas suas mais diversas formas de governo, precisam enfrentar a extensão do processo de globalização e com ele os questionamentos sobre a "relativização" do conceito de soberania, jurisdição ou competência jurídica.

Dessa forma, seguindo o entendimento mundial, surge uma nova conceituação acerca do tema soberania ou um novo entendimento do que seja; surge à necessidade de rever qual seria o limite legal de controle pelo Direito Internacional sobre a soberania Estatal. Em outras palavras, é preciso definir até onde o Estado pode e/ou deve abdicar de sua soberania em favor de um controle normativo de determinado sistema jurídico internacional.

Com a globalização econômica, a ideia de soberania torna-se relativizada ou, como defende José Eduardo Faria, torna-se compulsoriamente partilhada.

---

[91] http://www.conjur.com.br/2011-ago-17/cooperacao-internacional-nao-facil-distinguir-jurisdicao-competencia

> Sob pena de acabar ficando à margem da economia globalizada, tem obrigado o Estado-nação a rever sua política legislativa, reformular a estrutura de seu direito positivo e redimensionar a jurisdição de suas instituições judiciais, mediante amplas e ambiciosas estratégias de desregulamentação, deslegalização e desconstitucionalização, implementadas paralelamente à promoção da ruptura dos monopólios públicos (FARIA, 1999 apud FERREIRA 2006, p. 232).

Desse modo, verifica-se que a Constituição Federal de 88, de fato, agregou os princípios fundamentais do Direito Internacional, sinalizando talvez uma relativização da soberania estatal, mas, resta ainda perceber até que ponto esta agregação dos tratados internacionais deve ou pode limitar a liberdade de agir do Estado, uma vez que hoje são vários os fatores que limitam consideravelmente a soberania de um Estado-Nação. Dentre esses fatores, podem-se destacar: a interdependência econômica, social e cultural; o desenvolvimento de novas formas de comércio entre os Estados; as grandes empresas transnacionais que, mesmo não possuindo soberania, detêm poder maior que alguns Estados e, com isso, podem influenciar diretamente na política governamental desses Estados nas questões econômicas e na circulação de riquezas; entre outros fenômenos (FERREIRA, 2006).

Portanto, nessa nova realidade mundial, não há como desassociar o Direito Penal e Processual Penal do processo de globalização política, econômica e das relações internacionais estatais. Pois existem interesses comuns entre os Estados, quais sejam, o combate ao Cibercrime, bem como o desafio da nova ordem jurídica em conceituar e definir patrimônio e bem jurídico, comuns da humanidade, segurança internacional, jurisdição e competência jurídica dos Estados frente a esses crimes virtuais.

Ressalta-se que o "isolamento" de determinado Estado da ordem jurídica faz com que ele fique ainda mais vulnerável ou que se torne uma ilha dentro de um mundo informatizado. Neste ínterim, os Estados precisam estar inseridos em sistemas de combate e proteção aos delitos virtuais, mesmo que seja necessário se rever a questão da autonomia, em prol de bens jurídicos maiores. Isso não seria a decretação do fim do Estado-Nação, mas, sim, a possibilidade de um equilíbrio entre a autoreprodução e a abertura para outros sistemas jurídicos.

Assim, urge que, na era da informação, muitos países utilizem suas cotas de participação e colaboração, não apenas nas áreas econômica e política, mas também, na seara jurídica, por meio de acordos e pactos legais.

A transnacionalidade oriunda das diversas ações que ocorrem no mundo cibernético dificulta a atuação dos sistemas jurídicos de vários países e a aplicação de suas leis. Além do

mais, é muito comum que algumas práticas possam ser lícitas em um Estado e em outros não. Com isso, tentativas de homogeneizar certos mecanismos e práticas podem entrar em conflito com a ordem jurídica de alguns países.

Entretanto, conforme afirma Ikawa (2000 apud FERREIRA, 2006), ainda não há um sistema jurídico uniformizado que consiga atender às demandas globalizadas. Para ela, é preciso que mudanças sejam feitas na concepção de soberania, já que o processo de globalização alterou em definitivo a noção de tempo e espaço, além de romper toda e qualquer barreira nacional, forçando o Direito a sair da zona de conforto deixando de ser intracultural para tornar-se intercultural.

6.1.3 Cibercrime, Jurisdição, Competência e Transnacionalidade

Diante do narrado, o Direito Penal, no âmbito internacional, não obstante as distintas legislações existentes em cada país, dependerá, num futuro bem próximo, de uma grande cooperação entre os Estados do globo, para uma maior eficácia no processo investigatório e punitivo dos crimes intitulados transfronteiriços (CONTE; SANTOS, 2008).[92]

Em razão do caráter internacional da grande rede de computadores, torna-se um complexo desafio trabalhar com as temáticas sobre jurisdição e territorialidade na Internet, pois inexistem fronteiras e, portanto, surgem inúmeros questionamentos. Dentre muitos ,como determinar o juízo competente para analisar um caso referente a um crime ocorrido na rede? Exemplificando, um cibercriminoso pode estar no Uruguai e invadir o sistema informático de uma empresa com sede na Bélgica, utilizando-se de um provedor argentino, mas os prejuízos oriundos do ataque ao sistema ocorrerão no Canadá. E, com todo este zigue-zague digital muitas indagações surgem: qual o lugar do crime?; qual o Estado competente para processar e julgar o agente; se um país não pune certa atividade cibernética danosa, um país atingido deve usar o poder coercitivo de seu ordenamento jurídico para deter um individuo que está fora dos limites de sua soberania?

Apesar das indagações, Silva preceitua que:

> [...] o direito penal da era da globalização tem um objetivo eminentemente prático, deve buscar uma uniformidade de respostas no campo jurídico penal entre os Estados no tocante ao tratamento da delinquência supranacional. Com isso, deve-se evitar a criação de alguns paraísos jurídicos penais (SILVA, 2001, p.137).

[92] http://www.egov.ufsc.br/portal/sites/default/files/desafios_do_direito_penal_rdit.pdf

A tutela punitiva tecnológica é um tema ainda pouco explorado para os padrões da chamada Sociedade da informação, na qual se sobressai a intensa utilização de ultramodernos meios de comunicação filiados à tecnologia, notadamente a internet.

No cerne jurídico, o território representa o espaço limítrofe onde impera a vigência de uma ordem jurídica estatal, configurando-se assim, o local do exercício da soberania. Ocorre que a conceituação tradicional de território acabou sendo modificada com o surgimento da Rede Mundial de Computadores, uma vez que no ciberespaço não há a limitação física do território, mas apenas a celeridade das informações na vasta conexão em rede.

> Além da dificuldade em identificar um território dentro do ciberespaço outra problemática se apresenta, qual seja: um indivíduo pode estar em diversos espaços, ao mesmo tempo, na Internet. Vale dizer que um sujeito pode dispor de uma identidade no espaço real e de várias distintas na Internet, fato que, em última análise, pode gerar um conflito de competências entre os Estados e carrear numa dificuldade de localização do próprio agente do crime (CONTE; SANTOS, 2008).

Pela legislação nacional, a regra geral, quanto à aplicabilidade da lei penal no espaço, está prevista no art.5º, caput do CP, ou seja, o princípio da territorialidade, em que se aplica a lei brasileira, em regra, aos fatos puníveis que forem registrados em território nacional, independente da nacionalidade do infrator, da vítima e do bem jurídico ofendido.

Na lei penal brasileira, o lugar do crime é determinando em seu art. 6º: "Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado". Neste sentido, configura-se o princípio da ubiquidade, muito propagado nas legislações de vários países e que considera praticado o crime, tanto no momento da execução, quanto da consumação. A aplicabilidade da lei penal brasileira dentro dos limites do território é uma forma de exercício da soberania do Estado, caracterizando-se, portanto, como regra. No entanto, conforme o art. 5º, do CP, "Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional". Neste dispositivo, permite-se, de modo excepcional, a aplicação de lei estrangeira, quando assim estabelecer algum tratado ou convenção internacional, surgindo assim o princípio da territorialidade temperada.

Diante da ausência de uma legislação penal e processual penal específica no que se refere à sociedade de informação e suas peculiaridades, há também, outros princípios constantes no código penal pátrio que torna possível a aplicação da lei penal brasileira aos crimes cometidos no exterior, consoante determina o art. 7º do Código Penal, que trata da extraterritorialidade e se divide em condicionada e incondicionada (art. 7.º, §§ 2.º e 3.º).

O dispositivo legal em comento também trouxe alguns princípios norteadores no tocante à aplicação da lei penal nacional a crimes ocorridos em território estrangeiro. São eles: a) Princípio da Proteção (art. 7º, inciso I, §3º), segundo o qual prevalece a lei referente à nacionalidade do bem jurídico lesado, é também conhecido como Princípio da defesa real; b) Princípio da Justiça Universal (art. 7º, inciso II, alínea a), aplica-se a lei brasileira aos crimes que por tratado ou convenção internacional o Brasil se obrigou a punir; c) Princípio da Nacionalidade Ativa (art.7º, inciso II, alínea b), aplica-se a lei nacional aos brasileiros, onde quer que estes se encontrem; d) Princípio da Representação (art.7º, inciso II, alínea c), que torna possível a aplicação da lei brasileira aos crimes cometidos no estrangeiro em aeronaves ou embarcações privadas ou mercantes que se localizem em território estrangeiro e aí não sejam julgados. Em contrapartida:

> Alguns doutrinadores afirmam que somente a aplicação dos artigos 5º e 6º do nosso Código Penal não seria suficiente para a solução do problema da aplicação da lei penal no espaço, tornando-a, na realidade, dúbia e confusa no que tange aos crimes informáticos, dentre eles, Celso Valin. Referido autor, inclusive, aponta como melhor opção considerar-se como local do crime aquele em que está localizado o agente, o que não se apresenta como entendimento pacífico, constituindo, até mesmo, objeto de recusa internacional. Gabriel César Zaccaria de Inellas posiciona-se no sentido de que deve ser aplicada a regra geral do art. 6º do Código Penal, segundo a teoria da ubiquidade, sem prejuízo de convenções, tratados e regras de direito internacional, assim, os delitos cometidos fora do território nacional, poderiam aqui receber punição, desde que previstos em Convenções ou Acordos internacionais os quais o Brasil subscreva. Entretanto, independentemente da postura adotada, a doutrina é uníssona ao tratar da necessidade de se firmar um documento internacional que aponte parâmetros globais a serem tomados, com o fito de se evitar o problema de que todos ou nenhum país se considere apto a julgar referidos crimes (CONTE; SANTOS, 2008).

Os delitos cometidos em função da utilização da Internet consideram-se tipos plurilocais e cometidos a distância. Neste raciocínio, o aplicador da lei combinou o art.7º do CP com o art. 70, parágrafos 1º e 2º do CPP que aplicam a teoria do resultado aos crimes a distância cometidos além do território nacional, ou seja, é a aplicabilidade da lei penal no espaço na órbita legal internacional, independentemente de o autor estar no Brasil e o provedor e a vítima no exterior, ou vice-versa (FERREIRA, 2006).

A Declaração Universal dos Direitos Humanos afirma que: “Toda pessoa tem direito a receber dos tribunais nacionais competentes remédio efetivo para os atos que violem os direitos fundamentais que lhe sejam reconhecidos pela Constituição ou pela lei.” Em que pese tão importante instrumento ético-jurídico preceituar o sagrado direito de justiça, muitas vezes, a resposta em forma de sentença não se efetiva, mesmo com o mínimo de estrutura possível, tais como normas definidas, agentes e sistema jurisdicional. No caso em comento, as

circunstâncias são ainda mais alarmantes, pois, em razão das peculiaridades que norteiam a cibercriminalidade, tais como, a escassa legislação, a ausência de limites temporais e espaciais e, consequentemente, a imprevisibilidade, não há uma estabilidade jurídica no seio nacional, quiça além fronteiras para fazer valer direitos tão relevantes.

No intuito de efetivamente combater os crimes advindos da esfera ciberespacial de forma mais efetiva, pois tais delitos estão a cada dia tomando maiores proporções, cabe ao Estado reavaliar as limitações territoriais, juntamente com as limitações legais. O Direito Penal interno atua até as delimitações fronteiriças do país, não saindo desse órbita jurisdicional sem a devida autorização legal. Neste raciocínio, quando a criminalidade locomove-se livremente sem óbices temporais e territoriais, faz-se premente recorrer ao Direito Penal Internacional "enquanto ciência que visa, em complementaridade, à definição de condutas delitivas, as quais o direito penal interno não consegue, por falta de previsibilidade, ou algum outro fator, alcançar" (SILVA, M.A.D, 2015)[93].

Por isso, cabe aos países procurar soluções que freiem tais ameaças e permitam a utilização salutar das ferramentas tecnológicas.

> É impossível para o Estado não se utilizar das ferramentas desenvolvidas pela tecnologia, em prol do seu benefício, seja no âmbito nacional ou internacional, entretanto, desenvolver estratégias que possam aumentar a segurança dos Estados, quando utilizarem-se desses mecanismos, na defesa de seus interesses, é de inquestionável necessidade, principalmente diante da crescente ameaça apresentada pelos outros atores internacionais. Os ataques cibernéticos aos sistemas governamentais têm sido uma prática constante, que exigem a atuação dos Estados em prol do desenvolvimento, em cada um deles, de sistemas de segurança virtual, que preservem as informações, e, principalmente, as estratégias militares do Estado (BARROS, 2015, p. 87).

Sendo assim, quando interesses ou bens jurídicos comuns são afetados ameaçando o bem-estar da comunidade internacional deve-se criar um aparato jurídico-estratégico supranacional para salvaguardar os direitos ofendidos,especialmente se eles possuírem a característica de serem humanos. Na esteira desse raciocínio, o Professor George Sarmento classifica os direitos relativos ao cerne da informática, como sendo direitos humanos:

> No outro eixo dos direitos de 4ª geração está o direito da informática, produto da Sociedade da Informação e suas complexas formas de expressão comunicativa. As relações intersubjetivas nascem de atividades relacionadas à informática, telemática e telecomunicações, bem como a transmissão de dados através de meios eletrônicos e interativos. O grande desafio dessa geração é a solução de litígios que envolvam o

[93] http://www.jurisway.org.br/v2/dhall.asp?id_dh=15329

> comércio virtual, a pirataria, a invasão de privacidade, direitos autorais, propriedade industrial etc (SARMENTO, 2011)[94]

O fundamento maior do Direito Penal Internacional é, indubitavelmente, "evitar a impunidade universal das severas violações aos direito humanos, sendo este o fundamento jurídico-fático do Direito Internacional" (HATA, 2010, p.118). Neste pensar, os delitos virtuais tais como, o ciberterrorismo, *ciberbullying*, fraudes eletrônicas, ciberespionagem, dentre outros, ofendem muitos bens jurídicos importantes, especialmente, a honra, a liberdade e a vida.

"Com a interação entre o Direito Internacional e o Direito Interno, os grandes beneficiários são as pessoas protegidas [...] No presente contexto, o Direito Internacional e o Direito interno interagem e se auxiliam mutuamente no processo de expansão e fortalecimento do ser humano" (CANÇADO TRINDADE, 1996, p. 53 apud PIOVESAN, 2006).

Em razão de os crimes cibernéticos não se prenderem a ideia de tempo e espaço, fronteiras ou territórios, surge a necessidade de se implementar uma nova forma de repressão a tais delitos, envolvendo a colaboração sociojurídica das diversas nações no enfrentamento dos cibercrime.

> "A reprimenda à criminalidade praticada com o emprego de meios eletrônicos, notadamente os que avançam na rede mundial de computadores, terá de ser acionada por todos os povos civilizados e essa perspectiva deriva, com certeza, do próprio fenômeno da globalização. Enquanto isso, persistem as dúvidas quanto à lei a se aplicar em cada caso concreto: se a lex fori ou se a lex loci delicti comissi e, no tocante à competência, qual a jurisdição assumirá o processo e julgamento desses crimes" (DAOUN; BLUM, 2000, p. 117).

Assim, quando a estrutura do Direito nacional não consegue lidar com ofensas jurídicas que ultrapassam as fronteiras domésticas, cabe recorrer a uma espécie de Direito Positivo Universal que não se prenda a velhos conceitos de jurisdição e soberania, mas que leve em apreço as transformações sofridas pela comunidade mundial nas últimas décadas, especialmente com o advento da mundialização e a revolução na seara tecnológica e informacional.

O mundo, globalizado, sofre com as consequências das redes e sistemas de informação, hoje, mesmo com tantos avanços, seja na parte tecnológica, seja na parte investigativa, ainda é muito difícil controlar e punir o Cibercrime. Esses fenômenos criminais, bem como as estratégias de combate e punição a eles, não surgiram de uma vez, em 11 de

[94] http://www.georgesarmento.com.br/wpcontent/uploads/2011/02/GeraçõeS-dos-direitos-humanos-e-os-desafios-de-sua-efetividade1.Acesso

setembro de 2001, por exemplo. Após o episódio terrorista, a Comunidade Europeia, em Budapeste, editou a mais importante Convenção sobre o Cibercrime, já vista. Nesse momento, foram estabelecidos conceitos básicos de direito material e processual acerca do tema, além de um rol de padrões de crimes para se alcançar uma possível padronização universal, levando-se em consideração a característica da transnacionalidade, além do caráter metaterritorial, já mencionados no texto, sobre tais delitos (FERREIRA, 2006).

Se há limitações pelos Estados na regulamentação e tipificação dos crimes virtuais, o que dizer quando se refere à jurisdição no ciberespaço e a possibilidade de um controle para além dos limites geográficos ou territoriais? Diante desse cenário, a polêmica em torno do tema é grande e não se vislumbra uma solução a curto prazo, já que, ao mesmo tempo em que se defende a liberdade e o acesso às informações, se constata que só haverá uma possível punição real aos cibercriminosos se muitos assumirem uma responsabilidade jurídico-solidária

Alguns Cibercrimes surgiram da tentativa de regularização de determinadas condutas em prol de um objetivo maior, como é o caso da "ciberespionagem", que nasce da regularização da interceptação das telecomunicações feita através de correio eletrônico, telefones e fax, para garantir a segurança nacional dos Estados. Especificamente em relação ao combate a esse crime, já existem alguns organismos plurinacionais, a saber: o da Comunidade Europeia, a OIPC – Interpol; o grupo TREVI, o grupo SCHENGEN e a intenção futura da criação da EUROPOL - *Oficina central europea de policía criminal* (MOREIRA, 2002 apud FERREIRA, 2006), além de existir uma série de organismos relacionados com o controle da rede de Internet, dentre eles:

> a) Organismos técnicos: ICCB (*Internet Configuration Control Board*/Junta de Controle da Configuração da Internet), IAB (*Internet Architecture Board*/Junta para a Arquitetura da Internet), IETF (*Internet Engineering Task Force/*Grupo de Trabalho para a Ingerência da Internet), IRTF (*Internet Research Task Force*/Grupo de Trabalho para a Investigação sobre a Internet) e o ILTF (*Internet Law Task Force*/Grupo de Trabalho sobre o Direito da Internet);
> b) Organismos de coordenação e representação, cujo essencial é o ISOC (*Internet Society/*Sociedade da Internet);
> c) Organismos de gestão dos nomes de domínio, sendo que, no momento, o de maior relevância é o ICANN (*Internet Corporation for Assigned Names and Numbers*), seguido pelo Parlamento Europeu, que vem produzindo uma representação democrática e geograficamente equilibrada de seus órgãos (CONDE, 2002 apud FERREIRA, 2006).

Quando se trata de questões envolvendo a extraterritorialidade internacional no Cibercrime, tal temática extrapola o limite territorial e adentra o desconhecido ciberespaço.

Independentemente da lei material a ser adotada, há, como grande problema a ser resolvido, a questão da jurisdição, já que o fato ultrapassa as questões penais/territoriais e envolve relações civis, econômicas, culturais e comerciais. De qualquer modo, algumas nações já começaram a mitigar o ideário de soberania, dando os primeiros passos em direção a um sistema jurídico transnacional, como é o exemplo da Convenção de Budapeste e das primeiras normatizações acerca da ciberespionagem.

À luz do exposto, em que pese a grande diversidade diluída de posicionamentos, questionamentos, informações, escolhas e ações, já despontam, no horizonte mundial, algumas centelhas em forma de nações que começam a raciocinar juridicamente, ensaiando os primeiros diplomas legais fundamentados num Direito de cunho universal, para atender às prementes necessidade da comunidade mundial contemporânea.

Enquanto isso, o ciberespaço continua sendo um campo fértil para o cultivo de temas sociais, políticos e econômicos, mas também, para o submundo dos Cibercrimes. Por isso, urge que se faça um planejamento verdadeiramente estratégico para coibir tais práticas nocivas, uma vez que Cibersegurança não se resume à proteção de computadores, contas individuais, redes ou servidores. Ela vai mais além. A luta no ciberespaço envolve as bases, o sustentáculo de uma nação. A proteção alberga bens, infraestruturas e processos, tenta impedir grandes sabotagens e invasões aos serviços essenciais de um Estado, os serviços tecnológicos de que dependemos cotidianamente, como: caixas eletrônicos e dispositivos médicos, redes elétricas, satélites de comunicações e malhas de telefonia, ou seja, Cibersegurança ou Segurança cibernética busca resguardar os sistemas de dados primordiais na vida da humanidade.

6.2 DA GESTÃO JURÍDICO-ESTRATÉGICA NO PROCESSO INVESTIGATÓRIO

Antes de se fazer uma abordagem a respeito de gestão jurídica, há que se tratar de alguns conceitos, sobretudo o de gestão. Para tal, segue-se a definição através do verbete registrado por Houaiss (2009, p. 968) como “ato ou efeito e gerir”. Gerir, ainda segundo o mesmo dicionarista (HOUAISS, 2009, p.967), é “exercer gerência sobre; administrar”.

6.2.1 Gestão Jurídica

Nessa linha de raciocínio de que gestão e administração são sinônimos, recorre-se ao que assegura, para explicar gestão, um grande estudioso do assunto, Jules Henri Fayol (apud Caravantes, 1999, p. 43), Textualmente, Fayol explica que:

> Administrar é prever, organizar, comandar, coordenar e controlar. Prever é perscrutar o futuro e traçar o programa de ação; Organizar é constituir o duplo organismo material e social da empresa; comandar é dirigir o pessoal; coordenar é ligar, unir e harmonizar todos os atos e esforços; e Controlar é velar para que tudo ocorra de acordo com as regras estabelecidas e as ordens dadas.

Portanto, como se pode inferir, trazendo para a temática aqui abordada, gestão cuida da previsão dos cenários e dos recursos disponíveis, ou seja, "prever para prover", sistematizar de forma racional tais recursos – sejam eles materiais, tecnológicos ou humanos, dirigir de forma a otimizá-los, dispô-los de modo a que possam produzir bem, dar os resultados esperados e, enfim, medir tais resultados, monitorando-os, mensurando sua eficácia.

É impossível tratar de gestão sem se referir ao ator principal dessa função que é o gestor, o líder. Pode-se comparar o papel do gestor como um maestro. Óbvio que, no processo de gestão, é fundamental que se arregimentem talentos, que se busquem participação e comprometimento de quem é gerido. Importante também é auscultar a equipe, saber identificar lideranças entre os subordinados, uma vez que a liderança não é algo estanque, mas um fenômeno situacional e, desse modo, flutuante. Em determinadas situações, num cenário xis, pode despontar alguém que tem mais habilidade e que assume instintivamente o comando. Ora, o indivíduo encarregado da gestão tem, necessariamente, que perceber tal conjuntura e potencializar aquele recurso para o sucesso do empreendimento.

Para que esses líderes informais e positivos – sim, porque há lideranças negativas - possam despontar, é fundamental que haja confiança. Covey (1999, p.195) define que:

> A confiança é a forma mais elevada de motivação humana. Ela traz o que há de melhor nos seres humanos. Mas exige tempo e paciência, e não elimina a necessidade de treinar e aprimorar as pessoas, de forma que sua competência possa fazer jus à confiança depositada.

No âmbito jurídico, é crucial que se busque uma gestão pautada na eficiência, que se procurem estratégias capazes de alavancar situações, demandas que façam dar mais produtividade, mais eficiência e eficácia aos processos.

Em todas as áreas dos saberes humanos, em todas as profissões, percebe-se um cenário de competição muito grande. O que se busca, no momento, é a luta pela eficácia - obvio que ciosamente orientada pela ética – que possa fazer face ao universo competitivo da profissão.

Bertozzi[95] definiu algumas áreas que requerem atenção quando se trata de gestão jurídico-estratégica. Ei-las:

> a) Comunicação Jurídica – ser percebido pelo mercado de maneira ética e eficaz;
> b) Marketing de relacionamento – conseguir suprir as necessidades dos clientes;
> c) Tecnologia & Informática – administrar a informação e logística;
> d) Gestão Administrativa – modelos copiados de empresas com excelência;
> e) Gestão Financeira – máximo resultado e controle de custos;
> f) Recursos Humanos – selecionar, desenvolver e motivar talentos internos;
> g) Qualidade – implementação de sistemas qualitativos e de controle;
> h) Planejamento Estratégico – criando condições para o crescimento do negócio.

Diante desse cenário que se desenha na atualidade, é imperativo que os serviços jurídicos oferecidos pautem-se em pilares sólidos para que os profissionais que os ofereçam possam ser competitivos, sem, contudo, descurar de posturas versadas na ética.

É oportuno questionar se, sem um planejamento estratégico que contemple todos os saberes da área administrativa – e aqui se citam itens contemplados para definir Administração -, pode-se exercer uma advocacia com excelência.

Num artigo intitulado Os Cinco "Es" da Gestão Estratégica Jurídica – Parte I, Bertozzi e Selem fazem uma adaptação de conceitos de Jack Welch, pensador e estudioso sobre Administração, autor do que chamou de cinco habilidades que devem estar no dia a dia de um bom líder. São elas: Energia, Energizar, Escolher, Executar e Experimentação.

Energia, segundo o autor, é a capacidade de o líder levar em frente as tarefas, independentemente dos obstáculos com que se depare pelo caminho.

Por energizar, o autor chama o poder de fazer com que seus liderados possam potencializar capacidades, gerando sinergia. Assim sendo, os resultados são surpreendentes. Escolher é ter o bom senso de fazer a opção correta entre as muitas alternativas que se apresentarem diante de um problema. Trazendo para a gestão jurídica, é o poder de o profissional sair da perigosa zona de conforto e buscar as melhores decisões entre as que se mostrarem no portfólio de opções.

Por executar, ele trata o fato de sair da perigosa tentativa de ficar preso ao planejamento e partir para a busca de ações previstas ali. Não adianta desenhar um plano mirabolante e ficar olhando para ele sem pô-lo em prática. Enfim, a Experimentação é tratada

[95] http://www.estrategianaadvocacia.com.br/artigos2.asp?id=420#.VfvpF99VhHw

como a “a mais inovadora de todas as capacidades”. É o ato de explorar sem qualquer temor todo o leque de possibilidades. Desprender-se do pacato mundo das coisas existentes e ousar buscar algo novo, que revolucione, que faça a diferença.

Diante do exposto, gestão jurídico-estratégica vai muito além dos conceitos administrativos de Gestão simplesmente dita. Requer, sobretudo, uma dosagem potente de criatividade e senso de adequação, de aprendizagem constante. E, na esfera jurídica criminal, está diretamente ligada à persecução penal, investigação, obtenção de provas, conhecimento sobre o criminoso ou organizações, força-tarefa e investimento público para que se crie infraestrutura. A seguir, serão delineados os passos do procedimento investigatório no universo do Cibercrime.

6.2.2 O processo de Investigação Criminal no Cibercrimes

Com a era da informática e o amplo e irrestrito acesso à Internet, vimos que alguns crimes, “clássicos”, passaram também a ser cometidos no ambiente virtual. Hoje, por exemplo, o furto ao banco tanto pode ocorrer através de forma física na agência bancária, como no meio virtual. Já outros crimes, como a invasão de sistemas e/ou dispositivo informático só podem ser cometidos, exclusivamente, de forma virtual ou através da Internet. Somado a isso, os crimes praticados nos espaços virtuais ou ciberespaços possuem natureza transnacional, o que só aumenta e dificulta seu processo de investigação na rede mundial de computadores.

No ato de investigação dos Cibercrimes, além de se observar a característica principal da transnacionalidade, deve-se, também, levar em consideração a universalidade de informações e o fenômeno da mundialização (em seu sentido mais amplo), já que este último está intimamente relacionado com tais crimes, seja de forma direta ou indireta, em função do processo de virtualização do mundo moderno.

Assim, nesse processo, o virtual passa a ser um atributo de grande expressão, já que representa a liberdade e alcance irrestritos, uma vez que supera a questão física, fazendo com que as informações circulem instantaneamente. Neste compasso, os usuários interagem entre si e com o restante do mundo, fazendo surgir a ideia de uma sociedade nômade, que, com o mínimo esforço, estabelece novas relações e conexões sociais constantemente.

Esse movimento real/virtual demonstra o surgimento de novo traço cultural/ mundial, a Cibercultura, que, conforme foi visto e trabalhado, nada mais é do que o meio de informação e comunicação que possibilita a interação entre pessoas de várias ordens.

Com a universalização das informações e conhecimento via Internet, torna-se inevitável a necessidade de lidar com os aspectos negativos dessa Cibercultura, ou seja, lidar com usuários da rede que se beneficiam com a facilidade do acesso ao mundo virtual para praticarem condutas ilícitas e/ou criminosas. Por isso, como já discutido, é preciso compreender a necessidade de se criarem mecanismos de normatização do mundo virtual, uma vez que o mesmo avanço que impulsiona as relações sociais e econômicas também pode causar danos. Dessa forma, o Direito deve salvaguardar o poder que o Estado tem em punir o agente criminoso através de órgãos e instrumentos hábeis, defendendo bens jurídicos ameaçados.

6.2.2.1 Órgãos que combatem a cibercriminalidade: Polícia Federal, Judiciário e Ministério Público

Na era da evolução tecnológica, a cada dia surgem novos dispositivos de acesso à rede mundial e, concomitantemente, no mesmo ritmo ou até de modo mais célere, surgem diversas ameaças que se traduzem em novos tipos de cibercrimes. Nestes moldes, torna-se um verdadeiro desafio para os órgãos responsáveis pela persecução penal e pelo processo judicial, acompanharem toda esta celeridade, investigar e, ao final, punir os criminosos virtuais.

Atualmente, é necessário planejar e instrumentalizar a Polícia Federal, *o Parquet* e o Judiciário devidamente para o combate à delinquência virtual.

O art. 144, § 1º, da Constituição Federal estabelece a competência da Polícia Federal, definindo suas funções, dentre elas:

> § 1º A polícia federal, instituída por lei como órgão permanente, organizado e mantido pela União e estruturado em carreira, destina-se a:
> I - apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei;
> II - prevenir e reprimir o tráfico ilícito de entorpecentes e drogas afins, o contrabando e o descaminho, sem prejuízo da ação fazendária e de outros órgãos públicos nas respectivas áreas de competência;
> III - exercer as funções de polícia marítima, aeroportuária e de fronteiras; IV - exercer, com exclusividade, as funções de polícia judiciária da União.

Sobre as referidas atribuições da Polícia Federal, Morais Neto (2009)[96] esclarece:

[96] http://www.ccj.ufpb.br/pos/wp-content/uploads/2013/07/Arnaldo-Sobrinho-Cibercrime-e-Coopera%C3%A7%C3%A3o-Penal-Internacional.pdf

> Dentre as ações destacadas, insere-se, mormente, as práticas delituosas que se disseminam, quer internamente no país, com repercussões que vão além dos limites dos Estados-membros, quer nos delitos com caráter transnacional e vinculados a criminalidade organizada, sobretudo, como é o caso do cibercrime, cujas características pressupõem o emprego mais especializado e uniforme. Antes da expansão comercial da internet, que só veio ocorrer no Brasil em 1996, a rede só era utilizada com caráter acadêmico, o que nos leva a concluir pela inexistência, em tese, de condutas ilícitas. Com a abertura e disponibilização comercial dos serviços as primeiras práticas delituosas ou condutas que configuravam ilicitude passaram a ocorrer (MORAIS NETO, p. 100, 2009).

Desse modo, a Polícia Federal é um órgão competente para a investigação de crimes cibernéticos, pois apresenta, no rol de suas atribuições, o combate a delitos praticados nos Estados brasileiros (infrações de repercussão interestadual) assim como alcança também, crimes que cruzam as fronteiras nacionais possuindo características de transnacionalidade, ou seja, com repercussões em outras nações. Vale lembrar que se o crime ocorrer num dado estado da federação, sem sair dos seus limites territoriais estaduais, a competência é da polícia estadual.

O cibercrime é um destes tipos ilícitos que sofrem investigação da Polícia Federal. Neste raciocínio, para enfrentar o problema dos ciberdelitos, foi criado, no cerne do Departamento da Polícia Federal, o Serviço de Perícias de Informática- SEPFIN, um setor técnico, especializado nas áreas de ciências da computação, informática e tecnologia da informação, com especialistas concursados. Assim, há no âmbito da PF, setores específicos que tratam do combate às fraudes eletrônicas, *Internet banking*, clonagem de cartões de crédito/débito, a venda de medicamentos na Internet, os crimes de Alta Tecnologia, a pornografia infantil, dentre outros delitos.

No Brasil, tais núcleos de atendimentos especializados dão suporte e auxiliam as vítimas de crimes virtuais[97]:

> São Paulo:DIG-DEIC – 4ª Delegacia – Delitos praticados por Meios Eletrônicos**.** Presta atendimento presencial, por telefone e via Web. Endereço: Av. Zack Narchi, 152, Carandiru – São Paulo (SP) Fone: (11) 2224-0721 ou 2221 – 7030. Para denunciar qualquer espécie de delito virtual anonimamente, utilize o e-mail: 4dp.dig.deic@policiacivil.sp.gov.br
>
> A 4ª Delegacia – Delitos praticados por Meios Eletrônicos- investiga apenas fraudes patrimoniais praticadas por meio eletrônico no âmbito da Capital do estado de São Paulo tais como:Crimes de estelionato; furto mediante fraude; desvio de dinheiro de contas bancárias; pagamento de títulos por meio de fraudes, empresas falsas de empréstimos; compras de mercadorias em sites falsos (e-comerce).
>
> Assim, caso a denuncia trate acerca de crimes contra a honra (injuria, calunia e difamação), ou ameaças praticadas por meio de redes sociais, *blogs*, *e-mails*,

[97] <http://www.crimespelainternet.com.br/delegacias-de-crimes-digitais/>.

> falsidade ideológica (*fakes*, perfis falsos, documentos, sites falsos, etc), ofensas ao direito do autor, invasão de dispositivo informático, "furto" de senhas ou de dados, deverão ser registradas em qualquer outra delegacia.
>
> Crimes de pedofilia ou outros de cunho sexual que envolvam crianças ou adolescentes e extorsão, por meio da utilização da Internet para a pratica do delito, deverá ser apresentados ao Departamento de Proteção à Pessoa –D.H.P.P. Rua brigadeiro Tobias, nº 527 5º Andar. – Centro de São Paulo.
>
> Rio de Janeiro: Delegacia de Repressão aos Crimes de Informática (DRCI) – Rua Professor Clementino Fraga, nº 77 (2º andar), Cidade Nova (prédio da 6ª DP), Rio de Janeiro/RJ (CEP: 20230-250), telefones (0xx21) 2332-8192, 2332-8188 e 23328191 e e-mail- drci@pcivil.rj.gov.br
>
> Espírito Santo:Delegacia de Repressão a Crimes Eletrônicos (DRCE) – Av. Nossa Senhora da Penha, 2290, Bairro Santa Luiza, Vitória/ES (CEP: 29045-403), telefone (0xx27) 3137-2607 e e-mail drce@pc.es.gov.br;
>
> Minas Gerais: DEICC – Delegacia Especializada de Investigações de Crimes Cibernéticos – Av. Nossa Senhora de Fátima, 2855 – Bairro Carlos Prates – CEP: 30.710-020, Telefone (33) 3212-3002, e-mail dercifelab.di@pc.mg.gov.br;
>
> Paraná:Nuciber da Polícia Civil do Paraná – Rua José Loureiro, 376, 1º andar – sala 1 – Centro – 80010-000 – Curitiba-PR, Tel:(41) 3323-9448 – Fax: (41) 3323-9448, e-mail cibercrimes@pc.pr.gov.br;
>
> Rio Grande do Sul: Delegacia de Repressão aos Crimes Informáticos (DRCI/DEIC) – Av. Cristiano Fischer, 1440, Bairro Jardim do Salso em Porto Alegre, na mesma sede do DEIC. O telefone de contato é (0xx51) 3288-9815, e-mail drci@pc.rs.gov.br;
>
> Distrito Federal: Divisão de Repressão aos Crimes de Alta Tecnologia (DICAT) – Não atende diretamente ao público, neste caso a vítima pode procurar a delegacia mais próxima para efetuar registro de ocorrência. A DICAT é uma Divisão especializada em crimes tecnológicos que tem como atribuição assessorar as demais unidades da Polícia Civil do Distrito Federal, o telefone é (0xx61) 3462-9533 e e-mail dicat@pcdf.df.gov.br;
>
> Goiás:Gerência de Inteligência da Polícia Civil – Setor de Análise (0xx62) 3201-6352 e 6357)
>
> Pará:Delegacia de Repressão aos Crimes Tecnológicos – Travessa Vileta, n° 1.100, Pedreira. Belém-PA. CEP: 66.085-710, com telefone de contato (91) 4006-8103, e-mail drct@policiacivil.pa.gov.br. A DRCT é vinculada à Diretoria de Repressão ao Crime Organizado**.**
>
> Mato Grosso – Cuiabá:Gerência de Combate a Crimes de Alta Tecnologia – GECAT – Av. Cel. Escolástico Nº, Bandeirantes – Cuiabá – Cep: 78.010-200 – Telefone: (65) 363-5656
>
> Sergipe – Aracaju: Delegacia de Repressão a Crimes Cibernéticos (DRCC) – Rua Laranjeiras, nº 960, Bairro Centro – Aracaju – Cep: 4900-000 telefone: (79) 3198-1124[98]

Em função da complexidade dos cibercrimes, muitas vezes é imprescindível a união da PF, do Ministério Público (*parquet*) e do judiciário para enfrentar e solucionar os

[98] <http://www.crimespelainternet.com.br/delegacias-de-crimes-digitais/>.

problemas decorrentes da cibercriminalidade. Do mesmo modo em que as atribuições da PF são descritas na Constituição Federal, esta também define as atribuições específicas do Poder Judiciário (Art. 109) e do Ministério Público (Art. 129). Os dois referidos órgãos se dividem em esferas federal e estadual. Sendo assim, há o Poder Judiciário Federal e Ministério Público da União (incluindo o Ministério Público Federal) e, em nível estadual, há o Poder Judiciário e o Ministério Público Estaduais.

> Considerando que as práticas delituosas perpetradas com emprego de alta tecnologia são enquadradas, para efeitos de punição, como delitos comuns, podem suscitar dúvidas quanto à competência se, da Justiça Federal ou da Justiça Estadual (comum), conforme o bem jurídico ou alguma circunstância especial (MORAIS NETO, 2009, p. 106).

Levando em conta que os crimes decorrentes da utilização do ciberespaço, para fins de investigação e punibilidade, podem ser comuns, federais ou transnacionais, para uma verdadeira eficácia da aplicação da justiça, premente se faz uma conjugação de forças entre as três instituições para prevenir e combater tal espécie de delito.

Assim como são inúmeros os benefícios e utilização da Internet, também são incontáveis as formas de praticar os Cibercrimes, pois o avanço tecnológico também proporciona sua prática. Entretanto, na via inversa, o sucesso da investigação desses crimes também depende do conhecimento e utilização das ferramentas tecnológicas, já que o conhecimento técnico dos investigadores é fundamental para detectar a natureza do crime e como e com qual ferramenta será combatido.

Os investigadores (membros do MP e da PF) para identificarem a autoria do crime, usarão diferentes meios de investigação, variando conforme o fato e natureza do delito, podendo estes serem praticados através de *e-mail*, *websites*, programas de transferência de informações, grupos de debate, redes sociais, sites de comércio eletrônico, entre outros.

Os indícios da prática dos Cibercrimes possuem algumas particularidades, a saber: são instáveis, podendo ser feitos de maneira descomplicada, apagados, alterados, perdidos; os vestígios deixados são complexos e de difícil identificação; possuem natureza supranacional, podendo ser cometidos em todo e qualquer lugar do mundo com acesso à Internet; as evidências são de difícil identificação; há inúmeras quantidades de fluxo de dados ilegítimos que devem ser analisados e separados acarretando maior esforço para uma análise dos investigadores (CAVALCANTE, 2013)[99].

[99] https://jus.com.br/artigos/25743

A chance de os usuários cometerem crimes virtuais aumenta a cada dia já que, devido à insegurança jurídica, ou a não regulamentação normativa por parte do Estado, alguns se sentem inatingíveis em relação à punição e/ou sanção do Cibercrime porque estes nem sempre são investigados e, quando o são, nem todos os Estados possuem preparo técnico adequado, ou não dão prosseguimento à investigação e não conseguem identificar o autor do fato.

O fato de o Cibercrime ter, como característica, a dificuldade na identificação do seu autor, percebe-se que alguns usuários que praticam o delito virtual, provavelmente, não os cometeriam fora da Internet, pois só através deste meio conseguem a segurança necessária para o ato, seja ele indireto, como tráfico de drogas, ou direto, como o estelionato (SILVA, M.A.D., 2015)[100].

Como os Cibercrimes possuem caráter incomum, é preciso destacar que o Direito Penal, como propagador da ordem jurídica e protetor dos bens essenciais ao equilíbrio da vida social, precisa tutelar o bem jurídico afetado nos crimes virtuais, mesmo que este seja não convencional, mas que tenha sido afetado pela prática delituosa, exatamente como acontece nos crimes cometidos contra o bem jurídico definido como "comuns", fazendo com que cada conduta penalmente punível seja pragmaticamente aplicável (CRESPO, 2011).

Portanto, é visível a necessidade de prevenção, punição e proteção contra os Cibercrimes, devendo os mesmos sofrerem as penalidades cabíveis, assim como ocorre com os crimes já descritos no Código Penal, pois, a garantia dos direitos e a segurança no ciberespaço devem ser protegidas. Para tanto é imprescindível a realização de operações em conjunto entre a PF e o MP, bem como o empenho do judiciário na celeridade e conhecimento técnico para compreender e julgar o processo.

6.2.3 Táticas e desafios na investigação preliminar dos Cibercrimes

Em linhas gerais, os procedimentos e métodos adotados na investigação dos Cibercrimes estão em conformidade com a ciência forense. Eles buscam a aquisição, preservação, análise e apresentação das evidências que porventura existirem. Para tanto, é necessário que os profissionais sejam capacitados e constantemente aperfeiçoados nas técnicas de investigação tecnológica, pois as atividades ilícitas, normalmente, são cíclicas e criteriosas, dificultando assim a apresentação de evidências definitivas.

[100] http://www.jurisway.org.br/v2/dhall.asp?id_dh=15329

A defesa, ao formar o contraditório, pode arguir a legitimidade dos procedimentos de investigação, bem como a consistência do laudo pericial, solicitando novas provas, na análise e informações durante o andamento do processo. Por isso, para que não haja nenhuma contestação de provas, o processo investigativo deve cumprir alguns requisitos que garantam as evidências digitais juridicamente válidas. Conforme a RFC 32271, que fornece algumas recomendações de procedimentos de coletas de provas em meio digital, alguns pontos devem ser observados nesse processo. São eles:

> a) Admissível: ou seja, estar em plena conformidade com a lei para que possa ser apresentada à justiça.
> b) Autêntica: as provas devem ser comprovadamente relacionadas ao incidente/crime investigado. O trabalho de uma documentação de qualidade é essencial para o cumprimento deste item.
> c) Completa: o conjunto de evidências deve fornecer uma apresentação completa acerca do evento investigado. Nunca deve depender de elementos faltantes ou duvidosos. Deve "contar a história" completa, e não apenas fornecer perspectivas particulares.
> d) Confiável: não deve haver incertezas acerca da autenticidade e veracidade das evidências, bem como sobre as formas como foram coletadas e posteriormente manuseadas durante a investigação.
> e) Convincente: além de todas as características anteriores, deve ser documentada e apresentada de forma clara e organizada (BRASIL, 2013).

Quando se trata dos termos vestígios, indícios e evidências, às vezes eles são utilizados como sinônimos, mas possuem significados distintos, cabendo ao investigador responsável pelo processo saber discernir as diferenças entre eles, analisando que: “Enquanto o vestígio abrange, a evidência restringe e o indício circunstancia" (DIAS FILHO, 2009 apud BRASIL, 2013).

O vestígio, no processo de investigação digital, se apresenta como um registro digital decorrente de uma prévia intervenção humana. Esses vestígios podem ser, por exemplo, os *logs* armazenados por um software, ou uma mensagem recuperada na web. Quando o investigador consegue obter, através de apurações analíticas, as informações contidas nos vestígios, é possível inferir sobre o vínculo deste com o ato criminoso em análise, deixando claro que as evidências obtidas partiram inquestionavelmente do computador investigado. A abrangência desses vestígios deve ser limitada na medida do que se fizer necessário o bastante para a estruturação dessa evidência, devendo esta ser coerente e restrita à sua utilidade e importância no processo (BRASIL, 2013).

Para o Processo Penal, art 239, o indício é a “circunstância conhecida e provada, que, tendo relação como fato, autoriza, por indução, concluir-se a existência de outras circunstâncias”.

Dessa forma, pode-se dizer que a evidência adquirida por meio dos vestígios coletados é dizer que a mensagem foi enviada por meio de determinado computador, objeto de investigação. Associado a este indício, outros fatores de ordem subjetiva podem contribuir para montar essas evidências, como o local onde estiver o computador e quem mora na residência. Portanto, no processo penal, as evidências serão formadas por elementos objetivos e subjetivos somados a diligências diversas e procedimentos periciais que se fizerem necessários. Todos esses fatores juntos possibilitam a conclusão da existência ou não de circunstâncias – que também podem ser considerados indícios – que serviram para o convencimento das autoridades competentes, são as provas materiais contidas no processo (BRASIL, 2013, p. 169).

A evidência digital pode ser entendida como qualquer dado armazenado ou transmitido através de um computador de forma que esses dados possam demonstrar ou refutar uma hipótese sobre o fato, ou seja, desde que este forneça elementos críticos determinantes para a investigação, tal como: premeditação, dolo ou álibi (CASEY, 2004).

Nesse sentido, pode-se constatar que os vestígios para obtenção das provas materiais, que servem para condenar ou absolver o suspeito do crime, precisam ser muito bem definidos e expostos ou, caso contrário, a defesa do acusado poderá alegar ilegitimidade da investigação (BRASIL, 2013).

É preciso se estabelecerem alguns métodos investigativos para que o poder punitivo do Estado, através da sua jurisdição, não seja desacreditado e, com isso, se estabeleça uma insegurança jurídica no país. Uma vez determinado o monopólio da função jurisdicional estatal, a resolução de conflitos entre os membros da sociedade passa a ser de sua responsabilidade e com ela a tarefa de exercer a persecução penal, ou seja, praticada uma contravenção penal, caberá a ele a apuração e o esclarecimento dos fatos e circunstâncias.

Para isso, em geral, temos três principais modelos de investigação preliminar:

a) Investigação preliminar policial liderada pela polícia investigativa;
b) Investigação preliminar judicial comandada pelo juiz instrutor;
c) Investigação preliminar protagonizada pela acusação- nesse caso, os ofícios de investigador e acusador (normalmente função do Ministério Público) são realizados pela mesma autoridade (COLLI, 2010, p. 76-77).

Os órgãos que poderão compor a polícia judiciária e polícia investigativa, com distintas atribuições, estão descritos no artigo 144 da Constituição Federal de 1988.

Normalmente, a investigação é realizada pela polícia judiciária quando se trata de questões administrativas e, quando chega à fase comprobatória, pela jurisdição penal.

A investigação preliminar faz parte da fase pré-processual e caracteriza-se por ser um momento esclarecedor da infração penal e seus autores para que seja formado o convencimento da acusação para uma possível denúncia. Dessa forma, busca-se evitar acusações infundadas contra os acusados afastando-se o risco de injustiça.

Nesta fase, busca-se averiguar a materialidade do fato, indícios e autorias. Com isso, a ordem, paz e harmonia sociais justificam a investigação preliminar como meio de resguardar a sociedade. Para que se alcance esse objetivo, devem-se olhar o delito e suas consequências, como fator de desordem social e, dessa forma, faz-se necessário uma minuciosa investigação em busca do ao autor do delito.

A investigação preliminar tem como principal objetivo a busca possível da veracidade do fato evitando injustiça e insegurança jurídica. Além disso, a investigação preliminar também deve ter, como função, filtrar uma eventual ação penal, desprezando provas sem valor e resguardando aquelas que, de fato, podem auxiliar na acusação assegurando a aplicação dos direitos e garantias fundamentais (COLLI, 2010, p. 76-79).

Com todas as especificidades que envolvem a investigação, principalmente as dificuldades para a solução do fato delituoso, é importante que se preserve o anonimato do investigador, pois assim como os rastros dos criminosos ficam registrados no computador, o do investigador também fica. Com isso, um criminoso mais hábil poderá facilmente identificá-lo. Assim, é preciso dedicar atenção para não ser identificado como parte integrante do processo investigativo.

Os registros que ficam no computador, mesmo os acessos em *website*, podem ser visualizados e identificados. Com os *IPs* de origem e o horário dos acessos realizados, é possível determinar uma série de informações sobre a localização geográfica, o provedor, instituição responsável pela rede e a motivação do acesso. Essas informações podem ser obtidas tanto do autor do fato delituoso, como de quem o investiga.

Esses rastros também podem ser encontrados em outros serviços da Internet, como, por exemplo, os *e-mail*s. Dessa forma, é fundamental que o procedimento de investigação seja realizado com configurações que não permitam que o suspeito imagine que está sendo investigado, nem quem o investiga.

É fato que o Cibercrime possui característica e meios de execução específicos. Tais peculiaridades também estão presentes no processo investigatório e, em especial, na investigação preliminar, desenvolvida neste ambiente. Com isso, é possível destacar quatro

questões relevantes que fazem com que o modelo de investigação atual – situações que envolvem somente o espaço físico tangível – seja repensado. Essas questões estão diretamente ligadas à natureza jurídica, aos sujeitos, ao tempo e/ou lugar do fato e às provas materiais obtidas dos crimes digitais (COLLI, 2010, p. 81).

Entretanto, para a definição de Cibercrime, a grande questão está justamente no primeiro item do que seja crime, a tipicidade, já que a grande problemática desses crimes é comprovar a tipicidade da conduta, pois, infelizmente, o Direito não caminha na mesma velocidade e parâmetros em que evoluem as tecnologias e com elas os meios de acesso e utilização. Apesar da nocividade que uma conduta virtual pode causar, se ela não estiver devidamente prevista na ordem jurídica, ou se não houver uma forma de registrar a atividade lesiva, dificilmente haverá apreensão de provas e, consequentemente, punibilidade. É o que ensina o Mestre indiano Jaishankar citado por Sydow:

> Outra característica do cibercrime é que a conduta em questão pode não ser ilegal (Brenner 2001). Em maio de 2000, o vírus 'Eu te amo' atravessou o mundo em duas horas e causou bilhões de dólares em danos em mais de 20 países. Ele foi rapidamente rastreado com origem nas Filipinas, onde agentes do FBI e autoridades locais identificaram um suspeito. Mas como a lei filipina não criminalizava a disseminação de vírus, levou-se dias para se conseguir um mandado de busca no apartamento do suspeito, dando-lhe tempo para destruir as evidências. E ainda havia o problema processual [...] tendo-se em vista que disseminação de vírus não era crime local, o suspeito não poderia ser extraditado para ser processado nos Estados Unidos, onde o fato era crime [...] ninguém nunca foi processado pela disseminação em tela. (JAISHANKAR, 2008 apud SYDOW, 2015, p.108).

Dessa forma, percebe-se que o grande desafio da investigação dos Cibercrimes – típicos, ilícitos e culpáveis – é o ato de desvendar, ou seja, não caminhar por terrenos desconhecidos para seus profissionais, isso porque a incerteza a respeito da existência ou não da tipicidade de um fato pode levar a uma investigação "ilegal" .

Quanto ao agente do cibercrime, não há um perfil prévio, mas necessariamente, a pessoa que comete tal delito deve inicialmente ter uma escolaridade razoável para manusear programas e conhecer um pouco de língua estrangeira. (SYDOW, 2015). A possibilidade da existência de dois "mundos" – virtual e real – faz com que as características de um não necessariamente estejam vinculadas ao outro. O sujeito do crime virtual pode ter um perfil completamente oposto ao do sujeito do mundo real, pois, ao contrário deste, que terá somente uma representação diante da sociedade, o sujeito virtual poderá assumir várias identidades ou oculta-se.

O anonimato, mesmo que não absoluto, do mundo virtual proporciona uma liberdade quase que inatingível no mundo real. Os computadores podem ser utilizados por quaisquer

pessoas. Os usuários trocam informações, interagem, comandam aparelhos sem a necessidade de exposição ou identificação, podendo atuar de modo velado. Em função desse anonimato, surge a insegurança quanto aos verdadeiros dados do usuário, notadamente, sua real identidade. Em poucos casos, o máximo que se consegue é a obtenção do *IP* da máquina. A anonimidade dificulta a identificação do infrator virtual e, consequentemente, sua punibilidade.

Seja em sites, em conversas de *e-mail*, redes sociais ou em dados armazenados de bancos de dados de quem procura emprego, a liberdade para assumir características diversas de gênero, idade ou religião é ilimitada. Essa liberdade permite que o sujeito assuma uma personalidade e identidade que corresponda ou não ao sujeito do mundo real. Ser e fazer o que quiser no mundo virtual impõem limites.

No mundo real, identifica-se alguém pelos dados, informações, documentação e forma visual. Já no mundo digital, essas informações e características que podem ser medidas por três aspectos:

a) Não há ou não deveria haver identidade na rede sem identificação numérica, ou seja, o computador de acesso deverá ter um número vinculado à rede que o identifique;
b) A identidade, seja ela qualitativa ou numérica será sempre de um computador, nunca de um sujeito;
c) Um endereço numérico, o IP, por exemplo, pode ser atribuído em um curto período de tempo a diferentes computadores, não podendo, entretanto, possuir o mesmo endereço, ao mesmo tempo, dois ou mais computadores.

Identificar o sujeito a partir do número IP, aparentemente parece fácil, entretanto, existem duas questões problemáticas a serem resolvidas pelos órgãos responsáveis pela investigação dos Cibercrimes. São elas:

a) A correlação em um determinado espaço de tempo entre endereço IP x máquina;
b) A correlação em um determinado espaço de tempo entre a máquina e o sujeito que a opera (COLLI, 2010, p. 89-91).

Portanto, para uma investigação de determinado sujeito suspeito ter respaldo legal, precisa ser embasada em fatos e circunstâncias muito bem definidos. Em caso de investigação criminal baseada na mera suspeição a partir da titularidade de contrato de Internet, permite-se que o suspeito possa responsabilizar penalmente a atividade policial e seus investigadores.

Dessa forma, deve-se deixar claro que o que irá identificar e/ou rastrear o sujeito suspeito do Cibercrime é o número de registro da máquina na rede – endereço de IP, MAC, etc. – e nunca do sujeito (COLLI, 2010, p. 92).

Já em relação ao tempo e ao lugar, com a expansão da rede de computadores, principalmente a Internet, hoje é possível superar as questões territoriais e de nacionalidade na prática de determinados crimes digitais. O ciberespaço permite que os usuários desse ambiente virtual trafeguem livremente por todos os países, praticando, por meio de máquinas e locais diferentes, seus crimes. Exatamente nessa liberdade de acesso ilimitados aos dados, informações e computadores, por qualquer pessoa e em qualquer lugar, é que está embutida a dificuldade de se realizar uma investigação policial de Cibercrimes com repercussão internacional.

Na atualidade, pode-se está em vários lugares, simultaneamente, em função das facilidades oriundas da alta tecnologia. Sydow exemplifica tal proeza, ao dizer que:

> A partir de tecnologias de conexão sem fios e a distância, uma pessoa pode conectar-se a um provedor a dezenas de quilômetros de distância, compartilhar arquivos através de ondas de rádio a muitos metros, e a impressão é a de que o usuário está nos dois ou mais lugares ao mesmo tempo [...] A sensação de simultaneidade é tamanha que a cada dia mais se busca profissionais capazes de gerir diversas informações, de naturezas diferentes, sem qualquer dificuldade. O conceito de simultaneidade, inclusive, trouxe idéias como a de participar de funerais a distância, controlar as câmaras de segurança de empresa ou casa a distância, ou, até mesmo, pelo celular, ligar a banheira da casa, para preparar um banho (SYDOW, 2015, p.107).

Os sujeitos que praticam esse tipo de crime podem estar em qualquer país e o provedor por meio do qual se conecta à Internet, estar em outro completamente diferente, assim como os dados os quais ele acessa ou o computador que ele utiliza e esses materiais serem de propriedade de outra pessoa que esteja em um país completamente diferente dos demais.

Enfim, há uma complexa rede transnacional e transterritorial de sujeitos ativos e passivos, bens jurídicos ofendidos e objetos materiais do delito que envolve a prática do Cibercrime (COLLI, 2010, p. 95).

6.2.4 Diretrizes estratégicas do processo investigatório

Diante da complexidade do tema, para entender a investigação dos crimes virtuais é preciso entender o processo investigativo, sua fase inicial, técnica e a fase consequencial da

investigação policial propriamente dita, sendo essas fases denominadas por Emerson Wendt e Igor Vinícios Nogueira de fase técnica e fase de campo.

Na fase técnica dos Cibercrimes, são analisadas as informações para se tentar localizar e identificar o computador utilizado para o delito. Essas análises são:

> a) Análise das informações narradas pela vítima e compreensão do fato ocorrido na Internet;
> b) Orientações à vítima com o intuito de preservar o material comprobatório do delito e a sua proteção virtual;
> c) Coleta inicial de provas em ambiente virtual;
> d) Formalização do fato criminoso por intermédio de um registro ou boletim de ocorrência, com a consequente instauração do feito;
> e) Investigação inicial referente aos dados disponíveis na rede mundial de computadores sobre prováveis autores, origens de *e-mail*s, registro de hospedagem de domínio;
> f) Formalização de relatório ou certidão das provas coletadas e apuração preliminar;
> g) Representação perante o Poder Judiciário para a expedição de autorização judicial para quebra de dados, conexão ou acesso. Também poderão ser solicitados os dados cadastrais para os provedores de conteúdo;
> h) Análise das informações prestadas pelos provedores de conteúdo. (JORGE; WENDT, 2013, p. 52-53).

Quando analisadas as informações recebidas dos provedores, se necessário, encaminha-se ao poder Judiciário outras representações para o mesmo provedor ou ainda, poderá ser solicitado deste provedor o conteúdo de dados que irão complementar o conjunto probatório coletado.

Após a identificação e localização do computador utilizado para a prática do crime, o passo seguinte é encaminham-se para a fase de campo quando será necessário o deslocamento do agente policial, sempre de maneira discreta, para fazer o reconhecimento operacional do local. Depois dessa identificação do endereço que corresponda a uma residência e/ou rede não corporativa, solicita-se, de imediato, ao Poder Judiciário um mandado de busca e apreensão.

A identificação do usuário do computador ou ainda do meio pelo qual foi cometido o crime ocorre através de um processo investigativo que, para um melhor entendimento da matéria, pode ser dividido em modalidades que permitem a coleta das evidências, provas e punição das ações ilegais. Para entender melhor, eis algumas explicações, sobre registros, identificações, correios eletrônicos, dentre outros.

I- *LOGS*

Os *Logs* representam os registros ou anotações das atividades realizadas por programas de computadores. “No caso de *logs* relativos a incidentes de segurança, eles

normalmente são gerados por *firewalls* ou por IDSs [...] (Intrusion Detection System- Programa ou conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas." (PINHEIRO, 2013, p.492). Mesmo quando o usuário acessa um computador distinto do seu, os dados de suas ações ficam consignados (seja a rota ou curso trilhado pelas informações, sejam os pacotes que forem gerados). O usuário não consegue identificar a maneira como são expedidas as mensagens e nem o endereço do IP. Todo o acesso é facilitado pela interface dos dispositivos, deixando a parte complexa dos registros por conta de programas que gerem as informações necessárias.

Entretanto, mesmo não visíveis, as ações realizadas na Internet ficam anotadas virtualmente. Desse modo, registram-se o teor dos dados acessados, enviados, manipulados ou ainda, o tempo, lugar e modo como foram acessados os conteúdos, gerando os *LOGS* ou registros das ações.

Tais registros são necessários para o procedimento investigatório dos Cibercrimes, sejam esses cometidos por intermédio de chats, sites, *e-mail*s, redes sociais, ou qualquer outro meio interconectado. Dessa forma, o anonimato atribuído ao uso da rede não é tão eficaz assim, já que há a possibilidade de saber-se não só o local que o usuário acessou, mas diversos outros dados (CAVALCANTE, 2013).

II – Investigação de/em sites

Para uma melhor compreensão e análise do procedimento policial, envolvendo sites, é preciso que o agente investigativo tenha bastante conhecimento informático e conheça a sistemática dos nomes de domínios e como eles ficam disponíveis aos usuários. O percurso feito pelo registro dos acessos à Internet pode ser simplificado da seguinte forma: cabe ao internauta, digitar no seu *browser* ou programa de navegação, o endereço de domínio que, em seguida, será traduzido para o número IP, ofício desempenhado pelo servidor DNS (Domain Name System, relacionado a um sistema de nome e domínio) (JORGE; WENDT, 2013, pg.54-66).

No momento em que um site é criado, seu domínio necessita ser registrado na Rede Mundial de Computadores. No território brasileiro, esse controle é feito através do Comitê Gestor da Internet, por meio do Registro.com, sendo que cada Estado adota seu procedimento e órgão para efetuar o registro (CAVALCANTE, 2013). Pelas normas brasileiras, o domínio, para o registro na rede deve estar disponível e respeitar algumas regras (como não conter somente números, não iniciar ou terminar com hífen, etc).

Também são necessários pelo menos dois servidores DNS respondendo com autoridade pelo nome solicitado. Além disso, deve-se escolher a categoria pessoa física ou jurídica, para depois definir o nome de domínio e registrá-lo. Vale ressaltar que nomes adicionais podem se referir a computadores específicos de uma rede e não a um domínio secundário.

Cada país tem sua forma de efetuar o registro. Assim, em uma investigação, cada Estado pode ser identificado pela sua terminação e referência. No Brasil (e em alguns países), para registrar o domínio na Internet, é preciso fornecer o CPF ou CNPJ e pagar um valor previamente determinado, não havendo necessidade do envio de documentos, aumentando assim a possibilidade de crimes virtuais, em razão das informações e dados falsos.

O registro de um nome de domínio e as informações quanto a seus servidores DNS não significa dizer que o site está ativo e visível a todos. Para isso, é preciso que ele esteja hospedado em algum servidor, mesmo que seja o do proprietário do domínio.

A facilidade para a obtenção do registro na Internet acaba dificultando a investigação dos crimes virtuais, pois a possibilidade de fraude é muito grande e o controle é quase impossível, sendo necessário solicitar ao gestor de cada país as informações necessárias do usuário. No Brasil, por exemplo, pode-se entrar em suporte/ferramenta/serviço de diretório *whois* do site www.registro.br onde é possível obter dados cadastrais do internauta, tais como: a pessoa responsável pelo domínio e seu registro tributário, o servidor encarregado de manter site ativo, contatos de ordem técnica, dentre outros. Cabe ressaltar que, geralmente, os sites encontram-se hospedados em computadores de empresas que prestam serviços (JORGE; WENDT, 2013).

Com as informações do número do IP, onde o site está hospedado, o nome de domínio e solicitando aos provedores os *logs*, torna-se possível, porém não fácil, identificar o(s) autor(es) do crime. Esses dados também podem ser utilizados para encontrar informações através de busca em fontes abertas, a exemplo do Google.

Quem participa dessas investigações precisa ter capacidade técnica adequada para analisar toda espécie de teor constante no site investigado, pois a falta de percepção pode deixar passar dados relevantes para o desfecho do crime.

Com isso, no site, existem três informações importantes para o processo de investigação: identificação do “proprietário”; identificação dos servidores DNS; e identificação da responsabilidade pela hospedagem. (JORGE; WENDT, 2013, pg.54-66).

Dessa forma, é necessário que a originalidade do conteúdo da página investigada seja mantida para que os dados não sejam perdidos ou fraudados. Com isso, também, buscam-se

evitar possíveis questionamentos no processo penal sobre a veracidade das provas e a preservação das informações sem alteração. Sendo assim, o ideal é fazer o *download* das páginas utilizando-se ferramentas que produzem uma assinatura digital, com a qual se pode constatar a originalidade do teor apreendido (CAVALCANTE, 2013).

III - Endereço IP

No processo de investigação dos Cibercrimes, as evidências deixadas no endereço do IP são de considerável importância. Na navegação e utilização de computadores em rede é relevante que haja o endereço ou número que identifique o maquinário. As organizações competentes para a distribuição do IP são: a IANA (responsável pela coordenação global dos DNS raiz, endereçamento de IP, protocolo, etc.) e a LACNIC (autoridade de distribuição regional de endereços IPs em blocos da América Latina e Caribe, tendo como destinatários, os provedores e usuários finais). Caso as instituições sejam localizadas em território brasileiro, devem requerer "[...] os Recursos Internet (blocos IPv4, IPv6 e ASN) diretamente ao NIC.BR, que é o Registro Nacional Internet para o Brasil" (JORGE; WENDT, 2013, p.67).

Separadas por pontos, a sequência numérica compõe-se do formato XXXX, "sendo que o X corresponde a números variáveis entre 0 e 255. Por exemplo, o número 200.221.2.45 é o número IP do site www.uol.com.br" (CAVALCANTE, 2013).

Em regra, os endereços de IP da versão 4 no Brasil começam por 177, 187, 189, 200 e 201. Vale ressaltar que também é possível existir IPs privados, intitulados inválidos, que podem gerar dúvidas, especialmente quando:

> [...] aparecem em cabeçalhos de *e-mails* (ou em outras plataformas utilizadas para prática de crimes cibernéticos) ou em respostas às solicitações judiciais advindas de administradores de redes ou de TI. [...] Os IPs considerados válidos são aqueles que podem ser acessados diretamente pela Internet e são divididos em três classes: A: 1.0.0.0 a 126.0.0 B: 128.1.0.0 a 191.255.00 C: 192.0.1.0 a 223.255.0 Já os considerados inválidos, na verdade, são aproveitáveis apenas para redes locais privadas, como por exemplo escritórios, residências, etc. São eles: A: 10.0.0.0 a 10.255.255.255 B: 172.16.0.0 a 172.31.255.255 C: 192.168.0.0 a 192.168.255.255 (JORGE; WENDT, 2013, p.67).

Mas, havendo um envio de e-mail, por exemplo, será atribuído um número de IP. Notadamente, muitas instituições ou organismos públicos e privados possuem uma faixa de IPs que não se altera. Em contrapartida, o usuário comum recebe das operadoras um número de IP que se altera a cada conexão realizada. A partir do momento que o endereço IP revela o provedor de acesso, torna-se possível, em algumas situações, identificar o local aproximado da conexão. "Isso porque muitos provedores usam endereços IPs específicos para

determinadas regiões ou, às vezes, são provedores locais que atuam somente em uma cidade ou estado" (CASSANTI, 2014, p. 88). No entanto, é bom registrar que a obtenção do endereço IP não implica, necessariamente, na localização geográfica do usuário. É o que ratifica Cassanti:

> Por exemplo, um internauta pode usar uma conexão discada para se conectar a um provedor europeu e terá um IP na Europa, independentemente do lugar físico do computador. Para obter outras informações é preciso que a polícia obtenha uma ordem judicial para que o provedor revele os dados do assinante que estava com o endereço IP em uma determinada hora e dia. O detalhe da hora e data é importante porque é comum receber um novo endereço IP a cada vez que se conecta. Logo, sem uma informação precisa sobre a data e hora não é possível determinar quem pode estar usando um endereço. (CASSANTI, 2014, p. 88).

Nesse sentido, no processo de investigação, é necessário solicitar às concessionárias do serviço a identificação do usuário de determinado IP, bem como dia, horário e fuso horário em que foi utilizado.

É imprescindível abordar, neste ponto, duas questões correlativas altamente complexas trazidas por Colli e que devem ser enfrentadas pelos órgãos investigadores dos cibercrimes:

a) A correlação-espaço/tempo entre o endereço IP x Máquina;
b) A correlação-espaço/tempo entre Máquina x Sujeito que a opera.

Ao tratar da primeira questão, Maciel Colli apresenta o exemplo de um endereço IP X "gravado pelos servidores de um banco que foi furtado. O furto se realizou a partir de uma operação bancária não autorizada por meio da internet, às 12 horas, do dia 04.05.2009. Como descobrir a que máquina este endereço IP pertencia ? "(COLLI, 2010, p.90). Neste caso, foi identificado o IP,o provedor detentor do *IP*,a conta do usuário e o contratante do serviço de acesso à Internet.Foram obtidos os registros do *IP* atribuído ao roteador *wireless* na hora em que houve a conexão.No primeiro momento, a aparente autoria recai sobre o proprietário do roteador *wireless*, mas, ainda assim, seria necessário analisar *os logs(*registro das atividades) do roteador(caso existam) no intuito de localizar o endereço *MAC(* Media Access Control) ou seja, o endereço de controle de acesso da placa de rede,do suposto invasor. Identificando o referido endereço, o investigador poderia associar o IP encontrado à máquina.Ocorre que, já ciente disso, o cibercriminoso falsifica o *MAC* e, consequentemente, fazendo desaparecer assim, um importante indício que permitiria relacionar o endereço *IP* a máquina.

O segundo problema é ainda mais complexo, pois aliar máquina x sujeito que a opera, requer muita cautela e sensatez investigatória, uma vez que está em jogo a possível autoria de um delito, no cerne de uma investigação policial, que poderá culminar num possível processo

penal. As identificações ocorridas na esfera virtual, vistas até agora, são referentes ao maquinário e não a pessoas. Basear qualquer procedimento investigatório em meras suspeitas, em indícios ainda incertos no tocante ao titular da conduta delituosa representa uma ameaça à segurança jurídica. Sendo assim, para evitar injustiças, Maciel Colli aponta uma característica importante de considerável parte dos cibercrimes, que é sua natureza de delito permanente, ou seja, cuja consumação se protrai no tempo (enquanto durar o crime). Tal peculiaridade faculta a possibilidade de uma prisão em flagrante, no momento da execução criminosa, afastando as dúvidas quanto ao titular do delito.

> Portanto, tratando-se de uma investigação preliminar policial de um cibercrime, em especial se de natureza permanente, crê-se e sustenta-se ser necessária não só a prisão em flagrante do sujeito suspeito que opera uma máquina associada a um endereço IP, mas também que esta mesma máquina esteja operante. O risco do não atendimento a estes requisitos aqui apresentados poderia ensejar: a) para a investigação preliminar policial: a ausência de vestígios de materialidade (máquina desligada) e/ou a ausência de indícios suficientes de autoria (prisão em flagrante do sujeito passivo), a ensejar posterior trancamento do processo penal pela via do *habeas corpus* ou posterior arquivamento de inquérito policial pelo órgão competente; b) para a ação penal: a ausência de justa causa a ensejar a falta de uma das condições da ação penal, restando como consequência a rejeição da denúncia ou queixa (CPP, art. 395 e 396). (COLLI, 2010, p.95).

Conforme visto acima, num procedimento preliminar investigatório acerca dos cibercrimes, além da análise pormenorizada e técnica de todos os dados encontrados, tratando-se de um delito permanente, seria juridicamente cabível a prisão em flagrante do suspeito(ligado ao endereço *IP*) de uma máquina operante.

IV- Investigação de crimes envolvendo e-mail (correio eletrônico)

Alguns crimes virtuais podem proceder do envio de mensagens de *e-mail* com o objetivo de ofender, caluniar, difamar, além de difundir e estimular a pornografia infantil e programas maliciosos. Assim, é preciso ficar atento não só aos conteúdos criminosos, mas também aos dados do destinatário e remetente da correspondência eletrônica, o cabeçalho do *e-mail*.

Cabe ao investigador compreender todo o processo de formação, registro e hospedagem de domínios para melhor entender a origem de um *e-mail* nocivo. Assim, ao se observarem esses dados, é possível identificar o autor da mensagem. Mas, novamente, é importante frisar a imprescindibilidade do conhecimento técnico para realizar a expansão do cabeçalho e obter o acesso pleno ao conteúdo e, com isso, identificar a origem do *e-mail*.

Realizada, minuciosamente, a análise do *e-mail*, é possível obter os principais dados como o endereço IP, a data, hora e *time zone* da expedição da mensagem, buscando-se preservar os dados e evitar fraudes. Além disso, essa expansão do cabeçalho pode ser realizada por meio de ferramentas disponibilizadas pelos provedores de contas de *e-mail*, mas cada provedor possibilitará esta expansão de forma distinta, devendo ocorrer uma análise caso a caso.

Caso não seja possível a expansão do cabeçalho, mas, ao investigar a conta do *e-mail*, podem-se solicitar, ao provedor do serviço, informações e registros de eventos dessa conta. "É comum um cabeçalho possuir várias linhas que começam com a palavra *received*. A palavra mostra por quantos servidores a mensagem passou antes de chegar ao destinatário. O parágrafo que interessa é sempre o último *received"* (CASSANTI, 2014, p.59).

Após a coleta de dados do provedor da conta, procura-se um site de leitura de IPs, (como o www.en.trace.de, ou www.registro.br) e identifica-se qual o provedor de Internet que forneceu aqueles IPs. Com essas informações, solicitam-se a este os dados cadastrais de quem usou o IP (por ele fornecido) no dia, hora e fuso horário enviados e, a partir daí, pode-se chegar à localização física de quem acessou a conta de *e-mail*, da qual não existia nenhum dado preliminarmente (CAVALCANTE, 2013)[101].

Havendo impossibilidade de se identificar dados importantes como, data, hora, *IP*, mas seja possível obter o endereço eletrônico de quem enviou a mensagem, tanto o MP quanto a autoridade policial pode requisitar a quebra do sigilo de dados por ordem judicial para que o endereço *IP*, data e hora sejam fornecidos pelo provedor do *e-mail.* (CASSANTI, 2014).

É importante alertar para não se encaminhar o *e-mail* com o conteúdo ofensivo para ninguém, nem mesmo para a autoridade policial. "Fazendo isso você simplesmente está destruindo evidências sobrescrevendo o header (cabeçalho) da mensagem original por *tags* do seu provedor de *e-mail* SMT" (CASSANTI, 2014, p. 66).

Cabe lembrar que em casos de ameaças e delitos contra a honra, feitos por *e-mail*, é necessário preservar o teor da mensagem, além de identificar o cabeçalho e guardá-lo impresso como elemento probatório.

Ao longo das últimas décadas, o *e-mail* conquistou um lugar de grande relevância como meio de comunicação e informação, no entanto, passou a ser também, uma forma altamente nociva e eficaz de ataque virtual, causando inúmeras ofensas a vários bens

[101] https://jus.com.br/artigos/25743

jurídicos. São muitas espécies de vírus, golpes, ofensas, fraudes, clonagens e *spam* que desafiam a justiça e traz insegurança aos usuários. E tudo é fruto de uma curiosidade ingênua, ou, às vezes, por puro desconhecimento, quando se vê, já se clicou e as portas virtuais são abertas para criminosos reais.

V - Redes sociais online

O termo "rede" refere-se à estrutura que tem um padrão característico, onde na informática pode ser definida como um conjunto de equipamentos interligados que partilham informação. Já "social", significa aquilo que pertence ou que é relativo à sociedade[102]. Uma rede social *online* está relacionada a uma estrutura na Internet, onde um grupo de pessoas mantém algum tipo de vínculo, podendo ter funções e relações distintas, de acordo com o interesse dos utilizadores.

Essas redes sociais fazem parte da rotina diária de grande parte da população mundial, que está conectada quase que 24 horas por dia. Elas não apenas interligam pessoas, mas também empresas, sendo um espaço para relacionamentos, negócios, *marketing*, entretenimento, etc.

A exemplo dessas redes sociais pode-se citar o gigantesco Facebook, criado em 2004, que recebeu o título de maior rede social do mundo (G1, 2015)[103], tornando-se um negócio bilionário, devido aos seus anúncios de propagandas. Segundo dados divulgados por Mark Zuckerberg, diretor executivo da rede social, o Facebook conta com cerca de 1,49 bilhão de usuários no mundo todo, dos quais 1 bilhão acessa a rede social diariamente (G1, 2015). No Brasil, são 92 milhões de usuários, fazendo com que o país seja o segundo no mundo em acessos diários, ficando somente atrás dos Estados Unidos, lar da companhia (KATCHBORIAN, 2015)[104].

O grupo de Mark também controla o WhatsApp, que chegou recentemente à marca de 900 milhões de usuários em todo o mundo (HAMANN, 2015)[105], onde 100 milhões são brasileiros, tornando-se o aplicativo mais utilizado no país. Devido à explosão das redes sociais, certos serviços acabaram se tornando obsoletos, como os *e-mails* e as ligações telefônicas. Apesar de servirem para finalidades positivas, como relacionamentos, troca de conhecimentos e informações globais, elas também funcionam como refúgio para pessoas mal

[102] http://conceito.de/rede-social
[103] http://g1.globo.com/tecnologia/noticia/2014/02/facebook-completa-10-anos-veja-evolucao-da-rede-social.html
[104] http://dicascidade.com.br/entretenimento/com-1-4-bilhao-de-usuarios-facebook-agora-e-a-maior-nacao-do-mundo/
[105] http://www.tecmundo.com.br/whatsapp/85923-whatsapp-atinge-marca-900-milhoes-usuarios-ativos.htm

intencionadas e criminosos virtuais, que utilizam desse meio para praticar atos ilícitos e se beneficiarem do anonimato. Tal fato faz com que as redes sociais escondam perigos diversos, principalmente devido a grande exposição à qual os usuários estão submetidos, destacando-se as crianças e os adolescentes – vítimas fáceis de serem atingidas pelos cibercriminosos, devido à maior abertura para os contatos virtuais. Também são praticados diversos ataques, como a espionagem, terrorismo, guerra e protestos.

VI - Busca eletrônica

A era da tecnologia da informação fez com que a internet passasse por um grande desenvolvimento nos últimos anos, evoluindo bem mais rapidamente que o preparo dos agentes policiais capacitados para lidar com as investigações dos diversos tipos de crimes virtuais. A rede mundial de computadores permite que sejam utilizados recursos para facilitar a solução de diversos crimes, não se limitando apenas aos ocorridos na Internet (*cibercrimes*).

Com o constante uso das redes sociais e dos *websites*, propiciou-se uma maior abertura para se chegar às informações necessárias ao sucesso das investigações criminais. Isso desencadeou um mundo virtual mais transparente, principalmente em relação às informações oriundas dos órgãos públicos e da imprensa, que são encontradas muito facilmente a um toque na tela do computador.

Todavia, a *Web* armazena uma quantidade muito grande de informações relevantes, tanto para os criminosos, quanto para os investigadores. Dados pessoais são disponibilizados a todo o momento nas diversas redes sociais, onde as pessoas se expõem, muitas vezes além do devido. Em razão de toda essa exposição, é possível obter informações importantes, que podem até identificar criminosos e a localização de pessoas. Assim como os criminosos, os investigadores também conseguem se infiltrar em grupos ilícitos, criando os chamados perfis *fakes* e adquirindo a confiança dos membros para obter assim, informações necessárias e relevantes à solução dos mais variados crimes.

Todos os dias, fotos, vídeos e outras informações podem ser colocados indevidamente na Internet, podendo ser retirados do site ou da rede social em que tenha sido feita a publicação. Para isso, a vítima deve possuir alguma prova (imagens ou *prints*, por exemplo), e recorrer aos juízes especiais, que podem receber reclamações e decidir pela retirada do material de sites com mais rapidez (FAVORITO, 2015)[106].

[106] http://fernandafav.jusbrasil.com.br/noticias/114588701/com-marco-civil-juizes-podem-tirar-conteudo-mais-rapidamente?ref=topic_feed

6.2.5 **Gestão jurídico-estratégica no enfrentamento dos Cibercrimes**: desafios e perspectivas

O Cibercrime, no mundo contemporâneo, tornou-se um grande vilão da persecução penal, sendo imprescindível a capacitação adequada de todos os envolvidos no processo de investigação, bem como o judiciário, já que essa modalidade de crime traz imensos prejuízos à sociedade, além de ameaçar a questão da soberania estatal. Por isso, faz-se necessário adequar e solucionar algumas dificuldades presentes no mundo tecnológico.

Entre elas, podemos destacar a de se obter a origem de um evento na Internet e formar as evidências eletrônicas necessárias para identificar e condenar os autores dos fatos delituosos. Os usuários acessam seus computadores e também a rede mundial de computadores e sequer sabem quais os registros/*logs* são gerados por esse uso. Assim, costuma-se referir que esse acesso ocorre, em sua maioria, na pura inocência, pois, em geral, os usuários não precisam se preocupar com pacotes, endereços e IP ou rota.

Dessa maneira, após a obtenção do endereço IP correspondente a uma ação na Internet, adquire-se a identificação do local onde se originou o registro. Mas, infelizmente, existem meios de burlar estas evidências como os *proxies*, as redes *wi-fi* abertas, os *cybers cafés* e *lan houses*, além do uso de documento falso em cadastros, exigindo do investigador maior atenção para estes obstáculos (CAVALCANTE, 2013).

O trabalho difícil de gestão das atividades de nível mais básico da rede é realizado por programas e aplicativos. Os usuários interagem com estes programas através da interface do usuário. A maioria dos *hosts* da rede não possui funções de monitoramento, que são, em grande parte invisíveis e automáticos. Porém, quase todas as atividades de rede acabam sendo registradas em algum lugar.

Os *proxies* são serviços que ocultam o verdadeiro IP, utilizando o rastreamento de um determinado evento, de quem realizou a conduta. Tal mecanismo termina facilitando o anonimato na Internet. Ao se permitir o uso de portáteis como *smartphones*, *tablets* e *notebooks* em redes sem fio abertas, liberando o acesso à Internet, torna-se uma abertura para os ciberdelinquentes, possibilitando o uso da rede para fins ilícitos e dificultando a localização e identificação dos usuários.

Os *logs*, conforme já foi visto, são registros das atividades realizadas pelos usuários, configurando-se em importantes evidencias na apuração dos ciberdelitos. No entanto, não há legislação que normatize o arquivo desses registros, prejudicando assim, a ação investigatória.

Também merecem consideração os arquivos ou a computação nas nuvens ou *Cloud Computing.* Trata-se de serviços que proporcionam o acesso a programas, arquivos e a realização de diferentes tarefas pela rede, sem que estes arquivos estejam armazenados no maquinário do internauta. Caso o usuário deseje acessar arquivos, ele não precisa conectar-se do seu computador, necessariamente, podendo visualizar tais documentos em qualquer outro aparelho que permita o acesso à Internet. Um exemplo desta ferramenta é o *dropbox*, que permite a duplicação dos arquivos no servidor hospedeiro (CAVALCANTE, 2013)[107].

Apesar de útil, essa tecnologia dificulta a investigação criminal, pois sempre haverá problemas para apreender um computador que esteja em outro Estado, ou então haverá demora desses provedores em prestarem as informações solicitadas e para retirar os sites do ar, emperrando o serviço investigativo e tornando-se uma ameaça ainda maior à segurança na rede (JORGE; WENDT, 2013, p. 131).

Com tantos empecilhos enfrentadas no processo de investigação, identificação e punição dos Cibercrimes, é essencial o investimento do Estado no preparo da Polícia, Judiciário e Ministério Público, uma vez que, mesmo com uma vasta aplicação e difusão desse processo, os órgãos responsáveis por essa investigação ainda não estão adequadamente preparados para lidar com essa modalidade de crime. Infelizmente, ainda é possível constatar que, nesses órgãos, existem agentes sem qualquer conhecimento técnico na área tecnológica, terminologias e pontos do Cibercrime que afetam diretamente a sociedade (CAVALCANTE, 2013).

Com esse cenário ainda existente, a cooperação internacional, seja da polícia ou do judiciário, torna-se fundamental para enfrentar e combater os Cibercrimes, uma vez que esse tipo de crime tem como característica a transnacionalidade da Internet.

"Em razão de o Brasil ser signatário de um tratado para cooperação judicial – Mutual Legal Assistence Treaty- MLAT – órgãos investigativos do país podem representar pela concessão desse tipo de medida investigativa" (JORGE; WENDT, 2013, p. 132).

O Brasil ainda faz parte da rede para assuntos de crime de informática – *network for computer crime matters* – e, conforme o acordo assinado entre os países membros, em território brasileiro o contato localiza-se no núcleo de Crimes de Informática da Polícia Federal. A *network* faz parte de rede 24/7 do G8, também propagada para outras nações, inclusive para o nosso país, tendo como escopo a cooperação internacional no âmbito jurídico já que é uma rede menos formal, tendo como funções importantes a manutenção de evidências

[107] https://jus.com.br/artigos/25743

digitais e a retirada, dependendo para tanto, da legislação das nações destinatárias. A rede é internacional, com vasta gama de informações, possuindo usuários em várias partes do globo (JORGE; WENDT, 2013, p. 132).

Da mesma forma que as informações são globalizadas, o preparo, a execução e os resultados do Cibercrime também ocorrem nos diferentes quadrantes do mundo. Os criminosos virtuais, de diferentes regiões do planeta, se unem para realizar ataques a partir de suas fronteiras. Por isso, a cooperação penal internacional é uma necessidade premente para desarticular e coibir as ações criminosas.

A expansão da Internet, juntamente com o aumento dos provedores e serviços, concomitantemente, com o elevado número de usuários, alarga as interconexões em toda a aldeia global. Em contrapartida, urge a união de investigadores, membros do *parquet*, assim como magistrados em distintas partes do mundo para uma maior cooperação investigatória transnacional.

Infelizmente, ainda há muita burocracia nessa cooperação, sendo necessária a urgência no aperfeiçoamento da colaboração técnica entre países para a repressão a crimes cometidos pela rede mundial de computadores, sendo imprescindível a comunicação entre os policiais e os órgãos judiciários para atender à velocidade dos crimes que circulam de forma virtual (JORGE; WENDT, 2013, p. 131-141).

Os prejuízos causados pelos Cibercrimes são de grandes proporções. Segundo a Federação Brasileira de Bancos – FEBRABAN – apesar do investimento na prevenção e no combate a essa modalidade de delito, no ano de 2013, eles provocaram um prejuízo de 8 bilhões de reais para as instituições bancárias. No mundo todo, o prejuízo com as fraudes eletrônicas é devastador.

É verdade que esses dados estão muito aquém da realidade, de modo que os prejuízos decorrentes da prática dos Cibercrimes atingem patamares superiores. O principal aspecto para justificar esse ponto de vista é o fato de muitas pessoas não comunicarem à polícia sobre as ocorrências das quais são vítimas por intermédio da rede mundial de computadores.

Dentre as possíveis causas da subordinação, podem-se citar, como já visto, o sentimento de impunidade que gira em torno da prática desses crimes, o desconhecimento sobre as possibilidades de eles serem investigados e até, em alguns casos, o desconhecimento da vítima sobre a utilização dos recursos tecnológicos para a realização da ação criminosa. Além do caso de empresas que foram vítimas, mas não querem denunciar com receio de perder clientes, em razão da vulnerabilidade do sistema de segurança organizacional.

Os cibercriminosos conseguem obter lucros superiores aos auferidos por narcotraficantes. No Brasil, conforme rotineiras divulgações, o perfil dos criminosos virtuais é voltado principalmente para as fraudes eletrônicas. O prejuízo, conforme divulgado pela empresa de antivírus Symantec, chegaria a US$114 bilhões, o que torna o assunto ainda mais preocupante (JORGE; WENDT, 2013, p. 230-231).

Em que pese todos estes ciberataques (e seus prejuízos), assim como os demais Cibercrimes já analisados, há, no cenário atual brasileiro, uma reação que vem crescendo e tem como objetivo precípuo enfrentar os mencionados entraves que dificultam a investigação e, consequentemente, a punibilidade dos ciberataques no cenário nacional. Tais reações podem ser expressas na criação de organismos, legislações e na mobilização de instituições que visam ao aprimoramento da investigação e à eficácia na punição da cibercriminalidade.

Neste sentido, por meio de uma força- tarefa, algumas operações, envolvendo a Polícia Judiciária da União, Polícia Federal e Ministério Público, foram implementadas para o combate aos Cibercrimes. Somando-se a isso, foram criados órgãos e algumas medidas legais empreendidas buscando os avanços da Segurança Cibernética no Brasil, especialmente, nos últimos três anos.

Seguindo este raciocínio, em 2013, os fatos mais importantes quanto a esse tema foram: as publicações de Normas Complementares como a NC 17/IN01/DSIC/GSI/PR que estabelece diretrizes para a atividade dos Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF); e a NC 18/IN01/DSIC/GSI/PR que contemplou as linhas diretivas para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da administração Pública Federal (APF). Neste mesmo período, pôde-se destacar a Portaria SAE/PR nº 124 que criou o Grupo de Trabalho Interministerial (GTI) objetivando empreender propostas de Plano Estratégico para impulsionar os trabalhos a respeito das políticas públicas de ciberdefesa no espaço cibernético nacional. O artigo 3° dessa Portaria apresenta especificação dos membros Titulares e Suplentes que representam órgãos integrantes do GTI como o SAE/PR; MD; ANATEL; TELEBRÁS, etc. O Decreto Legislativo n º 3703 também representa essencial progresso na área da ciberdefesa, atualizando a Estratégia Nacional de Defesa e aprovando o Livro Branco de Defesa Nacional, reforçando a importância dos campos referentes a capacitação, inteligência, pesquisa, doutrina e gestão na proteção do ciberespaço (BRASIL, 2015).

Em 2014, a NC 07/IN01/DSIC/GSI/PR foi revisada, sendo instituída a “Biometria” como controle de acesso. Além disso, publicaram-se normas complementares à IN 01

GSI/PR, como a NC 19/IN01/DSIC/GSI/PR que destaca os Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta. Também foi publicado o Acórdão 3.051/2014 – TCU-Plenário de 5 de novembro de 2014, referente ao processo do TCU nº 023.050/2013-6, que traz especificações sobre as auditorias pelas quais são responsáveis órgãos da Administração Pública federal para avaliar a implementação dos controles de TI. A Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet (tema já analisado nesta pesquisa), institui princípios, garantias e regras para a utilização da Internet no âmbito nacional. Em 02 de maio de 2014 saiu a Portaria Interministerial MP MD MC nº 141 (regulamentando o Decreto nº 8.135/2013) que organiza a Administração Pública Federal, responsabilizando-a pela realização de suas comunicações, armazenamentos e recuperações de dados através de redes de telecomunicações e serviços de tecnologia de informação fornecidos por órgãos ou entidades da sua competência (SERPRO, TELEBRÁS, DATAPREV, etc). Outro importante destaque na área no período de 2014 foi a publicação do Relatório Final da CPI da Espionagem, elaborado pela Comissão Parlamentar de Inquérito (que investiga a denúncia do sistema de espionagem do governo dos Estados Unidos). E, a partir daí, a elaboração de uma Estratégia Nacional de Segurança Cibernética, traçando as principais medidas de cibersegurança para o Brasil, contando com a colaboração entre os setores público e privado (BRASIL, 2015).

Destaca-se, também, a operação de combate à fraude bancária denominada CORRIEU, ocorrida em novembro de 2014, em São Paulo, a fim de conter uma quadrilha responsável por roubo de cartões bancários, totalizando valor aproximado de 20.000.000 reais em fraudes. Em setembro do mesmo ano, a famosa IB2K, no Distrito Federal suprimiu a organização criminosa que faziam lavagem de dinheiro e furtos em contas de pessoas que realizavam compras virtuais que totalizaram cerca de dois milhões de reais, resultando a operação em várias prisões, buscas e apreensões dos agentes. Outra operação ocorrida em São Paulo, em março de 2014, conhecida como Tentáculos III, desarticulou uma organização criminosa voltada para fraudes com furtos de cartões bancários nos estados de São Paulo e Minas Gerais, ocasionando um prejuízo às vítimas de R$ 720.000.

Em 2015, os destaques são a operação SHEIK, ocorrida no mês de março em Goiás, na qual foi decretada a prisão do maior fraudador de Internet Banking da CEF SRCC/DICOR/DPF. Em outubro do mesmo ano, a operação Gênesis foi deflagrada, representando um marco no combate à pornografia infantil, com parcerias nacionais (MP e PF) e internacionais, ocorrendo em Alagoas, Acre, Ceará, Espírito Santo, Maranhão, Goiás,

Rio Grande do Sul, entre outros locais. Foram realizados cerca de quarenta mandados de busca e apreensão e as investigações foram baseadas em identificação dos usuários de redes sociais, serviços de *e-mail*s e armazenamento de arquivo proibido e distribuição. Houve também no período de 2015, a regulamentação do Marco Civil da Internet, Lei nº 12.965/2014, por intermédio de consultas públicas pelo Comitê Gestor da Internet e pelo Ministério da Justiça. A alteração da Instrução Normativa SLTI nº 04, em 12 de janeiro de 2015, estabeleceu a "Estratégia Geral de Tecnologia da Informação e Comunicações (EGTIC) – 2014/2015", contendo um instrumento de gestão do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), estabelecendo diretrizes de Tecnologia da Informação e Comunicações (TIC), e definindo planos estratégicos. Outro destaque foi o Decreto nº 8.414, de 26 de fevereiro de 2015, que instituiu o Programa "Bem Mais Simples Brasil" que visa simplificar o fornecimento dos serviços públicos proporcionando maior eficiência da gestão pública, inclusive na atuação em áreas de ciberdefesa (BRASIL, 2015).

E, por último, uma iniciativa importante: o presidente da Câmara dos Deputados, Eduardo Cunha do PMDB, anunciou a CPI de Crimes cibernéticos protocolada em fevereiro deste ano de 2015, junto a outras duas novas Comissões Parlamentares de Inquérito. A CPI surgiu em razão da percepção da gravidade dos crimes que ocorrem por intermédio da *web*, representada pelo relatório da Central Nacional de Denúncias de Crimes Cibernéticos, que aponta o crescimento de quase 200% entre os anos de 2013 e 2014 (dados já apresentados nesta pesquisa). A Comissão pretende investigar, por exemplo, a já discutida Operação IB2K, realizada pela Polícia Federal em 2014, desarticulando uma quadrilha que teria desviado cerca de R$ 2 milhões objetivando principalmente comprar armas e drogas. Tais ações criminosas ocorridas pela Internet vitimaram correntistas de diversos bancos. Além disso, a Comissão também tem como finalidade identificar crimes como pornografia infantil, falsificação de senhas, cartões de crédito, além das violações a direitos humanos, como a questão do racismo e a invasão de privacidade (a exemplo da exposição de fotos íntimas).

Diante dos fatos acima narrados, fica evidente que existem adversidades a serem superadas. As soluções ainda não são definitivas, estão nascendo, surgindo, mas existe uma perspectiva de melhora nos mecanismos de controle, notadamente com a criação, ainda que incipiente, de leis específicas sobre o assunto. Aliado a isso, verifica-se a preocupação com o treinamento de policiais, o estudo de novas técnicas de investigação por parte do Ministério Público, o compartilhamento de dados entre instituições de acesso à Internet e a cooperação policial e jurídica internacional.

Sendo assim, à luz do exposto, conclui-se que despontam, no cenário interno, diretrizes e organismos específicos em cibersegurança, planejamentos exclusivos voltados ao enfrentamento dos Cibercrimes, união entre os órgãos especializados na prevenção, investigação e punição dos crimes virtuais. No entanto, todas estas iniciativas necessitam buscar o aperfeiçoamento da segurança na rede, sem jamais olvidar das garantias dos direitos fundamentais e do equilíbrio ético-jurídico na era digital.

7 CONSIDERAÇÕES FINAIS

Nesta dissertação, buscou-se estabelecer uma relação entre os conceitos essenciais a este trabalho - Cibercultura, ciberespaço, Ciberdemocracia e cibrecrime, nomenclaturas que, até há pouco tempo, eram desconhecidas do grande público, mas que, por certo, dentro em breve, sairão do rol dos neologismos e farão parte de um novo contexto de vida humana evidenciada pela sociedade em rede.

Na pesquisa desenvolvida, observou-se que, em razão da era digital e da mundialização política e econômica, a democracia ganhou novos contornos, força e poder, encontrando, no ciberespaço, um território privilegiado onde é possível exercitar uma verdadeira Ciberdemocracia. Por meio do entrelaçamento da grande rede, da comunicação célere e sem fronteiras, houve o alargamento do espaço público, transformando-se em espaço público virtual.

A sociedade em rede conseguiu unir, numa mesma interface, mecanismos de troca interpessoal e instrumentos de comunicação de massa. É a fusão da conversação e informação, a ampliação do espaço público, caracterizada por uma dupla revolução: de um lado, o direito de apresentar, de defender um discurso em público, que se estende a qualquer pessoa; do outro, uma parcela de conversações de cunho privado que vai-se incorporando ao espaço público. O ciberespaço transformou-se num espaço aberto aos indivíduos. Houve entrelaçamento do mundo da informação com o mundo político, resultando em discussões, emissão de opiniões, convocações. A democracia, nascida neste ciberespaço, em meio a efervescência de uma Cibercultura, cresceu e se desenvolveu alimentada pelo ciberativismo, ganhou o mundo e também, chegou a solo brasileiro com os movimentos e protestos arquitetados pelas redes sociais, levando milhares de pessoas às ruas.

No estudo, muitas características presentes na chamada Ciberdemocracia relembram a democracia procedimental de Habermas, uma vez que também foi criada no seio de uma esfera pública, fruto do encontro dialógico e oriundo de uma política deliberativa orientada pela linguagem, tornando-se um genuíno meio de integração. Nasce, então, uma proposta de modelo democrático por meio da ação comunicativa que engloba a formação da vontade com a opinião dos indivíduos em espaços institucionais, bem como a construção das opiniões (maneira informal) em espaços não institucionalizados, como o é, o ciberespaço. O internauta, o cidadão do mundo digital, não é aquele limitado ao ato de votar e ser votado, é um cibercidadão que participa diretamente de uma esfera virtual, formada por bancos de dados,

uma sociedade interligada, de modo transnacional que se constrói diariamente, uma descrição de democracia habermasiana no século XXI.

Sobejamente tratada nesta dissertação, a Ciberdemocracia, de um modo ou de outro, quer por uma falha na sua engenharia de concepção, quer pela faculdade que têm alguns de transgredirem os princípios da boa convivência, em que pese ser um instrumento de valiosa contribuição para se veicularem e potencializarem todas as manifestações socioculturais, termina por propiciar, à revelia do seu objetivo, desvios que vão de encontro à integridade humana, abrindo possibilidade para o cometimento do Cibercrime.

No decorrer das análises aqui realizadas, à luz de conceitos e estudos feitos por filósofos, técnicos e demais estudiosos do território virtual da Internet, percebemos que o dilema - uso versus abuso desta ferramenta libertária e inclusiva que é a Ciberdemocracia – é mais complexo que se possa imaginar. Concomitantemente ao largo espectro de possibilidades para o exercício político democrático, não é de todo impróprio que se imagine o ciberespaço como sendo um campo que, por subjazer no território da virtualidade, possa facultar desde a solidão do isolamento, o que é um paradoxo, até o aproveitamento desse anonimato para, como disse, o cometimento de atitudes criminosas.

Sendo assim, a rede, por planificar as interações pessoais, culturais e até afetivas, expõe de tal modo a teia de relações, que possibilita não só o cometimento, como uma compreensão mais sistematizada dos desvios comportamentais nela (rede) praticados.

Ainda sobre essa poderosa ferramenta de navegação, é inegável que o ciberespaço propiciou um certo empoderamento aos atores que nele se inter-relacionam, de qualquer estrato social a que pertençam. Sendo assim, também como consequência da Ciberdemocracia cultivada no ciberespaço, modula-se a Cibercultura, esta muito mais abrangente e complexa que parece.

Um fenômeno interessante que se observou no estudo, acerca do ciberespaço, é a impossibilidade da construção de soberania quer seja de que modalidade for. Daí que, levando-se para o terreno da Cibercultura, nota-se que tudo é muito coletivo, tudo parece ainda por criar, tem perfil de algo inacabado, que não dá lugar à acomodação do produto final. Em sendo assim, a Cibercultura deslegitima qualquer intento de construção de soberania pessoal. É o empoderamento do conhecer e não mais da moeda ou dos latifúndios. E, em sendo assim, nenhum ditador resiste a uma comunicação global, desterritorializada, livre, sem contornos de limite geográfico, característica também, encontrada nos princípios ciberdemocráticos.

É oportuno acrescentar, nesta conclusão, uma analogia da Cibercultura com a Teoria da Complexidade, de Edgar Morin. Por complexidade não se toma, nesta acepção, algo complicado, de construção intrincada. Diretamente do Grego, lê-se *plexus* como algo que é tecido, portanto com+plexo passa a significar o que é tecido com, ou seja, tecido em conjunto. A Cibercultura tem um desenho arquitetônico de participação, cooperação, algo que resulta de um conjunto sinérgico de laborações, sem contornos de polo de emissão, sem chancela de propriedade. É exatamente isso que Morin trata na referida teoria.

Foi investigado que muitos dos atuais fenômenos criminosos migraram do mundo real para a grande rede. Ao analisar algumas importantes tipologias dos crimes em estudo, verificou-se que o Cibercrime é atualmente uma ameaça concreta, com indícios crescentes, como foi exaustivamente demonstrado. Os referidos tipos criminais desdobram-se em múltiplas facetas, afetando o equilíbrio da ordem econômica mundial, pois tem provocado prejuízos que somam bilhões de dólares, em vários países e com reflexos incisivos no Brasil. Estas práticas delituosas causam danos financeiros ao Estado, instituições privadas e pessoas, uma vez que implicam em reforçar a segurança dos sistemas informáticos.

Visando a uma melhor desenvoltura por parte dos responsáveis pela persecução criminal, imprescindivelmente, consoante foi pesquisado, deverá haver um investimento governamental considerável no preparo e capacitação desses profissionais de modo contínuo, para que haja uma atualização perene, pois uma das características marcantes deste tipo de delito é a mutabilidade. São infrações que se transmutam diariamente, chegando às quatro partes do globo, em sequência, numa celeridade atroz.

Desse modo, peritos, policiais, promotores e magistrados necessitam pesquisar, estudar e, se atualizar, constantemente. Em que pese todo esforço e ações contínuas, tais operações e diligências somente alcançarão êxito, se forem fruto da imprescindível união e do desempenho de todos aqueles que combatem estes crimes, sejam eles policiais federais, civis, advogados, membros do Ministério Público e integrantes do judiciário. Impreterivelmente, tem que haver uma soma de esforços, uma ação conjunta com um aparato estratégico que facilite a comunicação e a interação entre a polícia, promotores e juízes, incluindo também as organizações responsáveis pelos dados cadastrais, acesso e conexões. A criação de uma linha direta ou um canal eletrônico seguro, criptografado para a troca e o compartilhamento de informações, táticas e ideias, seria um avanço na gestão estratégica da persecução penal dos ilícitos cibernéticos, mas, para tanto, o governo tem que priorizar e investir nesta área.

Assim como é primordial uma força tarefa em nível nacional, tão imprescindível quanto, é o esforço conjunto mundial para enfrentar práticas que ofendem a integridade,

confidencialidade e segurança de dados dos sistemas computacionais. E, agregando a tudo isso, há os crimes já mencionados que lesam financeiramente a sociedade, bem como outros que põem em risco a personalidade, a integridade física e psíquica de pessoas ou grupos, tais como xenofobia, racismo, pedofilia, ciberterrorismo, entre outros.

É necessário agregar a legislação que se tem e não dissociá-la, seja a Lei Penal, o CC, ECA, o CDC, a Constituição e o próprio Marco Civil, em que pese às críticas, como, por exemplo, não ter abordado os direitos autorais. No entanto, a sua aprovação já é um primeiro passo, um avanço em relação a outros países, mas o sistema jurídico brasileiro ainda carece de novos dispositivos legais para combater a referida cibercriminalidade.

No plano jurídico externo, seria muito importante para o Brasil, tornar-se signatário da Convenção de Budapeste para alcançar a punibilidade num crime que vai além das fronteiras nacionais, essencialmente, em muitos casos, o Cibercrime é transnacional. A conjunção de forças em outros países, assim como a permissão para a realização da persecução penal "extramuros", são essenciais, sendo exemplos de gestão jurídico-estratégica de extrema relevância no enfrentamento do problema. Espera-se, ainda, a ampliação do aparato legal juntamente com uma estrutura adequada para melhor se combater a cibercriminalidade.

O Brasil, mesmo carecendo de instrumentos jurídicos adequados, vem conseguindo enfrentar grandes ameaças, desarticulando organizações criminosas de lesividade e alcance nacional e internacional, por meio de operações envolvendo, especialmente, a polícia federal e o Ministério Público. Contudo, tais ações são ainda insuficientes para diminuir a alta incidência dos crimes cibernéticos.

Diante dos dados pesquisados, o combate aos crimes cibernéticos não pode ser feito apenas pela justiça criminal, tão necessário quanto é a participação consciente e responsável de cada internauta. Para tanto, a organização de fóruns, palestras e debates que versem sobre os perigos, os novos meios e espécies de ameaças cibernéticas, faz-se urgente, pois é premente a necessidade de aprofundamento sobre o tema envolvendo a sociedade como um todo, especialmente por meio da nova ágora virtual, como exercício de cidadania. Assim, poderá haver um aprimoramento na legislação, de forma participativa para a busca de um consenso, uma melhor adequação legal aos delitos mutantes, resguardando sempre a liberdade de expressão e outros direitos constitucionais.

E, conforme foi visto, nenhum direito é absoluto. A própria Constituição reza que é livre o direito à expressão, mas é vedado o anonimato. Há sempre excepcionalidades em prol de valores maiores como a dignidade humana, a segurança pública, a integridade física e psíquica das pessoas. Estelionato, racismo, xenofobia, pedo-pornografia, terrorismo,

incitações ao suicídio, *trollismo*, *ciberbullying*, apologia ao ódio e tantas outras atrocidades cometidas no ciberespaço não podem ser praticadas sem punibilidade. Muitos delitos cometidos são exacerbadamente graves e, consequentemente, necessitam de medidas proporcionais à extensão lesiva e danosa. Ninguém pode praticar crimes e se resguardar no direito sagrado de se expressar. Exercer direitos implica responsabilidades e respeito ao próximo.

Outrossim, deve-se também salientar que, quanto mais desfechos positivos forem alcançados no desenrolar das investigações, maior será o grau de punibilidade, gerando uma sensação de controle e segurança. Ocorrendo o contrário, quanto maior o número de ciberataques, sem a identificação dos autores, maior a impunibilidade e a consequente proliferação dos Cibercrimes. O êxito das investigações e a punição dos infratores são as melhores formas de coibição desses delitos. E assim, justamente por possuírem características singulares, os referidos delitos necessitam de dispositivos legais que desburocratizem mais o processo, a obtenção das provas, a aquisição e preservação dos dados, uma vez que, a celeridade na investigação de tais crimes é fundamental para que se possa descobrir a autoria.

Uma estratégia bem sucedida no combate aos ciberdelitos passa por diagnósticos precisos sobre o número de incidência. Na atualidade, não há um mecanismo seguro que aponte fidedignamente a quantidade de ciberataques, pois, em muito dos casos, não são registrados os incidentes. As vítimas não o fazem por, ignorância (desconhecimento de como proceder); em outras situações, por vergonha, constrangimento (casos de fotografias íntimas, por exemplo); outras, por desacreditarem que a polícia identificará o autor e, no caso de empresas, especialmente de grandes organizações, estas acabam por guardar sigilo com receio de macular seu nome e perder clientes. É premente que se faça uma campanha instrutiva junto à população para tentar mudar este quadro.

As políticas públicas, na seara digital, deverão alcançar os milhares de pessoas que ainda não têm acesso à Internet, mas a inclusão digital, apenas, não previne crimes virtuais, outra medida de extrema necessidade e urgência é a educação e prevenção digitais. O esclarecimento dos perigos e dos ataques perniciosos que advêm da vasta rede mundial de computadores é uma estratégia fundamental. Gerir conhecimento, informação, na busca da prevenção e defesa cibernéticas são táticas de cibersegurança que devem ser dirigidas a toda nação (indivíduos e instituições públicas e privadas). Uma sugestão pertinente seria a educação como forma de conscientização, ou seja, o Governo Federal deveria estabelecer, nas instituições de ensino médio e superior, a criação obrigatória do componente curricular: Segurança Digital.

Destarte, foi possível constatar no estudo e enfrentamento do Cibercrime, que conceitos tradicionais como, soberania, tempo e local do crime e, por consequência, jurisdição e competência têm que ser revistos, sob um novo prisma, o da necessidade de integração ao mundo globalizado. Além do que, também, em razão das peculiaridades que cercam este ciberdelito, é imprescindível e urgente um regime de cooperação penal internacional no tratamento das novas questões relacionadas à Internet e ao ciberespaço.

Notou-se, no transcurso da pesquisa, que as tecnologias e os princípios da sociedade de informação, a democracia da Internet e os crimes cibernéticos são assuntos efervescentes e complexos, tanto para a administração estatal, quanto para a seara jurídica, pois ainda estão sendo redesenhados e estudados. No entanto, mesmo com tais tratamentos, devem ser objeto de um compêndio de diretrizes que apontem para possíveis soluções.

No quesito cibersegurança, foi visto que, em razão de o Brasil ter sediado eventos de relevância mundial, como (Rio+20) e a Copa do Mundo, um planejamento operacional militar foi realizado, levando em consideração as ameaças advindas do espaço cibernético. No entanto, foi após as denúncias de espionagem norte-americana, feitas por Edward Snowder, que a segurança virtual e defesa cibernética brasileira foram sendo discutidas com bastante ênfase, tanto na esfera civil quanto na esfera militar. Após tais revelações, a Administração Federal Brasileira promoveu algumas ações concretas (em 2015) a respeito do tema, criando o Comando de Defesa Cibernética (ComDCiber) e a Escola Nacional de Defesa Cibernética (ENaDCiber), além de lançar o Mapa Estratégico da Segurança da Informação e da Segurança Cibernética 2015-2018, documento que procurou simbolizar a visão crítica de gestão para o setor de segurança e defesa no país, tratando do tema com bastante desvelo e rigor.

Verifica-se que o sistema de inteligência brasileiro, apesar de muitos avanços na área, ainda precisa adequar-se, de fato, ao novo mundo globalizado e ultra tecnológico, aplicando-se e investindo-se em pesquisas, ampliando-se o conhecimento e trabalhando de modo estratégico no cerne da cibersegurança. É necessário um plano multilateral que possa preparar a nação contra as ameaças, ataques e invasões virtuais. A implementação concreta de diretrizes estratégicas que defendam os ativos de organizações, pessoas e a própria administração pública brasileira é imprescindível, uma questão de urgência estatal.

Como, então, conciliar o respeito à liberdade - que é pressuposto da Ciberdemocracia - com um modo de se coibir a prática de crimes usando-se este espaço de liberdade? Como passar pelo tênue corredor que separa uma convivência democrática, participativa, construtiva, do oportunismo criminoso de invasão do coletivo sadio através de cometimento

de desvios? Se o remédio é a coibição dos desmandos, das transgressões, também há que se cuidar para que ele não comprometa a vida do medicado.

Entendemos que a solução para esse dilema esteja, inicialmente na gestão de uma educação voltada para a nova realidade que nos cerca. Não apenas a educação em nível universitário; não somente aquela oriunda dos mais altos degraus da formação acadêmica. Ter-se-á que investir na Educação Fundamental. Ali é que se forjam os cidadãos. Ali é que se molda o caráter do ser humano do futuro. Portanto, nada melhor que esse espaço educacional para, semelhantemente ao que se faz nas escolas com a educação para o trânsito, instituir-se, como matéria obrigatória no Ensino Fundamental, o uso responsável do ciberespaço.

Neste raciocínio, depreende-se então que, antes de qualquer ação específica no tocante à cibersegurança, é imprescindível que se invista num processo pedagógico digital. Relembrando as lições de Asmann, não queremos extremismos, nem tecnofobia, nem tecnolatria, muito menos utilizar um instrumento democrático de alcance universal, que é a Internet, para fazer mal à humanidade. Medidas eficazes de segurança dependem antes de mais nada, de informação, educação e conscientização. Somente agindo dessa forma, a segurança informacional e cibernética poderão ser defendidas e protegidas com mais estratégia e eficácia, ou seja, de modo complexo e conglobante.

Concluindo, depois de se ter feito uma explanação sobre tecnologia de informação e comunicação, seu espectro de importâncias para a humanidade como um todo, ademais se discutindo sobre o tênue limiar entre os territórios da Ciberdemocracia e do Cibercrime, cabem algumas afirmações complementares: pode-se assegurar que a Ciberdemocracia é uma ferramenta de todo esse aparato de conquistas até então alcançadas a duras penas e ao despender de muita dedicação e estudo. Todavia, há que se lutar, com todas as armas, para que, em nome de se preservarem direitos de usuários das redes sociais e outros recursos, não se estabeleçam mecanismos que venham a se configurar censura ou algo que se assemelhe a este retrocesso.

Diante disso, há que se discutirem, com vagar e criteriosamente, todas as questões que envolvem esse "dilema", qual seja: Ciberdemocracia não deve, nem pode, ser um instrumento que faculte a impunidade mascarada pelo lado obscuro do anonimato ou do evocado direito de expressão. Deve, sim, ser um objeto de empoderamento social, ou seja, canal livre onde se busquem e se produzam saberes e conhecimentos. O conflito entre o estado de *laissez faire* permissivo e uma censura disfarçada em nome de uma legislação regulatória tem de ser tratado de forma responsável e cuidadosa, de modo a que se inibam os crimes e desmandos, fortalecendo esse veículo de grande carga sócioagregadora que é a Ciberdemocracia.

REFERÊNCIAS

ALMEIDA, G.A.; CHRISTMANN, M.O. **Ética e direito**: uma perspectiva integrada. São Paulo: Atlas, 2002.

ALVES, G.A outra face da Deep Web. **Revista Ler &Saber**, São Paulo, v. 3, n. 5, 2015.

AMADEU, S. **O que é Cibercultura**. Disponível em: <https://www.youtube.com/watch?v=eqJG9xmb0KE>. Acesso em: 24 ago. 2015.

AMARAL, B. **Seis em cada dez pessoas ainda estão offline no mundo**. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/seis-em-cada-dez-pessoas-ainda-estao-offline-no-mundo>. Acesso em: 25 out. 2015.

ANDRADE, M.M. de. **Introdução à metodologia do trabalho científico**. 6. ed. São Paulo: Atlas, 2002.

ARAS, V. **A questão penal no marco civil.** [2010]. Disponível em: <https://blogdovladimir.files.wordpress.com/2010/01/artigo-marco-civil-da-Internet.pdf>. Acesso em: 06 mar. 2015.

ARAÚJO FILHO, J.M. **Ciberterrorismo e cibercrime:** O Brasil está preparado? 2010. Disponível em: <http://mariano.delegadodepolicia.com/ciberterrorismo-e-Cibercrime-o-brasil-esta-preparado-parte-1/>. Acesso em: 16 abr. 2015.

ARNOUD, A.N.D. **Cyberbullying e responsabilidade civil do provedor de Internet na Lei do Marco Civil.** [2014]. Disponível em: <http://jus.com.br/artigos/32619/cyberbullying-e-responsabilidade-civil-do-provedor-de-Internet-na-lei-do-marco-civil>**.** Acesso em: 04 mar. 2015.

BARBAI, M.A. A criminalidade no espaço digital: a formulação do sentido. In. DIAS, Cristiane. **Formas de mobilidade no espaço e-urbano**: sentido e materialidade digital [*online*]. (Série e-urbano, v.2), 2013. Disponível em: <http://www.labeurb.unicamp.br/livroEurbano/ Laboratório de Estudos Urbanos - LABEURB/ Núcleo de Desenvolvimento da Criatividade.

BARROS, R.F. **Guerra cibernética**: Os novos desafios do Direito Internacional. Belo Horizonte: Editora D`Plácido, 2015.

BASTOS, C.D.V. **Análise da conduta de Edward Snowden**. 2014. Disponível em: <http://webcache.googleusercontent.com/search?q=cache:ugj2WpuAUgcJ:https://repositorio.ufsc.br/>. Acesso em: 06 ago. 2015.

BECCARIA, C. **Dos delitos e das penas**. São Paulo: Martin Claret, 2006.

BERTOZZI, R.; SELEM, L. **Os cinco "Es" da gestão estratégica jurídicaa** - Parte I. Disponível em: <http://www.estrategianaadvocacia.com.br/artigos2.asp?id=420#.VfvpF99VhHw> acesso em 17 set. 2015.

BERTOZZI, R. **O mundo da gestão estratégica chegou aos escritórios jurídicos**. Disponível em**:** <http://www.ambito-juridico.com.br/site/index.php?n_*link*=revista_artigos_leitura&artigo_id=3608>. Acesso em: 16 set. 2015.

BLUM, R.O. **Coluna do Augusto Nunes**. Disponível em: <http://veja.abril.com.br/blog/augusto-nunes/videos-veja-entrevista/renato-opice-blum-advogado-especializado-em-direito-digital-o-conceito-de-privacidade-esta-mudando-talvez-esteja-acabando/>. Entrevista concedida a Veja, em 04/11/2011.

BOBBIO, N. **O Futuro da democracia:** uma defesa das regras do jogo. 5. ed. São Paulo: Paz e Terra, 1986.

BOBBIO. N.; MATTEUCCI, N.; PASQUINO, G. (Org.). **Dicionário de política.** 11. ed. Brasília: UNB, 1998.

BOFF, Leonardo. **Ética e moral**. Disponível em: <http://www.leonardoboff.com/site/vista/2003/jul04.htm>. Acesso em: 02 mar. 2015.

_____. **As multidões nas ruas**: como interpretar? Disponível em:<https://leonardoboff.wordpress.com/2013/06/28/as-multidoes-nas-ruas-como-interpretar/>. Acesso em: 18 jun. 2015.

BOTELHO, T. **Impeachment já.** Disponível em: <http://thiaguinhobotelho.blogspot.com.br/2015/07/impeachment-ja.html>. Acesso em: 14 out 2015.

BRASIL. [Constituição 1988]. **Constituição da República Federativa do Brasil**. 35. ed. Brasília: Câmara dos Deputados, Edições Câmara, 2012. Disponível em: <file:///C:/Users/Nots/Downloads/constituicao_federal_35ed.pdf>. Acesso em: 22 ago. 2015

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão. **Roteiro de atuação:** crimes cibernéticos. 2 ed. Brasília: MPF/CCR, 2013.

BRASIL. Presidência da República, Casa Civil. **Lei nº 12.965, de 23.04.2014**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 05 mar. 2015.

BRENNAND, E.G.G.**;** BERTEN, A.; MEDEIROS, W. . Democracia e construção do espaço público: dialogando com Jürgen Habermas. In: BRENNAND, E.G.G. et. al. (Org.). **Diálogos com Jürgen Habermas**. João Pessoa: Editora Universitária/UFPB, 2006.

BARRUCHO, L.B. **IBGE**: Metade dos brasileiros estão conectados à internet; Norte lidera em acesso por celular. 2015. Disponível em: <http://www.bbc.com/portuguese/noticias/2015/04/150429_divulgacao_pnad_ibge_lgb>. Acesso em: 02 out. 2015

CALAMANDREI, P. **Direito Processual Civil**. Campinas: Bookseller, 1999.

CANALTECH. **Brasil e Europa terão cabo de comunicação para fugir da espionagem dos EUA**. [2015]. Disponível em: <http://canaltech.com.br/noticia/espionagem/Brasil-e-Europa-terao-cabo-de-comunicacao-para-fugir-da-espionagem-dos-EUA/>. Acesso em: 15 ago. 2015.

CANOTILHO, J.J.G. **Direito constitucional e teoria da constituição**. 7. ed. Coimbra: Almedina, 2003.

CAPELLA, A.C.N. **Formação da agenda governamental**: perspectivas teóricas. 2005. Disponível em: <http://www.anpocs.org/portal/index.php?option=com_docman&task=doc_view&gid=3789&Itemid=318>. Acesso em: 05 ago. 2015.

CARAVANTES, G.R. **Teoria geral da administração.** Porto Alegre: Editora AGE, 1999.

CARVALHO, L.G. **Segurança nas redes**. Rio de Janeiro: Ciência Moderna, 2005.

CASADO, A.G.P. **Cyber bullying**: violência virtual e o enquadramento penal no Brasil. Disponível em: <http://www.viajus.com.br/viajus.php?pagina=artigos&id=4231&idAreaSel=20&seeArt=yes>. Acesso em: 4 mar. 2015.

CASEY, E. **Digital evidence and computer crime**. 2. ed. [S.l.]: Academic Press, 2004.

CASSANTI, M.O. **Crimes virtuais, vítimas reais**. Rio de Janeiro: Brasport, 2014.

CASTELLS, M. **A Galáxia da Internet**: reflexões sobre a Internet, os negócios e a sociedade. Rio de Janeiro, ZAHAR, 2003.

_____. **Manuel Castells analisa as manifestações civis brasileiras**. [2007]. Disponível em: <http://www.fronteiras.com/artigos/manuel-castells-analisa-as-manifestacoes-civis-brasileiras>. Acesso em: 20 jul. 2015.

_____. **Redes de indignação e esperança.** Disponível em: <http://www.fronteiras.com/artigos/manuel-castells-analisa-as-manifestacoes-civis-brasileiras>**.** Acesso em: 15 jul. 2015. Entrevista concedida a Portal Fronteiras.

CAVALCANTE, W.F. Crimes cibernéticos: investigação e ameaças na internet. **Revista Jus Navigandi**, Teresina, ano 18, n. 3782, 8 nov. 2013. Disponível em: <https://jus.com.br/artigos/25743>. Acesso em: 15 fev. 2015.

CERT.br. **Cartilha de segurança para Internet.** Disponível em:<http://cartilha.cert.br/>. Acesso em: 20 set. 2015.

CHATFIELD, T. **50 coisas que hay que saber sobre mundo digital**. Buenos Aires: Ariel, 2012.

CHILDHOOD**. Denúncias anônimas de crimes na Internet passam de 180 mil em 2014.** Disponível em: <http://www.childhood.org.br/denuncias-anonimas-de-crimes-na-internet-passam-de-180-mil-em-2014>. Acesso em: 08 out. 2015.

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

CONCEIÇÃO, L.F.S. **Desafios na definição do ciberespaço brasileiro**. 2015. Monografia (Bacharelado em Defesa e Gestão Estratégica Internacional) – Universidade Federal do Rio de Janeiro. Disponível em: <http://dgei.ufrj.br/images/Monografias/tcc-luiz-felipe-conceicao.pdf>. Acesso em: 22 ago. 2015.

CONCEITO de rede social. Disponível em: <http://conceito.de/rede-social>. Acesso em: 12 out. 2015.

CONTE, C.P.; SANTOS, C.A. **Desafios do Direito Penal no mundo globalizado:** A aplicação da Lei Penal no espaço**.** Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/desafios_do_direito_penal_rdit.pdf>. Acesso em: 15 out. 2015.

CORRÊA, F. **A defesa em debate- Espionagem, política internacional e guerra:** o Mundo e o Brasil. 2000. Disponível em: <http://www.defesanet.com.br/defesa/noticia/12114/A-Defesa-em-Debate---Espionagem--politica-internacional-e-guerra---o-Mundo-e-o-Brasil-/>.Acesso em: 10 set. 2015.

CORRUPTECA. **Publicações científicas**. Disponível em: <http://corrupteca.nupps.usp.br/publicacoes/?q=modelo+de+m%C3%BAltiplos+fluxos>. Acesso em: 06 set. 2015.

COSTA, J.F. **Noções fundamentais de direito penal**. Coimbra Editora. 2007.

COVEY, S.R. **Os 7 hábitos das pessoas muito eficazes.** 22. ed. São Paulo: Editora Best Seller, 1999.

CREMADES, J. **Micro Poder:** A força do cidadão na era digital. Tradução de Edgard Charles. São Paulo: SENAC, 2009.

CRESPO, M.X.F. **Crimes digitais**. São Paulo: Saraiva, 2011.

DAOUN, A.; BLUM, R.O. In: CYBERCRIMES. **Artigo em Direito & internet**: aspectos jurídicos relevantes. Bauru: Edipro, 2000.

DIAS FILHO, C.R. Cadeia de custódia: do local de crime ao trânsito em julgado; do vestígio à evidência. **Revista dos Tribunais**, v. 833, 2009.

DINIZ, L. **O caso Snowden e a espionagem que chegou ao Brasil**. 2013. Disponível em: <http://observatoriodaimprensa.com.br/caderno-da-cidadania/o_caso_snowden_e_a_espionagem_que_chegou_ao_brasil/>. Acesso em: 21 ago. 2015.

DULLIUS, A.A.; HIPLLER, A.; FRANCO, E.L. **Dos crimes praticados em ambientes virtuais**. [2012]. Disponível em: <http://www.conteudojuridico.com.br/artigo,dos-crimes-praticados-em-ambientes-virtuais,38483.html>. Acesso em: 13 fev. 2015.

ELAZARI, K. Como sobreviver à guerra cibernética**. Scientific american**, Portugal, v. 13, n. 156, p. 56-59, maio 2015.

FAVORITO, F. **Com Marco Civil, juízes podem tirar conteúdo mais rapidamente**. Disponível em: <http://fernandafav.jusbrasil.com.br/noticias/114588701/com-marco-civil-juizes-podem-tirar-conteudo-mais-rapidamente?ref=topic_feed>. Acesso em: 14 out. 2015.

FERNANDES, M. **Pigmaleão**. Porto Alegre: L&PM, 2005.

FERREIRA, E.L.L. **Jurisdição Metaterritorial para a Cibernética**. São Paulo: Lex, 2006.

FERREIRA, J.N. **Acessando a rede:** um olhar sobre a formação da agenda para a regulação da Internet no Brasil. 2014. Dissertação (Mestrado em Administração Pública e Governo) - Escola de Administração de Empresas de São Paulo, Fundação Getúlio Vargas, São Paulo, 2014. Disponível em: <http://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/11572/disserta%C3%A7%C3%A3o_final.pdf?sequence=9&isAllowed=y>. Acesso em: 13 fev. 2015.

FOLEY, J.P. **Ética na Internet.** 2002. Disponível em: <http://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_ethics-Internet_po.html>. Acesso em: 10 mar. 2015.

GALVÃO, W.N. **Assange, Snowden e Ellsberg, por Walnice Nogueira Galvão.** Disponível em:<http://jornalggn.com.br/noticia/assange-snowden-e-ellsberg-por-walnice-nogueira-galvao>. Acesso em: 21 ago. 2015.

G1. **Entenda o caso de Bradley Manning, condenado por vazar segredos**. Disponível em: <http://g1.globo.com/mundo/noticia/2013/08/entenda-o-caso-de-bradley-manning-condenado-por-vazar-segredos.html>. Acesso em: 21 ago. 2015.

G1. **Entenda o caso de Edward Snowden, que revelou espionagem nos EUA**. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 05 ago. 2015.

G1. **Internautas brasileiros chegam a 105 milhões, segundo pesquisa do Ibope**. 2013. Disponível em: <http://g1.globo.com/tecnologia/noticia/2013/10/internautas-brasileiros-chegam-105-milhoes-segundo-pesquisa-do-ibope.html>. Acesso em: 21 ago. 2015.

G1. **Facebook completa 10 anos; veja a evolução da rede social.** Disponível em: <http://g1.globo.com/tecnologia/noticia/2014/02/facebook-completa-10-anos-veja-evolucao-da-rede-social.html>. Acessado em: 14/10/2015.

G1. **Leia a íntegra da carta do atirador que invadiu escola no RJ.** Disponível em: <http://g1.globo.com/leiaaintegradacartadoatiradorqueinvadiuescolano-RJ>. Acesso em: 08 out. 2015.

G1. **Pergaminho hebraico de 1.500 anos é decifrado graças à tecnologia**. Disponível em:<http://g1.globo.com/mundo/noticia/2015/07/pergaminho-hebraico-de-1500-anos-e-decifrado-gracas-tecnologia.html>. Acesso em: 19 jul. 2015

G1. **Programa de espionagem vazado por Snowden está ligado a muitos países**. Disponível em: <http://g1.globo.com/mundo/noticia/2015/01/programa-de-espionagem-vazado-por-snowden-esta-ligado-muitos-paises.html>. Acesso em: 15 ago. 2015.

G1. **Snowden recebe asilo temporário da Rússia e deixa aeroporto, diz advogado**. Disponível em: <http://ultimosegundo.ig.com.br/mundo/2013-08-01/snowden-recebe-asilo-temporario-da-russia-e-deixa-aeroporto-diz-advogado.html>. Acesso em: 19 ago. 2015.

G1. **Twitter de comando militar dos EUA é hackeado**. 2015. Disponível em: <http://g1.globo.com/mundo/noticia/2015/01/twitter-militar-dos-eua-publica-mensagens-de-cibercalifado.html>. Acesso em: 05 out. 2015.

GIBSON, W. **Neuromancer**. São Paulo: Aleph, 2003.

GIL, A.C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2010.

GLENN, G; MACASKILL, E; POITRAS, L. **Edward Snowden: the whistleblower behind the NSA surveillance.** Disponível em: <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Acesso em: 21 ago. 2015.

GLENNY, M. **Mercado sombrio:** O Cibercrime e você. São Paulo: Companhia das letras, 2011. 392 p.

GODOI, C.J. O valor da cultura nas organizações contemporâneas. in: **Revista Espaço Ética:** Educação, Gestão e Consumo, v. 1, n. 01, p. 100-116, jan./abril 2014.

GOODMAN, A. **O castigo de Julian Assange**: condenado sem ter sido acusado. Disponível em: <http://cartamaior.com.br/?/Editoria/Internacional/O-castigo-de-Julian-Assange-Condenado-sem-ter-sido-acusado/6/33638>. Acesso em: 20 ago. 2015.

GOODMAN, M. **Future Crimes**. [S.l.]: Transworld Publishers, 2015.

GOUVEIA, S.M.P. **O direito na era digital**: Crimes praticados por meio da informática. Rio de Janeiro: Mauad Editora, 1997.

GRECO, R. **Curso de Direito Penal**. 16. ed. Rio de Janeiro: Impetus, 2014.

GREENWALD, G; KAZ, R; CASADO, J. **EUA espionaram milhões de *e-mail*s e ligações de brasileiros**. Disponível em: <http://oglobo.globo.com/mundo/eua-espionaram-milhoes-d*e-mail*s-ligacoes-de-brasileiros-8940934>. Acesso em: 22 ago. 2015.

HABERMAS. J. **Direito e democracia.** Entre facticidade e validade. Rio de Janeiro: Tempo Brasileiro. 1997. (v. 1-2).

_____. **Mudança estrutural da esfera pública**. 5. ed. Rio de Janeiro: Biblioteca Tempo Universitário, 1989 .

_____. **Pensamento pós-metafísico.** Estudos Filosóficos. 2. ed. Rio de Janeiro: Tempo Brasileiro, 2002.

HAIKAL, V.A; PINHEIRO, P.P. **A nova lei de crimes digitais.** Disponível em: <http://www.gazetadopovo.com.br/vida-publica/justica-direito/artigos/a-nova-lei-de-crimes-digitais-evf935c0vqjw7rh9b4cq75tfy>. Acesso em: 22 ago. 2015.

HAILER, M. **Ativista digitais se mostram pessimistas quanto ao futuro da Internet e afirmam que, enquanto existirem governos, a espionagem na rede vai continuar.** Disponível em: <http://revistaforum.com.br/digital/138/criptografia-e-distopia-da-sociedade-controle/>. Acesso em: 19 ago. 2015.

HAMANN, R. **Whatsapp atinge a marca de 900 milhões de usuários ativos.** Disponível em: <http://www.tecmundo.com.br/whatsapp/85923-whatsapp-atinge-marca-900-milhoes-usuarios-ativos.htm>. Acesso em: 14 out. 2015.

HARDING, L. **Os arquivos de Snowden**: a história secreta do homem mais procurado do mundo. Rio de Janeiro: LeYa, 2014.

HATA, F.Y.F. Direito Penal Internacional. **Revista SJRJ**, Rio de Janeiro, v. 17, n. 29. p. 117-141, dez. 2010.

HENRIK, R.B. **Mapa exibe lista de países Bitcoin Friendly**. Disponível em: <http://bestbitcoin.com.br/bitlegal-mapa-exibe-lista-de-paises-bitcoin-friendly/>. Acesso em: 20 set. 2015.

HERSEY, P.; BLANCHARD, H.K. **Psicologia para administradores**. São Paulo: EPU, 1986.

HOUAISS, A. **Dicionário da língua portuguesa.** Rio de Janeiro: Objetiva, 2009.
IANNI, O. **Teorias da globalização**. 9. ed. Rio de Janeiro: Civilização Brasileira, 2001.

IUSKNOW, A. Uma aula para ensinar metodología científica. In: Philos. **Revista Brasileira de Filosofia no Ensino Fundamental**, Ano 6, n. 12, 1999.

JESUS, D.; MILAGRE, J.A. **Marco Civil da Internet**: Comentários à Lei n 12. 965/14. São Paulo: Saraiva, 2014.

JORDÃO, F. **O que é IP estático?** E dinâmico? Disponível em: <http://www.tecmundo.com.br/1836-o-que-e-ip-estatico-e-dinamico-.htm>. Acesso em: 20 set. 2015.

JORGE, H.V.N.; WENDT, E. **Crimes cibernéticos:** ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2013.

KATCHBOIAN, P. **Com 1,4 bi de usuários, facebook é a maior "nação" do mundo.** Disponível em: <http://dicascidade.com.br/entretenimento/com-1-4-bilhao-de-usuarios-facebook-agora-e-a-maior-nacao-do-mundo/>. Acesso em: 14 out. 2015.

KOCHE, J.C. **Fundamentos de metodologia científica**: teoria da ciência e prática da pesquisa. 15ª ed. Petrópolis, Rio de Janeiro: Vozes, 1997.

KOGUCHI, T. Bullyng 2.0. **Revista Ler e Saber**, v. 1, n. 1, 2015.

_____.. O lado sombrio da Deep Web. **Revista Ler &Saber**, v. 3, n. 5, 2015.

LAKATOS, M.E; MARCONI, M.A. **Fundamentos de metodologia científica**. 7. ed. São Paulo: Atlas, 2010.

LARA, B. **Ética e informação**. [2014]. Disponível em: <http://observatoriodaimprensa.com.br/news/view/_ed820_etica_e_informacao>. Acesso em: 3 mar. 2015.

LEMOS, A. **Ciberespaço:** As estruturas antropológicas do ciberespaço. 2014. Disponível em: <http://www.institutodofuturo.com.br/CIBER.html>. Acesso em: 05 mai. 2015.

LEMOS, A.; LÉVY, P. **O futuro da Internet**: Em direção a uma ciberdemocracia planetária. São Paulo: Paulus, 2010.

LÉVY, P. **Cibercultura**. São Paulo: Editora 34, 1999.

_____. **Cibercultura**. 3. ed. São Paulo: Editora 34, 2010.

_____. **Ciberdemocracia**. 2. ed. Lisboa: Instituto Piaget, 2002.

_____. "**O que acontece aqui não é por democracia, mas contra a corrupção"**. Disponível em:<http://epoca.globo.com/ideias/noticia/2013/11/pierre-levy-o-que-acontece-aqui-nao-e-por-bdemocraciab-e-sim-contra-bcorrupcaob.html>. Acesso em: 23 jul. 2015. Entrevista concedida a Revista Época.

LIMA, C. **Nanofobia**: Será que você tem e não sabe? Disponível em: <http://elo.com.br/portal/colunistas/ver/228318/nomofobia--sera-que-voce-tem-e-nao-sabe-.html>. Acesso em: 23 jul. 2015.

LIMA, M.R. **O futuro da Internet:** Em direção a uma Ciberdemocracia planetária. 2012. Disponível em: <http://www.sbu.unicamp.br/seer/ojs/index.php/rbci/article/viewFile/518/pdf_24**>.** Acesso em: 06 abr. 2015.

LINDOLFO, P.N. **Crimes Cibernéticos:** necessidade de uma legislação específica no Brasil. 2009. 39 f. Monografia (Bacharelado em Direito) - Faculdade de Ensino Superior da Paraíba, João Pessoa, 2009.

LOPES JUNIOR, A. **Direito Processual Penal e sua conformidade constitucional**. Rio de Janeiro: Lumen Juris, 2010. (v.1).

_____. **Sistema de investigação preliminar no Processo Penal**. Rio de Janeiro: Lumen Juris, 2001.

LOUREIRO, G. Caiu na net: E agora, dá pra tirar? **Revista Galileu**, n. 279, 02 out. 2014.

LUBENOW, J.A. **Esfera pública e democracia deliberativa em Habermas.** Modelo teórico e discursos críticos. Disponível em:

<http://www.scielo.br/scielo.php?pid=S0100512X2010000100012&script=sci_arttext>**.** Acesso em: 03. abr. 2015.

MACHADO, P.H. **Janelas.** Disponível em: <http://variosprismasinfinitoslados.blogfolha.uol.com.br/>. Acesso em: 6 mar. 2015.

MACHADO, R.C**. Marco civil da Internet**: Análise dos pontos relevantes da Lei nº 12.965/2014. Jus Navigandi, Teresina, ano 19, n. 4138, 30out.2014. Disponível em: <http://jus.com.br/artigos/30162>. Acesso em: 5 mar. 2015.

MADRUGA, A. **Não é fácil distinguir jurisdição e competência.** Disponível: <http://www.conjur.com.br/2011-ago-17/cooperacao-internacional-nao-facil-distinguir-jurisdicao-competencia>. Acesso em: 10 set. 2015.

MAGRI, W. **Era das transições:** Jürgen Habermas. Disponível em: <http://wallacemagri.jusbrasil.com.br/artigos/112023802/era-das-transicoes-jurgen-habermas>. Acesso em: 12 fev. 2015.

MANAUS. Câmara Municipal. **Câmara aprova tramitação de projeto que prevê campanha de combate ao cyberbullyng**. 2014. Disponível em: <http://www.cmm.am.gov.br/camara-aprova-tramitacao-de-projeto-que-preve-campanha-de-combate-ao-cyberbullying/>. Acesso em: 02 out. 2015.

MARQUES, F.P.J.A. **Dimensões da Ciberdemocracia**: Conceitos e experiências fundamentais. 2004. 207 f. Dissertação (Mestrado em Comunicação e Cultura Contemporâneas) - Universidade Federal da Bahia, 2004.

MARTINS, A. **Ciberativismo:** ativismo nasce nas redes e mobiliza as ruas do mundo. Disponível em: <http://vestibular.uol.com.br/resumo-das disciplinas/atualidades/ciberativismo-o-ativismo-da-rede-para-as-ruas-o-ativismo-da-rede-para-as-ruas.htm>. Acesso em: 13 abr. 2015.

_____. **Nova lei sobre espionagem nos EUA é "primeiro passo" para reformas profundas.** Disponível em: <http://www.publico.pt/mundo/noticia/nova-lei-sobre-espionagem-nos-eua-e-um-primeiro-passo-para-reformas-profundas-1697825>. Acesso em: 18 Ago 2015.

MATOS, L. M. de. Ciberativismo: O lado bom da rede. **Grandes temas do conhecimento, Psicologia**, São Paulo, n. 15, p. 20-25, 2014.

MELO, J.A. **Cyberbullying**: A violência virtual. 2 ed. Recife: EDUPE, 2011.

MELO NETO, J.C. **Catar Feijão.** Disponível em:<http://antoniocicero.b*log*spot.com.br/2012/03/joao-cabral-de-melo-neto-catar-feijao.html>. Acesso em: 04 ago. 2015.

MIGLIORISI, D.F. **Crímenes em la web**: Los delitos del siglo. Buenos Aires: Del Nuevo Extremo, 2014.

MIRABETE, J.F. **Código Penal Interpretado**. 3. ed. São Paulo: Atlas, 2003.

MONTALVÃO, M. **Inteligência e indústria**: Espionagem e Contraespionagem Corporativa. [S.l.; s.n], 2015.

MONTEIRO, S.D. **O Ciberespaço: o termo, a definição e o conceito.** Disponível em: <http://www.dgz.org.br/jun07/Art_03.htm>**.** Acesso em: 12. abr. 2015.

MORAIS NETO, A.S. **Cibercrime e cooperação penal internacional**: Um enfoque à luz da convenção de Budapeste. 2009. Dissertação (Mestrado em Ciências Jurídicas) – Universidade Federal da Paraíba, João Pessoa. Disponível em: <http://www.ccj.ufpb.br/pos/wp-content/uploads/2013/07/Arnaldo-Sobrinho-Cibercrime-e-Coopera%C3%A7%C3%A3o-Penal-Internacional.pdf>. Acesso em: 07 ago.2015.

NAÍM, M. **Assange, Snowden e você**. Disponível em: <http://brasil.elpais.com/brasil/2015/06/20/internacional/1434832338_805333.html>Acesso em: 20 ago. 2015.

NASSIF, L. **Cibercrimes crescem 197% no Brasil em um ano.** Disponível em: <http://jornalggn.com.br/noticia/Cibercrimes-crescem-197-no-brasil-em-um-ano>. Acesso em: 27 de out. 2015.

NÓBREGA. L.P. A Construção de identidades nas redes sociais. **Fragmentos da Cultura,** Goiânia, v. 20, n. 1/2, p. 95-102, jan./fev., 2010. Disponível em : <http://revistas.ucg.br/index.php/fragmentos/article/viewFile/%201315/899> Acesso em: 06 ago. 2015.

NOGUEIRA, S.A. **Crimes de informática**. São Paulo: BH, 2008.

OLIVEIRA, A.J.O. Como a Internet das coisas vai atropelar o capitalismo. **Revista Galileu,** n. 283, fev. 2015.

OLIVEIRA, R.A. **Marco civil da Internet delineou a responsabilidade civil.** Disponível em: <http://www.conjur.com.br/2014-abr-28/rogerio-oliveira-marco-civil-Internet-delineou-responsabilidade-civil>. Acesso em: 05 mar. 2015.

OLIVEIRA, S.L. **Metodologia científica aplicada ao Direito**. São Paulo: Thomson, 2002.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS - ONU. **Declaração Universal dos Direitos Humanos.** Disponível em: <http://www.dji.com.br/diversos/declaracao_universal_direitos_humanos.htm>. Acesso em: 4 nov. 2015

ORWELL, G. **1984**. São Paulo: Companhia das Letras, 2009.

PAGLIUSI, P. **A Internet profunda:** Segredos, riscos e ameaças. Disponível em: <https://cryptoid.com.br/destaques/a-Internet-profunda-segredos-riscos-e-ameacas/>. Acesso em: 20 set. 2015.

PARTIDO SOCIALISTA DOS TRABALHADORES UNIFICADO - PSTU. **Dia 18 é dia da Marcha Nacional da Liberdade.** 2015. Disponível em: <http://www.pstu.org.br/node/16480>. Acesso em: 10 out 2015.

PAWELS, L.; BERGIER, J. **O despertar dos mágicos**. 23. ed. Rio de Janeiro: Editora Bertrand Brasil, 1989.

PORTAL Brasil. Disponível em: <http://www.brasil.gov.br/>. Acesso em: 10 set. 2015.

PEIXOTO, A.C.F. **Regulação da Internet**: Os desafios do Estado desenvolvimentista para a construção de um ambiente competitivo, inovador e democrático no espaço digital. 2014. 194f. Dissertação (Mestrado em Direito) – Universidade de São Paulo, 2014.

PEREIRA, W. Jornadas de junho: repercussões e leituras. In: SOUSA, C.M.; SOUZA A.A. (Org.). **Livro eletrônico**. Campina Grande: EdUEPB, 2013.

PEREIRA, M.C.G; TEIXEIRA, M.A.C. **A inclusão de catadores em programas de coleta seletiva: da agenda local à nacional.** Disponível em: <http://webcache.googleusercontent.com/search?q=cache:cUwWbBnzju4J:www.scielo.br/pdf/cebape/v9n3/a11v9n3.pdf+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 12.09.2015.

PINHEIRO, P.P. **Direito digital.** 5. ed. São Paulo: Saraiva, 2013.

PINHEIRO, P.P.; HAIKAL, V.A. **A nova lei de crimes digitais**. Disponível em: <http://www.gazetadopovo.com.br/vida-publica/justica-direito/artigos/a-nova-lei-de-crimes-digitais-evf935c0vqjw7rh9b4cq75tfy>. Acesso em: 10 out. 2015.

PINTO, T.S. "Sputnik e a guerra espacial". **Brasil Escola** [*online*]. Disponível em <http://brasilescola.uol.com.br/historia/sputnik.htm>. Acesso em: 19 abr. 2015.

PIOVESAN, F. **Direitos humanos e o Direito Constitucional Internacional**. 15. ed., rev., ampl. e atual. São Paulo: Saraiva, 2015.

POSTER, M. Cidadania, mídia digital e globalização. In MORAES, D. (Org.). **Por uma outra comunicação**. Rio de Janeiro: Record, 2010.

PRESSE, F. **As principais revelações de Edward Snowden**. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/as-principais-revelacoes-de-edward-snowden.html>. Acesso em: 10 ago. 2015.

PROUDON, P.J. **“O que é a propriedade?”.** Lisboa, Portugal: Editora Estampa,1997.

RAMOS, M.G. **Democracia procedimental e ordenamento jurídico**: afirmação do discurso como prática política da igualdade e a experiência histórica da democracia no Ocidente. 2008. Disponível em: <periodicos.ufpb.br/index.php/primafacie/article/viewFile/7244/434>. Acesso em: 25 mar. 2015.

RAUPP, F.M.; BEUREN, M.I. (Org.). **Como elaborar trabalhos monográficos em contabilidade**. Teoria e prática. 2. ed. São Paulo: Atlas, 2003.

REZENDE, P.A.D. **Como entender essas denúncias de vigilantismo global, parte IV**. Disponível em: <http://www.cic.unb.br/~rezende/trabs/entrevistaCJ.html>. Acesso em: 12 out. 2015. Entrevista concedida ao jornalista Pedro Canário.

RIBEIRO, M.A. **Sobre os recentes movimentos sociais urganos no Brasil.** Disponível em:<http://observatoriodaimprensa.com.br/cadernodacidadania/_ed752_sobre_os_recentes_movimentos_sociais_urbanos_no_brasil/>. Acesso em 21.07.2015.

RODEGHERI, L.B; SANTOS, N.F.; OLIVEIRA, R.S. de. A construção da Ciberdemocracia por meio do debate público na blogosfera. **Revista Democracia Digital e Governo Eletrônico**, n.6, p.98-119, 2012.

ROMAGNOLO, C.A. **O que é criptografia? .** Disponível em: <https://www.oficinadanet.com.br/artigo/443/o_que_e_criptografia> Acesso em:18 ago. 2015.

ROSSINI, A.E.S. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SABINO, J. **Web 3.0 e Web semântica:** do que se trata? Disponível em: <www.cin.ufpe.br/~hsp/Microsoft-web.pdf>. Acesso em: 03 mar. 2015.

SANTOS, M.F. **Ciberdefesa. Disponível em:** <http://segurancaecienciasforenses.com/2013/10/28/ciberdefesa/>. Acesso em: 12 ago. 2015.

SANTOS, V. Além da Superfície. **Revista Ler &Saber**, Ano 3, n. 5, 2015.

SARMENTO, G. **Gerações dos direitos humanos e os desafios de sua efetividade**. Disponível em: <http://www.georgesarmento.com.br/wpcontent/uploads/2011/02/GeraçõeS-dos-direitos-humanos-e-os-desafios-de-sua-efetividade1.Acesso>. Acesso em: 15 out. 2015.

SELVATTI, G. C. A. L.**A relação interna entre democracia e direitos fundamentais**: um estudo à luz da teoria discursiva de Jürgen Habermas**.** Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_*link*=revista_artigos_leitura&artigo_id=10621>. Acesso em: 12. abr. 2015.

SEN, A. A ideia de justiça. São Paulo: Companhia das Letras, 2011.

SEVERINO, J.A. **Metodologia do trabalho científico**. 23. ed. São Paulo: Cortez, 2007.

SHELLEY, M. **Frankenstein**. Porto Alegre: L&PM, 1997.

SILVA, L. **Espionagem Industrial**. Disponível em: <http://www.alunos.dcc.fc.up.pt/~c0116005/sei/tp_0/>. Acesso em: 15. abr. 2015.

SILVA, M.A.D. **A deep web:** a Internet que abusa de várias modalidades de crimes. Disponível em: <http://www.jurisway.org.br/v2/dhall.asp?id_dh=15329>. Acesso em: 20 set. 2015.

SILVA, M.A.M. **Acesso à justiça penal e Estado Democrático de Direito**. São Paulo: Juarez Oliveira, 2001.

SILVA, R.P. **E-bola**. Disponível em: <http://www.linuxnewmedia.com.br/images/uploads/pdf_aberto/LM_115_03_03_01_editorial.pdf>. Acesso em: 02 set. 2015.

SILVA, S.M.L. **A ciberespionagem no contexto português.** 2014. Disponível em:<http://comum.rcaap.pt/bitstream/123456789/8750/1/Ciberespionagem%20no%20Contexto%20Portugu%C3%AAs%20Jul%202014%20Susana%20Silva.pdf>. Acesso em: 20 set. 2015.

SILVEIRA, M.D.P. Efeitos da globalização e da sociedade em rede via Internet na formação de identidades contemporâneas. **Psicol. cienc. prof.**, Brasília , v. 24,n. 4, p. 42-51, dez. 2004. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S141498932004000400006&lng=en&nrm=iso>. Acesso em: 03 nov. 2015.

SINGER, I.B. **O Golem**. São Paulo: Perspectiva, 1982.

SNOWDEN, E. **A sociedade aberta avança**. Disponível em: <http://brasil.elpais.com/brasil/2015/06/04/opinion/1433436340_438817.html>. Acesso em: 18 ago. 2015.

SOUZA, A. **A democracia em tempos de globalização.Jus Navigandi.** 2004. Disponível em: <http://jus.com.br/artigos/5686>. Acesso em: 4 jan. 2015.

SOUZA, T. **Democracia onde?** Disponível em: <http://umadosedesimpatia.blogspot.com.br/>. Acesso em: 12 out. 2015.

SOUZA, E. **Dicionário de tecnologia: entenda o significado dos termos.** Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2014/04/dicionario-de-tecnologia-entenda-o-significado-dos-termos.html>. Acessado em: 08 mar. 2015.

SOUZA, F. A democracia, face política da globalização? **Revista brasileira de política internacional** [*online*], v.49, n.1, p. 5-24, 2006.

SOUZA, G.L.M; PEREIRA, D.V**. A convenção de Budapeste e as leis brasileiras.** Disponível em: <http://www.academia.edu/786458/A_CONVEN%C3%87%C3%83O_DE_BUDAPESTE_E_AS_LEIS_BRASILEIRAS>. Acesso em: 25. ago. 2015.

SYDOW, S.T. **Crimes informáticos e suas vítimas**. 2. ed. São Paulo: Saraiva, 2015.

TAVARES, V.R.S; BARBOSA, B.R; SANTOS, F.M. **O uso das redes sociais como meio de mobilização social nos protestos nacionais de junho de 2013.** Disponível em: <http://revistas.ucg.br/index.php/panorama/article/view/3457/2026>. Acesso em: 20 jul.2015.

TEIXEIRA, M.A.C. **O modelo de múltiplos fluxos, de John Kingdon**. Disponível em: <http://www.scielo.br/pdf/cebape/v9n3/a11v9n3.pdf>.Acesso em: 02.ago 2015.

TOLEDO, F.A. **Ilicitude penal e causas de sua exclusão.** Rio de Janeiro: Forense, 1984.

TONHATI, W. **Cracker ataca outra empresa de MS e exige 3 mil dólares para devolver dados**. 2015. Disponível em: <http://www.midiamax.com.br/policia/251980-cracker-ataca-mais-empresa-de-ms-e-exige-us-3-mil-dolares-devolver-dados.html>.

TRAUTMANN, D.A. **Educação, ética e tecnologia**: impressões e reflexões. 2002**.** Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de Santa Catarina, Florianópolis, SC. Disponível em: <http://www.tede.ufsc.br/teses/PGCC0327.pdf. Acesso em 28/08/2010>. Acesso em: 4 mar. 2015.

TUMBLR. **O sofativista**. Disponível em:<http://osofativista.tumblr.com/>. Acesso em: 19 jul. 2015.

VALENTE, M.M.G. **Teoria geral do Direito Policial**. 3. ed. Coimbra: Almedina, 2012.

VÁSQUEZ, A.S. **Ética**. Rio de Janeiro: Civilização Brasileira, 1998.

VECCHIO, D**.** Entrevista concedida a Claufe Rodrigues para a Globonews. Disponível em:<www.globosatplay.globo.com/glonoews/V/4330299/>. Acesso em: 19.jul 2015.

VICENTE, A.B. **A Arte da computação em políticas públicas**: legislação, prevenção e combate aos cibercrimes. 2014. Monografia (Bacharelado em Gestão de Políticas Públicas) – Escola de Artes, Ciências e Humanidades, USP, São Paulo. Disponível em: <http://pt.slideshare.net/AymeVicente/monografia-a-arte-da-computao-em-polticas-pblicas-legislao-preveno-e-combate-aos-Cibercrimes>. Acesso em: 28 ago.2015.

VOIGT, J. A democracia antes e agora, o que mudou?. **Revista de Psicologia,** n. 15, p. 28-37, 2014.

WANDERLEI, F.P. **Crimes cibernéticos**: Obstáculos para punibilidade do infrator. 2012. 52f. Monografia (Bacharelado em Direito) - Faculdade Católica Dom Orione, Araguaína, TO 2012.

WEBSENSE. **The sevens stages of advanced threats.**Disponível em: <http://www.websense.com/assets/white-papers/whitepaper-7-stages-of-advanced-threats-cyber-attack-kill-chain-en.pdf?cm_sp=TMCShowcase-_-PromoCol4-_-Websense+7stages>. Acesso em: 26 out. 2015.

WIENER, N. **Cibernética e sociedade:** o uso humano de seres humanos. São Paulo: Cultrix, 1984.

WIKIEDUCAÇÃO. **Web 2.0.** [2012]. Disponível em: <http://alveslima-edu.wikidot.com/grupo-v-wikifire>. Acesso em: 05 abr. 2015.

WIKIPÉDIA. **Edward Snowden**. Disponível em: <https://pt.wikipedia.org/wiki/Edward_Snowden>. Acesso em: 20.ago. 2015.

WITCKER, I. Occidente ante las nuevas tipologías del terrorismo. **Estudios públicos**, Santiago, Chile, n. 98, out. 2005. Disponível em: <http://www.cepchile.cl/dms/ lang_1/doc_ 3551.html>. Acesso em 10 jan. 2015.

XIMENES, J.M. **Levantamento de dados na pesquisa em Direito:** a técnica da análise de conteúdo. Disponível em: <http://webcache.googleusercontent.com/search?q=cache:Yj0dkmaBpeoJ:www.idp.edu.br/component/docman/doc_*download*/145-+&cd=1&hl=pt-BR&ct=clnk&gl=br>. Acesso em: 10 abr. 2015.

ZAMPRONHA, L. F. **Brasil tem de adotar leis contra espionagem internacional.** Disponível em: <http://www.conjur.com.br/2013-set-08/luis-flavio-zampronha-brasil-adotar-leis-espionagem-internacional1>. Acesso em: 05 set. 2015.

ZANINI, D.; SOUZA, L. **Entevista**. Disponível em: <http://hashtag.ms/blog/nossas-cientistas-sociais-analisam-a-importancia-das-redes-sociais-para-os-movimentos-populares/>. Acesso em: 18 jul.2015.

GLOSSÁRIO

Accounting rate systems – Acerto de contas entre as telefonias para completar ligações de Internet internacionais.

ADSL – Do Inglês *Asymmetric Digital Subscriber Line*. Sistema que permite a utilização das linhas telefônicas para transmissão de dados em velocidade maiores que as permitidas por um *modem* convencional.

Adware – Do inglês *Advertising Software. Software* especificamente projetado para apresentar propagandas. Constitui uma forma de retorno financeiro para aqueles que desenvolvem *software* livre ou prestam serviços gratuitos.

Antivírus – Programa ou *software* especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de códigos maliciosos.

AP – Do inglês *Access Point.* Dispositivo que atua como ponte entre uma rede sem fio e uma rede tradicional.

Arquitetura cliente/servidor – É toda arquitetura de rede onde estações (microcomputadores) executam aplicações de clientes que se utilizam de programas servidores para transferência de dados do próprio servidor ou comunicação com outras estações e suas aplicações clientes.

Arquivo – É um agrupamento de *bits* que formam uma unidade lógica que possa ser interpretada pelo processador do PC.

Assinatura digital – Código utilizado para verificar a integridade de um texto ou mensagem. Também pode ser utilizado para verificar se o remetente de uma mensagem é mesmo quem diz ser.

Atacante – Pessoa responsável pela realização de um ataque.

Ataque – Tentativa, bem sucedida ou não, de acesso ou uso não autorizado a um programa ou computador. Também são considerados ataques as tentativas de negação de serviço.

Ativos de informação – Patrimônio composto de todas as informações, base de dados e arquivos, documentação de sistemas, manuais de usuário, material de treinamento, procedimentos de suporte ou operação.

Backdoor - Programa que permite a um invasor retornar a um computador comprometido. Normalmente esse programa é colocado de forma a não ser notado.

Backup – Cópia exata de um programa, disco ou arquivo de dados, feita para fins de arquivamento ou para salvaguardar arquivos importantes na eventualidade de que a cópia

ativa (original) seja danificada ou destruída. Por esse motivo, o *backup* também é chamado de cópia de segurança.

Banco de dados – Arquivo composto de registros, contendo cada um deles campos, com um conjunto de operações para pesquisa, classificação, recombinação e outras funções.

BISDN –*Broadband Integrated Services Digital Network*, rede digital de serviços integrados integrados em banda larga. Utiliza fibra óptica e permite uma taxa de transferência de 155 *megabits* por segundo.

Bluetooth – Termo que se refere a uma tecnologia de radiofrequência (RF) de baixo alcance, utilizada para a transmissão de voz e dados.

Boato –*E-mail* que possui conteúdo alarmante ou falso e, geralmente, tem como remetente – ou aponta como autora da mensagem – alguma instituição, empresa importante ou órgão governamental.

Bot – Programa que, além de incluir funcionalidades de *worms*, sendo capaz de se propagar automaticamente por meio da exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em um computador, dispõe de mecanismos de comunicação com o invasor, permitindo que o programa seja controlado remotamente.

***Browser* –** Significa pesquisar, e podemos traduzi-lo como navegador. Na Internet,o termo deve ser interpretado como uma ferramenta que permite a paginação ou folheamento.

Certificado digital – Identidade digital ou ID digital, permite a codificação e a assinatura de mensagens para assegurar sua autenticidade, integridade e inviolabilidade. É muito utilizado em páginas comerciais na Internet.

Chat/Internet relay chat – Conversa em tempo real pelo computador.

Código malicioso – Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador.

Comércio eletrônico – Também chamado de *e-commerce*, é qualquer forma de transação comercial em que as partes interagem eletronicamente.

Conexão segura – Conexão que utiliza um protocolo de criptografia para a transmissão de dados, por exemplo, HTTPS ou SSH.

Confidencialidade – Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Cookies – Absorventes de textos com informações sobre o comportamento dos usuários na rede. Permitem que servidores gravem informações de seu interesse em outro microcomputador remoto.

Cyberspace – Ciberespaço. Assim se designa habitualmente o conjunto das redes de computadores e serviços existente na Internet. É uma espécie de planeta virtual, no qual as pessoas se relacionam virtualmente, por meios eletrônicos.

Display – Termo utilizado para definir dispositivo de tela.

DNS –*Domain Name Server*. Na Internet, é o sistema por meio do qual *hosts* têm endereços de nome de domínio e endereços IP. O endereço de nome de domínio é utilizado pelos usuários e automaticamente traduzido no endereço IP, que é utilizado pelo *software* de roteamento de pacotes.

DoS –*Denial of Service,* ataque *hacker* que consiste em fazer com que o seu computador ou um servidor *web* pare de responder ou até mesmo trave por um excesso de processos solicitados, o que resulta numa negação de serviço.

***Download* –** Ato de transferir o arquivo de um computador remoto para o seu próprio computador, usando qualquer protocolo de comunicações. Processo de transferência de cópia de um arquivo em um computador remoto para outro computador local.

E-book – Livro em formato eletrônico que pode ser baixado pela Internet.

E-business – Palavra que identifica transações e comércios pela Internet que estão baseados em algum sistema de *e-commerce*. Qualquer tipo de negócio efetuado por meio da rede mundial é tratado como um e-business.

Engenharia social – Método de ataque em que uma pessoa faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores.

FAQ –*Frequently Asked Questions.* É um texto que pretende responder, dentro de uma determinada matéria, a questões colocadas frequentemente pelos usuários.

Firewall – Uma *firewall* consiste em um *hardware* e/ou *software* que se interpõe entre duas redes, por exemplo, uma rede interna e um fornecedor de serviço Internet. A *firewall* protege sua rede impedindo o acesso de utilizadores indesejáveis e a passagem de mensagens para receptores específicos externos à rede, tais como os concorrentes.

Fornecedor de *host*ing – Todo aquele que fornece o serviço de *hosting* ou servidor conectado à Internet.

Frame – São subdivisões da janela principal do navegador (ou *browser*). Cada subdivisão funciona como uma pequena janela, exibindo conteúdos independentes.

Freeware – Programa disponível publicamente, segundo condições estabelecidas pelos autores, sem custo de licenciamento para uso.

Gerenciador de Banco de Dados - Interface de *software* entre o banco de dados e o usuário. Um sistema de gerenciamento que permite o controle central da segurança e da integridade dos dados.

GPS- *Global Positioning System.* Consiste numa "constelação" de 24 satélites que estão na órbita da Terra a uma altura de 10.900 milhas, tornando possível às pessoas que utilizem receptores no solo determinar sua posição geográfica entre 10 e 100 metros.

Hipermídia Documento que contém imagens, sons, textos e vídeos, utilizando ligações de hipertextos para permitir o acesso a outro documento.

Hipertexto-São palavras marcadas no texto que permitem acesso a documentos relacionados com o assunto em questão, criando uma linha de pesquisa. Normalmente estão sublinhadas.

Homepage- Assim é chamada a página de abertura de um serviço ou de uma página pessoal

Host - Computador principal de um sistema de computadores ou terminais conectados por enlaces de comunicação.

Hosting- Hospedagem eletrônica locando parte do servidor para distribuição de conteúdos e serviços na rede.

HTML- Extensão para arquivos gerados e salvos no formato *Hiper Text Transfer Marked Language* (Linguagem de Hipertexto Marcado), para construção de *homepages.*

Incidente de segurança-É qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo tratado pela política de segurança.

Intranet- São redes corporativas que se utilizam da tecnologia e infraestrutura de comunicação de dados da Internet. São utilizadas na comunicação interna própria empresa e/ou na comunicação com outras empresas.

Invasão- Ataque bem-sucedido que resulte em acesso, manipulação ou destruição de informações em um computador.

Invasor- Pessoa responsável pela realização de uma invasão (comprometimento).

IP *Internet Protocol,* protocolo responsável pelo percurso de pacotes entre dois sistemas que utilizam a família de protocolos TCP/IP desenvolvida e usada na Internet.

Link- Elo ou ligação. Conexão entre um elemento de um documento de hipertexto, como uma palavra, expressão, símbolo ou imagem, e outro elemento do documento, outro documento de hipertexto, um arquivo ou um *script.* Os *links* são indicados em um documento de hipertexto por meio de *tags* de linguagens de marcação, como a SGML e a HTML. Em geral, essas *tags* não são visíveis ao usuário.

Log- Registro de atividades gerado por programas de computador. No caso de *logs* relativos a incidentes de segurança, eles normalmente são gerados por firewalls ou por IDSs.

Ma1ware-Do inglês *Malicious software (software* malicioso).

MMS -Do inglês *Multimedia Message Service.* Tecnologia amplamente utilizada em telefonia celular para a transmissão de dados, como texto, imagem, áudio e vídeo.

Modem- Modulador DEModulador. Conversor de sinais analógicos (linha telefônica) em sinais digitais (microcomputador) e vice-versa. E usado para ligações entre computadores por meio da linha telefônica. Ao adicionar-se uma placa FAX/ - MODEM ampliam-se os recursos de microcomputador.

MP3- MP3, que significa *Motion Picture Experts Group-Layer* , é um formato de compressão de áudio que cria ficheiros com uma qualidade próxima dos CDs, osquais são 10 ou 20 vezes menores que os ficheiros de música ou os CDs normais. MP3 torna possível mover ficheiros de som de alta qualidade através de um *modem* e pode armazenar 150 canções num CD.

Opt-in- Regra de envio de mensagens que define ser proibido mandar *e-mails* comerciais/spam, a menos que exista uma concordância prévia por parte do destinatário.

Opt-out- Regra de envio de mensagens que define ser permitido mandar *e-mails* comerciais/spam, mas deve-se prover um mecanismo para que o destinatário possa parar de receber as mensagens.

P2P- Acrônimo para *peer-to-peer*. Arquitetura de rede em que cada computador tem funcionalidades e responsabilidades equivalentes. Esse tipo de rede é normalmente implementada via *softwares* P2P, que permitem conectar o computador de um usuário ao de outro para compartilhar ou transferir dados, como MP3, jogos, vídeos, imagens etc.

Password-Veja *Senha.*

Pay-per-view- Serviço de acesso a conteúdo em que se paga no ato de ver o conteúdo.

Phishing- Mensagem não solicitada passa por comunicação de uma instituição conhecida, como um banco, empresa, ou *site* popular, e que procura induzir usuários ao fornecimento de dados pessoais financeiros.

PPP- *Point to Point Protocol.* O PPP implementa o protocolo TCP/IP numa linha telefônica, sendo por meio desta que um computador pessoal se liga à Internet e pode usufruir de todos os serviços e aplicações existentes. E posterior ao SLIP mais completo.

Provedor de Acesso- Instituição que se liga à Internet, via um ponto de presença ou outro provedor, para obter conectividade IP e repassá-la a outros indivíduos

e instituições, em caráter comercial ou não. O provedor de acesso torna possível ao usuário final a conexão à Internet por meio de uma ligação telefônica local.

Proxy- Servidor que atua como intermediário entre um cliente e outro servidor. Normalmente é utilizado em empresas para aumentar a performance de acesso a determinados serviços ou permitir que mais de uma máquina se conecte à Internet.

Rede sem fio- Rede que permite a conexão entre computadores e outros dispositivos por meio da transmissão e recepção de sinais de rádio.

Redes sociais- São plataformas *onhine* que reúnem pessoas em torno de um mesmo interesse. Exemplos: *Facebook, Twitter, Linkedln, Orkut* etc.

Rootkit- Conjunto de programas que tem como finalidade esconder e assegurar presença de um invasor em um computador comprometido.

Roteador- *Router.* Dispositivo responsável pelo encaminhamento de pacotes de comunicação em uma rede ou entre redes. Uma instituição, ao se conectar à Internet**,** deverá adquirir um roteador para conectar sua rede local ao ponto de presença mais próximo. Roteadores vivem se falando aos pares, como *modems.*

Scam -Esquemas ou ações enganosas e/ou fraudulentas. Normalmente, têm como finalidade obter vantagens financeiras.

Scan Técnica normalmente implementada por um tipo de programa, projetado para efetuar varreduras em redes de computadores. Veja *Scanner*

Scanner - Programa utilizado para efetuar varreduras em redes de computador com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. Amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador. Ou dispositivo óptico de entrada que usa sensores de luz para capturar uma imagem no papel ou algum outro meio. Há diversos *scanners,* entre eles: de mão (o usuário passa o dispositivo sobre um documento estático), de mesa (o cabeçote de varredura é movimentado sobre um documento fixo), com alimentação de papel (o documento é passado sobre um cabeçote de varredura estático), tambor (o documento é girado ao redor de um cabeçote varredura estática).

Screen1ogger -Forma avançada de *keylogger,* capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse é* clicado, ou armazenar a região que circunda a posição em que o *mouse* é clicado. Veja também *Keylogger.*

Server- Servidor. É o computador que administra e fornece programas e informações para os outros computadores conectados. No modelo cliente-servidor, é programa responsável pelo

atendimento a determinado serviço solicitado por um cliente. Serviços como *archie, gopher*, WAIS e *web* são providos por servidores. Referindo-se a equipamento, o servidor é um sistema que provê recursos tais como armazenamento de dados, impressão e acesso *dia/—up* para usuários de uma rede de computadores.

Shareware- *Software* que é distribuído livremente, desde que seja mantido o seu formato original, sem modificações, e seja dado o devido crédito a seu autor. Normalmente é feito para ser testado durante um curto período de tempo. Sistema de Pagamento Seguro

SPS Sistema de pagamento eletrônico que possui **s***oftware* de segurança *firewall*, utilizado, principalmente, em Bancos.

SMS- Do inglês, *Short Message Service.* Tecnologia amplamente utilizada em telefonia celular para a transmissão de mensagens de texto curtas. Diferentemente do MMS, permite apenas dados do tipo texto e cada mensagem é limitada em caracteres alfanuméricos.

SMTP *Simple Mau Transfer Protocol.* Protocolo Internet usado para correio eletrônico.

Sniffer- Dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um Invasor para capturar informações sensíveis (como senhas de usuários), nos casos em que estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.

Sockets- O nome da interface que implementa os protocolos TCP/IP. Interface é um conjunto de chamadas possíveis a bibliotecas que contém rotinas que implementam determinados objetivos.

Software- Programas de computador; instruções que o computador é capaz de entender e executar.

Spam- Termo usado para se referir a *e-mails* não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem também é referenciada como UCE (do inglês, *Unsolicited Commercial E—mail).*

Spammer- Pessoa que envia *spam.*

TCP- *Transmission Cotrol Protocol.* O protocolo dentro do TCP/IP que controla a subdivisão das mensagens de dados em pacotes a serem enviados por meio do protocolo IP e a remontagem e verificação das mensagens completas do cotes recebidos pelo IP.

Trojan horse- Veja *Cavalo de troia.*

UCE- Do inglês, *Unsolicited Commercial E-mail.* Termo usado para se referir a *e—mails* comerciais não solicitados.

UIT- União Internacional de Telecomunicações.

Upgrade- O mesmo que atualização. Passar para uma versão mais nova, geralmente mais poderosa ou mais sofisticada de um programa.

Up1oad- Em português, carregar. Operação de transferência de um arquivo ou uma página da Internet do computador para um provedor de acesso.

URL - *Universal Resource Location.* É um identificador na Internet que mostra qual tipo de servidor deve ser acessado, o equipamento em que a informação reside sua localização nesse equipamento, por exemplo: http://www.patriciapeck.com.br.

Usuário- Todo aquele que acessa a rede Internet.

Vírus- Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende execução do programa ou arquivo hospedeiro para que possa tornar-se ativo e dar continuidade ao processo de infecção.

VPN- Do inglês *Virtual Private Network.* Termo usado para se referir a construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública.

VRML- *Virtual Reality Markup Language.* Formato padrão para representar a 3ª dimensão seria o 3D, em vetor gráfico. Foi superado pelo X3D.

Vu1nerabilidde- Falha no projeto, na implementação ou na configuração de *um software* ou sistema operacional que, quando explorada por um atacante, resulta n*a* vio1ação da segurança de um computador.

WAP- *Wireless Aplication Protocol.* É um conjunto de especificações, desenvolvida pelo WAP *Forum,* que permite aos programadores usar a linguagem *Wirdi Markup Language* (WML) para montar aplicações em rede destinadas a dispositivos de mão sem fios. O WAP foi concebido para funcionar dentro dos limites de tais dipositivos: uma memória e potência de *Central Processing Unit* (CPU) limitadas; visores pequenos e monocromáticos; baixa largura de banda; e conexões algo instáveis.

Wi-Fi -Do inglês, *Wireless Fidelity.* Termo usado para se referir genericamente a redes sem fio que utilizam qualquer um dos padrões 802.11.

Wireless- Do inglês, sem fio.

Worm Programa capaz de se propagar automaticamente por meio de redes, enviando cópias de si mesmo de computador para computador. Diferentemente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente

executado para se propagar. Sua propagação se dá mediante a exploração de vulnerabilidades existentes ou falhas na configuração de *softwares* instalados em computadores.

WPA- Do inglês, *Wi-Fi Protected Access.* Protocolo de segurança para redes fio desenvolvido para substituir o protocolo WEP, devido a suas falhas de segurança. Essa tecnologia foi projetada para, por meio de atualizações de *software,* operar com produtos *Wi-Fi* que disponibilizavam apenas a tecnologia WEP. Inclui duas melhorias em relação ao protocolo WEP que envolvem melhor criptografia para transmissão de dados e autenticação de usuário.

Fonte: PINHEIRO, P.P. **Direito digital.** 5. ed. São Paulo: Saraiva, 2013.

APÊNDICE A – Tabela de Amostragem nº 1

Site: Google Acadêmico

Categoria pesquisada: "Ciberdemocracia"

Resultados: 884 resultados (sendo 587 em português). Alguns dos mais relevantes foram os seguintes:

Categorias	Título	Autor(es)	Ano
Ciberdemocracia	Ciberdemocracia: análise dos desafios e possibilidades de iniciativa popular via Internet no Brasil.	Rafael Santos de Oliveira e Letícia Bodanese Rodegheri.	2012
Ciberdemocracia	O futuro da Internet: em direção a uma Ciberdemocracia planetária.	Márcio Roberto de Lima.	2012
Ciberdemocracia	Cidadania, comunicação e Ciberdemocracia: Uma leitura crítica da comunicação e o desenvolvimento social.	Francisco Sierra Caballero.	2013
Ciberdemocracia	Ciberdemocracia: (re)pensar a democracia representativa a partir das redes sociais virtuais.	GrasielaGrosselli.	2012
Ciberdemocracia	Ciberespaço, globalização e novas tecnologias: (re)pensando as relações entre cidadania e administração pública em um contexto de formação da Ciberdemocracia.	Ricardo de Macedo Menna Barreto.	2012
Ciberdemocracia	Ciberdemocracia, ativismo digital e novas mídias: redefinições da esfera pública no século XXI.	Rafael Santos de Oliveira.	2012
Ciberdemocracia	Educação para Ciberdemocracia: possibilidades de empoderamento e ativismo das classes populares.	Michel Carvalho da Silva.	2014
Ciberdemocracia	A construção da Ciberdemocracia por meio do debate público na blogosfera.	Letícia BodaneseRodegheri, Noemi de Freitas Santos e Rafael Santos de Oliveira.	2012

APÊNDICE B – Tabela de Amostragem nº 2

Site: Google Acadêmico

Categoria pesquisada: "Cibercrime"

Resultados: 138 resultados (sendo 134 em português). Sendo relevantes:

Palavra-chave	Título	Autor(es)	Ano
Cibercrime	Competência nos Cibercrimes de pedofilia: aplicação da lei penal no espaço e a necessidade de cooperação internacional.	Inácio Pal Lins Neto.	2012
Cibercrime	Taxonomia do Cibercrime no contexto da legislação vigente.	LUZ, A.G.P.; CASTRO, R.C.C.	2013
Cibercrime	Os novos crimes de informática criados com o advento das leis 12.735/2012 E 12.737/2012.	Danielly Maia dos Santos.	2015
Cibercrime	Malefícios causados pelo mau uso do computador e da Internet.	Caio Regis Caroca, Ed Porto Bezerra e Emy Porto Bezerra	2013
Cibercrime	Crimes contra o patrimônio na sociedade da informação.	Jeísa dos Santos Pereira Linhares Pordeus.	2014
Cibercrime	Preconceito e discriminação pela Internet.	José Eduardo Lourenço dos Santos.	2013
Cibercrime	A privacidade e a proteção dos dados pessoais no ciberespaço como um direito fundamental: Perspectivas da construção de um marco regulatório para o Brasil.	Vinícius Borges Fortes e Salete Oro Boff.	2014
Cibercrime	Crianças e adolescentes internautas como alvo da criminalidade online: pedofilia e pornografia na Internet.	Laura Pereira do Nascimento e Rosane Leal da Silva.	2014

APÊNDICE C – Tabela de Amostragem nº 3

Site: Google Acadêmico

Categoria pesquisada:“Crimes no Ciberespaço”

Resultados: 10 resultados (ambos em português) sendo relevante:

Palavra-chave	Título	Autor(es)	Ano
Crimes no Ciberespaço	Implicações de Externalidades Negativas da Internet sobre a Legislação Brasileira de Crimes no Ciberespaço: o Caso de Ataques por Negação de Serviço.	David Pereira Barbosa, Anderson Luiz Coan, Tharsis Martins Novais.	2012

APÊNDICE D – Tabela de Amostragem n° 4

Site: Google Acadêmico

Categoria pesquisada:“Crimes na Internet”

Resultados: 107 resultados (sendo 105 em português). Sendo relevantes:

Palavra-chave	Título	Autor(es)	Ano
Crimes na Internet	A Responsabilidade Civil dos Provedores de Hospedagem por “Perfis Falsos” na Internet.	Fábio Murilo Nazar.	2013
Crimes na Internet	Fundamentos dos crimes virtuais: da Cibercultura à prática ilícita no ciberespaço.	Liziane Menezs Souza, Mariele Oliveira Pulga, Angelita Woltmann, Raquel Buzatti Souto, Adalberto Fernandes Falconi, Raoni Paiva Pereira e Luis Gustavo Durigon.	2013
Crimes na Internet	Marco civil e a proteção da privacidade.	Sergio Amadeu da Silveira.	2014
Crimes na Internet	Cibersegurança: Os desafios do Brasil no ciberespaço.	Victor Mateus Espindula.	2012

APÊNDICE E – Tabela de Amostragem nº 5

Site: Google Acadêmico

Categoria pesquisada:"Democracia na Internet"

Resultados: 20 resultados (em português) sendo estes os mais relevantes:

Palavra-chave	Título	Autor(es)	Ano
Democracia na Internet	A democracia na Internet e a inclusão digital brasileira.	Egon Walter Wildauer, Talita Midori Moura Inaba, Guilherme Parreira da Silva.	2014
Democracia na Internet	Limites e possibilidades da política e da democracia na Internet: um olhar a partir da realidade brasileira.	José Antonio Gomes de Pinho, Júlio César Andrade de Abreu, Ingrid Winkler, Kátia Morais e Fabiano Maury Raupp.	2012
Democracia na Internet	Mudanças institucionais e cidadania: da participação social ao marco civil da Internet.	LitonLanesPilau Sobrinho e Thami Covatti Piaia.	2015
Democracia na Internet	Democracia digital: os rumos da regulamentação legislativa no ordenamento jurídico brasileiro.	Bruna Pinotti Garcia e Guilherme Domingos de Luca.	2012

APÊNDICE F – Tabela de Amostragem nº 6

Site: Google Acadêmico

Categoria pesquisada:"Cybercrime"

Resultados: 11.500 resultados (período de 2012 a 2015), sendo relevantes alguns textos em língua inglesa, como:

Palavra-chave	**Título**	**Autor(es)**	**Ano**
Cybercrime	Measuring the Cost of Cybercrime	Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore, Stefan Savage	2013
Cybercrime	Cybercrime: The Case of Obfuscated Malware	MamounAlazab, SitalakshmiVenkatraman, Paul Watters, Moutaz Alazab, Ammar Alazab	2012
Cybercrime	The Economic Impact of Cybercrime and Cyber Espionage	James Lewis and Stewart Baker	2014
Cybercrime	Cybercrime and virtual offender convergence settings	Melvin R. J. Soudijn, Birgit C. H. T. Zegers.	2012
Cybercrime	Cybercrime in Asia: Trends and Challenges	RodericBroadhurst Ph.D., Lennon Y. C. Chang Ph.D.	2012

APÊNDICE G – Tabela de Amostragem n° 7

Site: Google Acadêmico

Categoria pesquisada:“Ciberdelincuencia”

Resultados: 266 resultados (período de 2012 a 2015), sendo relevantes em língua espanhola alguns como:

Palavra-chave	Título	Autor(es)	Ano
Ciberdelincuencia	Ciberdelincuencia un mal que afecta a la sociedad actual.	MSc. Emilio Javier Flores Villacrés, MSc. María Isabel Asanza Molina, Ing. Marcelo Berrones Miguez	2014
Ciberdelincuencia	Retos y riesgos de la ciberdelincuencia: el ciberbullying.	Calmaestra Villén, Juan	2014
Ciberdelincuencia	El ciberdelitola contribución de las estrategias de seguridad a la lucha contra la ciberdelincuencia: armas jurídicas contra el nuevo enemigo.	Rafael Alvarez Oreja-Egaña	2012
Ciberdelincuencia	Ciberdelincuencia: desarrollo y persecución tecnológica.	Mateos Pascual, Iván	2013
Ciberdelincuencia	Reflexiones sobre ciberdelincuencia y redes sociales digitales	Manuel Ollé Sesé	2014

APÊNDICE H – Tabela de Ameaças

Vírus de *boot* Esse tipo de vírus se manifesta na inicialização do sistema do computador. Um CD, DVD, *pen drive* ou outros tipos de armazenadores de arquivos podem ser contaminados se fixados na máquina quando o sistema se inicializa. São exemplos dessa modalidade os chamados ping-pong, Jerusalém, entre outros. Essa espécie de vírus é avaliada como pioneira, surgindo no final da década de 80.	Vírus *time bomb* Esse vírus é caracterizado por ter uma data certa para se manifestar no computador infectado. A ameaça é chamada por vezes de bomba-relógio e gatilho, já que possui determinada circunstância para ativar os seus efeitos. Conhecidos exemplos desse vírus são o michelangelo, o eros, o 1º de abril e o sexta-feira 13.
Worm Modalidade de código malicioso que reside na memória ativa do computador, muitas vezes, por intermédio de uma vulnerabilidade desse que poder ser em razão do sistema está desatualizado.Conhecido como verme, ele replica-se automaticamente. Os computadores infectados podem gerar *e-mail*s de conteúdo malicioso para a lista de contatos do usuário, e esses vírus também são espalhados nas redes sociais da vítima.	*Botnets* Os computadores infectados por vírus que proporciona ao agente "invadir" as operações nele realizadas e possibilitam que ele realize atividades na máquina são denominados*botnets.* Estes computadores são invadidos por vulnerabilidades principalmente na configuração do sistema ou softwares. Um exemplo da atuação de criminosos que realizam tal invasão é a promoção de ataques "DDoS", que consiste no envio por computadores de solicitações para um servidor ou rede visando bloqueá-los.
Deface Esta ameaça diz respeito a desconfiguração de sites, b*logs* ou perfis de redes sociais.Certas vezes, essas são implantadas com a finalidade de defender concepções religiosas, políticas e até mesmo de cunho filosófico. Este também foi promovido juntamente com o DDoS nos ataques aos sites governamentais.	Cavalo de Tróia Tal ameaça se instala no computador por meio do *download* de um arquivo que ao ser executado permite que o invasor possa controlar o computador da vítima à distância, obtendo até mesmo dados confidenciais dessa, como o número do cartão de crédito ou senhas de redes sociais.O simples ato de abrir um anexo de *e-mail* pode fazer com que outra pessoa roube seus dados a partir da invasão por intermédio do Cavalo de Tróia.
Keylogger Esse software realiza o monitoramento de informações digitadas pelo usuário da máquina, para que assim o criminoso possa roubar informações sobre a vítima e cometer alguns crimes a partir dessas. Eles são infiltrados no computador alheio, muitas vezes, através de programas de spam que possibilitam o envio de *e-mail* para milhares de pessoas de uma vez.	*Hijacker* Esta ameaça permite o direcionamento do usuário a sites diferentes do que ele buscou, sequestrando o navegador, e também definindo determinado site como página inicial do navegador, além de *download* de pop-ups com conteúdo pornográfico, por exemplo. Os Hijackeres se aproveitam das brechas de segurança para modificar o registro do Windows promovendo ações sem o consentimento do usuário.
Sniffer Esse tipo de ameaça possui o objetivo de monitorar a dinâmica da rede do computador da vítima para que os dados transmitidos por ela possam ser explorados, dispondo deleso criminoso pode realizar diversas ações, prejudicando o usuário. O Cain and Abel e o Wireshark são os programas mais comuns de realizar tais funções.	*Backdoor* O *backdoor*é um tipo de programa que uma vez instalado deixa o computador infectado propenso a invasões.

Rootkit Os *rootkits* são programas que contaminam atividades e processos de memória, podendo gerar mensagens de erro. São bastante eficientes já que a maioria dos antivírus não consegue detectá-los, pois eles permanecem ocultos, podendo ser instalados fisicamente ou à distância por intermédio de outro computador. Podem ser instalados através da abertura de *e-mail* com anexo ou *link* com arquivo infectado. Este arquivo precisa ser executado e para o convencimento do usuário a fazê-lo são utilizados diversos meios fraudulentos para despertar o interesse dele. Como, por exemplo, *e-mail*s de agentes criminosos que fingem ser de determinado órgão como SERASA, Ministério Público, lojas virtuais, entre outros.	*Hoax* O hoax consiste em fatos e histórias postadas e compartilhadas na *web*, alarmantes e comoventes, de forma que chamem atenção das pessoas para que essas espalhem o conteúdo e o criador de tal alcance seu objetivo. São exemplos histórias de pessoas doentes ou órgãos de ajuda e proteção para arrecadar dinheiro, projetos de lei que serão votados nas assembleias, lendas urbanas, correntes entre outros episódios que gerem contrariedades e incômodos às vítimas. Por conta do teor alarmante e exorbitante dos fatos eles são compartilhados em redes sociais e outros meios por milhões de pessoas, geram transtornos as pessoas ingênuas que acreditam nas mentiras e afetam a credibilidade das informações da Internet. Existem alguns sites que ajudam a desmascarar tais boatos, como o www.e-farsas.com.
PhishingScam Esta ameaça refere-se também a criação de uma falsa história para seduzir os usuários de computadores, mas o objetivo é descobrir informações desses para obter lucros ou causas danos a eles. Um exemplo são pessoas que se passam por instituições conhecidas, como uma empresa, para que as vítimas acessem sites fraudulentos que vão roubar suas informações, como número de conta bancárias e senhas. Outro ato típico do PhishingScam são as mensagens que induzem o usuário a preencher formulários com seus dados com o mesmo objetivo abordado (JORGE; WENDT, 2013, p. 18-39).	Chave mestra (*superzapping*) Trata-se do uso não autorizado de programas para modificar, destruir, copiar, inserir, utilizar ou impedir o uso de dados arquivados em um sistema informático. O nome provém de um programa chamado superzap, que permite abrir qualquer arquivo de um computador, ainda que paralisado e mesmo que se ache protegido por sistema de segurança. (JORGE; WENDT, 2013, p. 18-39).