UNIVERSIDADE DO ESTADO DO AMAZONAS
ESCOLA SUPERIOR DE CIÊNCIAS SOCIAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM SEGURANÇA PÚBLICA, CIDADANIA E DIREITOS HUMANOS

CLAUDEMARA ALBANO GUIMARÃES

AS REDES VIRTUAIS DO SISTEMA DE SEGURANÇA PÚBLICA E AS COMUNIDADES DE INTELIGÊNCIA: UMA REFLEXÃO LEGAL.

MANAUS
2018

CLAUDEMARA ALBANO GUIMARÃES

AS REDES VIRTUAIS DO SISTEMA DE SEGURANÇA PÚBLICA E AS COMUNIDADES DE INTELIGÊNCIA: UMA REFLEXÃO LEGAL.

Dissertação apresentada ao Programa de Pós-Graduação em Segurança Pública, Cidadania e Direitos Humanos da Universidade do Estado do Amazonas, como requisito para obtenção do grau de Mestre em Segurança Pública, Cidadania e Direitos Humanos.

Orientador: Prof. Dr. Alfredo Wagner Berno de Almeida.

MANAUS
2018

CLAUDEMARA ALBANO GUIMARÃES

AS REDES VIRTUAIS DO SISTEMA DE SEGURANÇA PÚBLICA E AS COMUNIDADES DE INTELIGÊNCIA: UMA REFLEXÃO LEGAL.

Dissertação apresentada ao Programa de Pós-Graduação em Segurança Pública, Cidadania e Direitos Humanos da Universidade do Estado do Amazonas, como requisito para obtenção do grau de Mestre em Segurança Pública, Cidadania e Direitos Humanos, pela Banca Examinadora formada por:

Manaus, de março de 2018

_____

Prof. Alfredo Wagner Berno de Almeida, Dr - Orientador, UFAM

_____

_____

Dedico esse trabalho à Lusmar Villarouca Guimarães, meu marido dedicado e compreensivo, aos meus filhos amados Cláudio Albano Guimarães e Jéssica Albano Guimarães. Sem vosso apoio esse trabalho não seria possível. Muito obrigada.

AGRADECIMENTOS

Agradeço pela oportunidade e pelo apoio do meu orientador, Prof. Dr. Alfredo Wagner Berno de Almeida, por acreditar neste projeto desde o início e por me incentivar a finalizar esta pesquisa.

Agradeço pelas horas dedicadas ao atendimento e orientação, com a finalidade de desenvolver uma pesquisa relevante tanto para o Sistema de Segurança Pública do Estado do Amazonas como para o meio acadêmico.

Agradeço aos professores doutores Izaura Rodrigues Nascimento e Erivaldo Cavalcante e Silva e Filho pelas suas orientações, apresentadas durante a banca de qualificação, que foram de grande valor para a realização desta pesquisa.

Agradeço por todo o carinho e apoio durante este processo de pesquisa e desenvolvimento, não apenas profissional, mas pessoal. A minha família, agradeço pela compreensão durante minha ausência e por me incentivarem a nunca desistir dos meus objetivos.

Agradeço ao meu querido Deus por ter me dado sabedoria e discernimento para iniciar, ousar, desenvolver e finalizar este projeto, sempre com a intenção de apresentar o melhor, na busca de aprimorar os dons e talentos que Ele me dispensou.

Nunca tenha certeza de nada, porque a sabedoria começa com a dúvida." (SIGMUND FREUD)

RESUMO

O presente trabalho contribuirá com novas informações ao meio acadêmico e profissional, sistematizando um problema que já vem sendo observado há algum tempo no sentido de procurar identificar até que ponto, as comunidades de inteligência conseguem conter as violações nas redes virtuais do sistema de segurança pública pelas comunidades de rede e como vem sendo aplicado o ordenamento jurídico brasileiro diante dessa invasão e quebra de sigilo. Todo esse processo de investigação será realizado através de uma análise de forma exploratória, documental e descritiva com a finalidade de verificar se ocorrem invasões em redes virtuais do sistema de segurança pelas comunidades de rede, e como o sistema de segurança pública através das comunidades de inteligência vem tolhendo e aplicando o ordenamento jurídico brasileiro diante desses comportamentos complexos. As questões norteadoras foram detalhadamente direcionadas, por intermédio de roteiros flexíveis para orientação a gestores responsáveis pela segurança da rede e à Secretaria Executiva Adjunta de Inteligência objetivando que através de seus relatos acerca da experiência sobre o assunto possam nos ajudar a responder o que originou o problema de pesquisa, ou seja, se ocorre ou não essa violação por essas comunidades de rede ao sistema de segurança, se há ordenamento jurídico para coibir essa violação, e se as comunidades de inteligência estão preparadas para tolher esse comportamento e efetivar esse controle.

Palavras-chave: Redes Virtuais. Sistema de Segurança Pública. Comunidades de Inteligência. Comunidades de Rede. Violação ao Sistema Virtual. Ordenamento Jurídico.

ABSTRACT

This study will contribute new information to the academic and professional environment, systematizing a problem that has already been observed for some time in order to seek to identify to what extent the intelligence communities can contain violations in virtual networks of the public security system by network communities and as has been applied Brazilian legal system before this invasion and confidentiality breaches. This entire process of investigation will be carried out through an analysis of exploratory, documentary and descriptive in order to verify if there are intrusions into virtual network security system by network communities, and how the public security system through the intelligence communities comes retaining and applying the Brazilian legal system on these complex behaviors. The guiding questions were detailed in detail through flexible roadmaps for guidance to managers responsible for network security and to the Deputy Executive Secretary of Intelligence who, through their reports about the experience on the subject, can help us to answer what gave rise to the problem of search, if it occurs or not this violation by these network communities the security system, if there is law to curb this violation, and intelligence communities are prepared to stunt this behavior and carry out this control.

Keywords: Virtual networks. Public Security System. Intelligence communities. Network communities. Violation of the Virtual System. Legal System.

LISTA DE SIGLAS

AM	Amazonas.
ABIN	Agência Brasileira de Inteligência
CI	Contra-Inteligência
CIA	*Central Intelligence Agency* (Agência Central de Inteligência dos Estados Unidos)
CGI	Coordenação Geral de Inteligência da SENASP
DSI	Departamento de Sistemas de Informação
DG	Delegacia Geral.
DEL	Delegado de Polícia.
DIP	Distrito Integrado de Polícia.
ESC	Escrivão de Polícia.
INV	Investigador de Polícia.
NSA	*National Security Agency* (Agência Nacional de Segurança).
PCAM	Polícia Civil do Amazonas.
PRODAM	Processamento de Dados da Amazônia
SSP	Secretaria de Estado da Segurança Pública.
SEAI	Segurança Executiva Adjunta de Inteligência
SENASP	Secretaria Nacional de Segurança Pública
SISBIN	Sistema Brasileiro de Inteligência
SISP	Sistema de Inteligência de Segurança Pública
UEA	Universidade do Estado do Amazonas.

SUMÁRIO

1 INTRODUÇÃO

A necessidade de investigar o presente tema, surgiu com a constante veiculação na mídia sobre a invasão em ambientes virtuais por integrantes de comunidades de rede, responsáveis pela obtenção de informações e acessos não autorizados de particulares, comportamento este que vem causando grande preocupação nos meios virtuais, tanto no tocante a segurança do sistema, quanto ao controle de dados pelos órgãos da segurança pública.

O referido projeto de pesquisa apresenta-se como primeira investigação no estado do Amazonas, acerca da invasão em redes virtuais do sistema de segurança pelas comunidades de rede, e como a secretaria de segurança pública através das comunidades de inteligência vem tolhendo e aplicando o ordenamento jurídico brasileiro diante desses comportamentos complexos.

A produção acadêmica brasileira sobre comunidades de inteligência e comunidades de rede é quase inexistente, portanto tivemos o cuidado em agrupar o pensamento de alguns autores que tratam tanto da questão comunidade, como comunidades de inteligência e comunidades de rede, para que pudéssemos analisar suas definições e a partir daí nos posicionarmos em relação ao tema intrigante e desafiador que iremos descrever quando nos reportarmos a verificação de invasão às redes virtuais do Sistema de Segurança Pública do Estado do Amazonas.

No presente trabalho de pesquisa nos deteremos apenas ao estudo relacionado a invasão em redes virtuais do sistema de segurança pelas comunidades de rede, e como as comunidades de inteligência do sistema de segurança pública vem conseguindo tolher essa invasão operacionalizando o controle dessa rede virtual, através de aplicativos e softwares especializados que possam deter quaisquer tipos de acesso não autorizados a rede de dados, observando-se, ainda a aplicação do ordenamento jurídico brasileiro diante desses comportamentos com o intuito de prevenir estes comportamentos complexos e punir os responsáveis pela invasão no ambiente virtual dos sistemas de informação, tomando como parâmetro as leis nº 9.296/96, 12.737/2012 e 12.965/2014.

O referido estudo apresenta-se de grande importância institucional e acadêmica, pois visa orientar futuras pesquisas e políticas públicas voltadas a corroborar para uma melhor prestação dos serviços das polícias do Estado do Amazonas e demais órgãos que venham a ter interesse no assunto.

Será utilizado neste projeto o método dedutivo e iniciar-se-á com uma pesquisa bibliográfica na literatura (livros, jornais, revistas especializadas, artigos, teses e dissertações, vídeos, documentários e filmes), e documental com dados pertinentes ao assunto, com análise sobre o recorte.

Faremos ainda uma análise descritiva, objetivando identificar até que ponto o comportamento complexo dessas comunidades de rede interfere no ambiente de trabalho do policial, e como o sistema de segurança pública através das comunidades de inteligência pode resguardar esse ambiente, através de um sistema de segurança virtual com a finalidade de proteger dados, aplicando o ordenamento jurídico brasileiro diante de sua intrusão nos sistemas de informação.

Dentro dessa problemática da pesquisa, tentaremos em nosso estudo descrever quem são os *hackers*, eles vistos como celebridades, a sua cultura e o comportamento complexo dessas comunidades de rede.

Quanto à abordagem do problema a tipologia a ser adotada será a qualitativa. A seguir, promover-se-á a pesquisa de campo, onde esse universo específico se estabelecerá através da elaboração despadronizada e não-estruturada de um roteiro flexível para orientação das conversas informais, com especialistas no assunto, onde poderão ser exploradas mais amplamente algumas questões neste sentido, não havendo limitação a um questionário com perguntas fixas e imutáveis, podendo ocorrer uma variação das mesmas consoante as informações, observando-se a necessidade de um roteiro diferenciado para cada um deles, em razão de suas distinções. Será também aplicado o critério de seleção destes colaboradores, direcionando-se o referido roteiro de pesquisa a profissionais de inteligência pertencentes à Secretaria de Segurança Pública que tenham experiência no trabalho de análise, confidencialidade e controle de dados dos sistemas de informação da Secretaria Executiva Adjunta de Inteligência, e a analistas da Prodam que tenham conhecimento em proteger e neutralizar a ação de *hackers*, por intermédio de *softwares* específicos, e que controlem e protejam o Sistema de Rede da Secretaria de Segurança Pública, além de outros órgãos que possam nos ajudar a complementar e enriquecer o estudo.

Pierre Bourdieu nos esclarece que "ainda que a relação de pesquisa se distinga da maioria das trocas da existência comum, já que tem por fim o mero conhecimento, ela continua, apesar de tudo, uma *relação social* que exerce efeitos (variáveis segundo os diferentes parâmetros que a podem afetar) sobre os resultados obtidos.

Sem dúvida a interrogação científica exclui por definição a intenção de exercer qualquer forma de violência simbólica capaz de afetar as respostas; acontece, entretanto, que nesses assuntos não se pode confiar somente na boa vontade, porque todo tipo de distorções está inscrito na própria estrutura da relação de pesquisa. Essas distorções devem ser reconhecidas e dominadas; e isso na própria realização de uma prática que pode ser refletida e metódica, sem ser aplicação de um método ou a colocação em prática de uma reflexão teórica."

Para o desenvolvimento deste Projeto, optou-se primeiramente em realizar uma pesquisa bibliográfica e documental, durante os meses de julho, agosto, setembro, outubro, novembro e dezembro de 2016, objetivando compreender invasão em redes virtuais do sistema de segurança pelas comunidades de rede, e como o sistema de segurança pública através das comunidades de inteligência vem tolhendo e aplicando o ordenamento jurídico brasileiro diante desses comportamentos complexos.

Em janeiro de 2017 apresentamos o primeiro esboço do projeto para exame de qualificação a ser verificado pelo nosso orientador, para as devidas observações.

Foram feitas pesquisas de campo dentro do ambiente da Secretaria de Segurança Pública para então através de um levantamento realizado por intermédio de roteiros aplicar o critério de seleção, ocasião em que esses roteiros foram direcionados a profissionais de inteligência pertencentes à Secretaria de Segurança Pública que tivessem experiência no trabalho de análise, confidencialidade e controle de dados dos sistemas de informação da Secretaria Executiva Adjunta de Inteligência, e a analistas da Prodam que também tivessem conhecimento em proteger e neutralizar a ação de *hackers*, por intermédio de softwares específicos, e que controlassem o Sistema de Rede da Secretaria de Segurança Pública, para que então pudéssemos relatar as experiências vivenciadas por eles com a finalidade de enriquecer a pesquisa voltada a contribuição ao meio acadêmico.

Após aprovação no exame de qualificação foram aplicados roteiros diferenciados aos analistas e responsáveis envolvidos com a administração, gestão e controle de segurança das redes virtuais do sistema de segurança pública, que em razão da atividade que desenvolvem, e por questões de segurança não puderam se identificar.

A intenção dessa pesquisa orientou-nos no sentido de responder, após esse levantamento de informações, se há ou não, invasão dos sistemas virtuais do sistema de segurança pública pelas comunidades de rede, qual a importância do sigilo,

controle e segredo dessas informações, se há controle pelas comunidades de inteligência para dirimir ou eliminar o risco neste ambiente virtual do sistema de segurança, se há previsão no ordenamento jurídico para coibir essa invasão aos sistemas, e quem seriam estes profissionais responsáveis por este monitoramento e controle, e suas qualificações específicas.

Trataremos também da violação da segurança, da legislação cibernética aplicada a essas ocorrências, e do estado de direito e de liberdade que descaracterizam a privacidade pessoal.

2 METODOLOGIA

2.1 PROBLEMA DA PESQUISA

A investigação deste projeto será no sentido de procurar identificar: Até que ponto, as comunidades de inteligência conseguem conter as violações nas redes virtuais do sistema de segurança pública pelas comunidades de rede e como vem sendo aplicado o ordenamento jurídico brasileiro diante dessa invasão e quebra de sigilo?

2.2 QUESTÕES NORTEADORAS

Se há invasão pelas comunidades de rede no meio virtual do ambiente de dados do sistema de segurança pública?

Em caso positivo, como essas comunidades de rede conseguem invadir o sistema de segurança?

Se há algum mecanismo de segurança da informação ou privacidade existente no ambiente virtual da secretaria de segurança?

O sistema de segurança pública, através das comunidades de inteligência, tem conseguido tolher a invasão pelas comunidades de rede nos sistemas de informação?

Se há no ordenamento jurídico brasileiro meios para inibir a invasão dessas comunidades de rede que atuam nessas redes virtuais policêntricas?

Se há especialistas ou profissionais responsáveis pela segurança da rede da secretaria de segurança?

Que políticas públicas de segurança pública já existem ou estão sendo implementadas para que se protejam dados da segurança pública e se possa dificultar essa violação ao sistema virtual?

2.3 OBJETIVO GERAL

Analisar de forma exploratória, documental e descritiva a invasão em redes virtuais do sistema de segurança pelas comunidades de rede, e como o sistema de segurança pública através das comunidades de inteligência vem tolhendo e aplicando o ordenamento jurídico brasileiro diante desses comportamentos complexos.

2.4 OBJETIVOS ESPECÍFICOS

Descrever as comunidades de rede e as comunidades de inteligência e como se comportam no ambiente virtual da secretaria de segurança pública.

Investigar como ocorre a invasão nos sistemas virtuais do sistema de segurança pública pelas comunidades de rede e a importância em manter o sigilo e o segredo dessas informações.

Verificar se há no ordenamento jurídico alguma previsão para coibir a invasão pelas comunidades de rede em razão dos crimes registrados no sistema de segurança pública.

Identificar se há controle da segurança pelas comunidades de inteligência a essas interferências virtuais no sistema de segurança pública pelas comunidades de rede, e se podem prejudicar as investigações criminais e o ambiente do trabalho policial.

3 COMUNIDADES

Chamamos comunidade a uma relação social quando a atitude na ação social - no caso particular, em termo médio ou no tipo puro - inspira-se no sentimento subjetivo (afetivo ou tradicional) dos partícipes da constituição de um todo. (FERNANDES, 1920, p.140).

A *comunidade* pode apoiar-se sobre toda espécie de fundamentos afetivos, emotivos e tradicionais: uma confraria *pneumática*, uma relação erótica, uma relação de piedade, uma comunidade "nacional", uma tropa unida por sentimento de camaradagem. Este tipo é expresso com maior adequação pela comunidade familiar. Entretanto, a imensa maioria das relações sociais participam em parte da "comunidade" e em parte da " sociedade". Toda relação social, mesmo aquela mais a estritamente originada na persecução racional de algum fim (a clientela, por exemplo), pode dar lugar a valores afetivos que transcendem os simples fins almejados. Toda " sociedade" que exceda os termos de uma mera união para um propósito determinado e que, não estando limitada previamente a certas tarefas, seja de longa duração e dê lugar a relações sociais entre as mesmas pessoas - como as "sociedades" criadas dentro de um mesmo quadro militar, numa mesma classe da escola, num mesmo escritório, numa mesma oficina - tende, em maior ou menor grau a promover os referidos afetos. Ao contrário, uma relação que por seu sentido normal é uma comunidade, pode estar orientada por todos ou parte de seus participantes segundo certos fins racionalmente sustentados. (FERNANDES, 1920, p. 141).

Os significados e sensações que as palavras carregam não são, é claro, independentes. “Comunidade” produz uma sensação boa por causa dos significados que a palavra “comunidade” carrega — todos eles prometendo prazeres e, no mais das vezes, as espécies de prazer que gostaríamos de experimentar, mas que não alcança mais. (BAUMAN, 2003, p. 7).

Numa comunidade, todos nós entendemos bem, podemos confiar no que ouvimos, estamos seguros a maior parte do tempo e raramente ficamos desconcertados ou somos surpreendidos. Nunca somos estranhos entre nós. Podemos discutir — mas são discussões amigáveis, pois todos estamos tentando tornar nosso bem-estar juntos ainda melhor e mais agradável do que até aqui e, embora levados pela mesma vontade de melhorar nossa vida em comum, podemos discordar sobre como fazê-lo. Mas nunca desejamos má sorte uns aos outros, e

podemos estar certos de que os outros à nossa volta nos querem bem. (BAUMAN, 2003, p. 8).

Também em Max Weber (1987, p. 77) pode-se encontrar uma conceituação de comunidade que permite vislumbrar algo similar:

> Chamamos de comunidade a uma relação social na medida em que a orientação da ação social, na média ou no tipo-ideal, baseia-se em um sentido de solidariedade: o resultado de ligações emocionais ou tradicionais dos participantes.

Essa ideia de Weber sobre comunidade está vinculada à de “estado” social guarda certa consonância com o pensamento de Bauman. A solidariedade é subjetivamente sentida pelos seus membros, enquanto a sociedade se limita ao prescrito pelas normas legais e pode, no máximo, entender-se como filantropia. A noção de sociedade está relacionada com a ideia de “humanidade civilizada e progressista” própria dos filósofos do iluminismo, enquanto o conceito de comunidade refere-se sobretudo à união orgânica e natural do homem à sua pátria.

Ao se referir a relações comunitárias, Weber as define como relações espontâneas, onde há graus de parentesco, e onde as pessoas têm a mesma religião, não se trata, portanto, de uma forma contratual entre as partes, todos são livres para seguir o que melhor lhes aprouver, onde há a observância de um sentimento subjetivo de pertencimento ao mesmo grupo, diferenciando-se das associações ou sociedades, que apresentam uma relação social apoiada em um acordo racional, havendo a deliberação de grupos, formação de associações de bairros, estatutos entre outros.

Chamamos sociedade a uma relação social quando a atitude na ação social inspira-se numa compensação de interesses por motivos racionais (de fins ou de valores) ou também numa união de interesse com idêntica motivação. A sociedade, de um modo típico, pode basear-se especialmente (mas não unicamente) em acordo ou pacto racional, por manifestação recíproca. Então a ação quando é racional, está orientada: a) racionalmente com relação a valores: em virtude da crença na própria vinculação; b) racionalmente com relação a fins: pela expectativa da lealdade da outra parte. (FERNANDES, 1920, p.140).

A comunidade, para Tönnies (1995a), desenvolveu-se a partir de três diferentes instâncias: o parentesco, a vizinhança e a amizade. A primeira emerge da vida familiar e fundamenta-se na autoridade dos membros da família – sendo essa autoridade

traduzida em termos de idade, força e sabedoria. A segunda emerge da vida em comum, do território partilhado. Nesse caso, as necessidades de trabalho e de uma organização comum promovem o compartilhamento dos hábitos, dos conhecimentos e a emergência das tradições. A terceira emerge da semelhança de interesses e formas de pensar. Ela nasce da similitude de atividades, mas deve ser alimentada por encontros frequentes, sendo mais comum nas aldeias e pequenas cidades. De maneira diferente, pode-se falar de comunidade de sangue, de lugar e de espírito e também notar que, mesmo nomeadas como sendo diferentes comunidades, são encontradas em conjunto e fortemente ligadas.

Assim, a vida comunitária se contrapõe à vida societária. Em uma, impera a homogeneidade, na outra, a heterogeneidade; em uma, encontram-se princípios gerais que orientam a ação do grupo, na outra, princípios relativos que orientam ações de membros individuais.

A comunidade só pode ter seus aspectos demarcados e delineados a partir de seu grande contraste com seu oposto moderno, a sociedade, pois, só a partir de então – do momento em que deixa de ser a única forma de relação social de grupo –ela passa a ganhar centralidade; e, só diante da conturbada vida metropolitana – que, mesmo possibilitando um aumento dos contatos sociais, levou a uma menor profundidade desses contatos –, a coerente vida comunitária passa a ser uma metáfora de tudo o que é social.

Bauman (2003), partindo de Tönnies e da ideia de que a comunidade necessita de um entendimento partilhado entre seus membros, busca superar os argumentos desenvolvidos pelo autor. Na sociedade moderna nascente, o entendimento não poderia mais ser partilhado, tendo sido substituído pelo consenso. No entanto, consenso não significa partilha, mas apenas negociação entre pessoas e interesses divergentes. O entendimento, diferentemente do consenso, não precisa ser procurado, está sempre disponível aos membros de uma comunidade. A transição da comunidade para a sociedade é também a transição do entendimento ao consenso.

Florestan Fernandes ao enunciar o posicionamento de F. Töonies, apresenta-nos a visão de comunidade como uma situação tácita, onde existem entre as partes laços de acordos tácitos e implícitos, no entanto ao tratar de sociedade nos remete a questão contratual, onde há uma troca estritamente racional segundo fins e livremente pactuada no mercado, havendo uma ação permanente orientada em seus propósitos e meios à persecução dos interesses objetivos dos membros partícipes deste acordo.

Tanto em Tönnies como em Weber, a ideia de comunidade aparece como uma tipologia. No caso de Tönnies, ele parte das comunidades para as associações modernas e, a partir disso, cria uma filosofia da história, e o desenvolvimento tem um rumo ao longo do tempo. Mas não se trata apenas disso. Tönnies converte o caso específico que lhe era disponível – a diferença histórica entre comunidade e sociedade – em uma classificação que busca dar conta da análise de qualquer sociedade do passado e do presente (Nisbet, 1967, p. 74). Da mesma forma, tanto para Tönnies quanto para Weber, a comunidade deve ser entendida como um tipo ideal, um construto intelectual útil para a análise de grupos sociais, mas que deve considerar que, na realidade, comunidade e sociedade se misturam.

Em Durkheim (1978b) também se encontra uma formulação da ideia de comunidade. Mesmo que muitas vezes não seja explícito, em seu conceito de solidariedade mecânica, encontram-se “ressonâncias” da vida comunitária das pequenas aldeias. Também a individualização ganha seu lugar, em decorrência da diferenciação dos indivíduos nas sociedades orientadas pela solidariedade orgânica. E, apesar de não fazer referência direta a Tönnies, e sendo suas conclusões sobre as diferentes formas de solidariedade ligeiramente diferentes das concepções de comunidade e sociedade, de um modo geral, encontram uma conceituação que permite entender as ideias de ambos os autores como referentes.

3.1 AS COMUNIDADES DE INTELIGÊNCIA

O termo *intelligentsia* ou *intelligentzia* (do russo интеллигенция, do latim *intelligentia*) refere-se, geralmente, a uma categoria ou grupo de pessoas envolvidas em trabalho intelectual complexo e criativo direcionado ao desenvolvimento e disseminação da cultura, abrangendo trabalhadores intelectuais, significa também “capacidade de entender”, ou aquele que compreende, percebe, conhece e sabe discernir sobre determinadas questões.

A princípio, a palavra tinha um sentido restrito, baseado na autodefinição de uma certa categoria de intelectuais. Posteriormente, passou a ser empregada para designar coisas diferentes: tanto o conjunto dos intelectuais de um dado país, como os grupos mais restritos de intelectuais que se fazem notar por sua capacidade de fornecer uma visão compreensiva do mundo, por sua criatividade ou por suas atividades direta ou indiretamente políticas.

Esta nomenclatura passou a fazer parte do cenário político brasileiro a partir da década de 1990, após a extinção do Serviço Nacional de Informações (SNI), emergindo no intuito de amenizar a imagem desgastada que se formou acerca das atividades de informações existente no regime militar, que se relacionavam a repressão e a violação dos direitos civis.

A Política Nacional de Inteligência (PNI), veio definir através do Decreto nº 8.793 de 29 de junho de 2016, os parâmetros e os limites de atuação da atividade de Inteligência e de seus executores, estabelecendo seus pressupostos, objetivos, instrumentos e diretrizes, no âmbito do Sistema Brasileiro de Inteligência (SISBIN), tendo sido fixada pelo Presidente da República, após exame e sugestões do competente órgão de controle externo da atividade de Inteligência, no âmbito do Congresso Nacional.

As comunidades de inteligência guardam uma relação direta com a Constituição Federal e sua finalidade de bem servir a sociedade e o Estado, desenvolvendo suas atividades em estrita obediência ao ordenamento jurídico brasileiro, e pautam-se pela fiel observância aos Princípios, Direitos e Garantias Fundamentais expressos na Constituição Federal, em prol do bem-comum e na defesa dos interesses da sociedade e do Estado Democrático de Direito.

Por ser a inteligência atividade exclusiva de Estado ela se constitui em um instrumento de assessoramento de mais alto nível de seus sucessivos governos, no que diz respeito aos interesses da sociedade brasileira, necessitando atender precipuamente ao Estado, não se colocando a serviço de grupos, ideologias e objetivos mutáveis e sujeitos às conjunturas político-partidárias.

As comunidades de inteligência exercem também atividades que objetivam produzir e difundir conhecimentos às autoridades competentes, relativos a fatos e situações que ocorram dentro e fora do território nacional, de imediata ou potencial influência sobre o processo decisório da ação governamental e da salvaguarda da sociedade e do Estado, constituindo-se em um dos ramos da atividade de inteligência que diz respeito ao exercício permanente de ações especializadas, voltadas para a produção e difusão de conhecimentos, com vistas ao assessoramento das autoridades governamentais nos respectivos níveis e áreas de atribuição, para o planejamento, a execução, o acompanhamento e a avaliação das políticas de Estado.

Hoje, a Política Nacional de Inteligência é considerada o documento de mais alto nível de orientação das atividades de Inteligência no País, tratando-se de um

discurso oficial que orienta o funcionamento a nível de governos dos órgãos que compõem a inteligência, tendo sido concebida em função dos valores e princípios fundamentais consagrados pela Constituição Federal, das obrigações decorrentes dos tratados, acordos e demais instrumentos internacionais de que o Brasil é parte, das condições de inserção internacional do País e de sua organização social, política e econômica.

A inteligência governamental é baseada em um conjunto particular de organizações que recebem nomes como serviços de inteligência ou comunidades de inteligência. A atividade de inteligência é o que eles fazem, e o conhecimento de inteligência é o que produzem. Pode-se então definir inteligência a partir de seu contexto organizacional.

Cumpre à Inteligência acompanhar e avaliar as conjunturas interna e externa, buscando identificar fatos ou situações que possam resultar em ameaças ou riscos aos interesses da sociedade e do Estado. O trabalho da Inteligência deve permitir que o Estado, de forma antecipada, mobilize os esforços necessários para fazer frente às adversidades futuras e para identificar oportunidades à ação governamental.

Exige-se das Comunidades de Inteligência o emprego de meios sigilosos, como forma de preservar sua ação, seus métodos e processos, seus profissionais e suas fontes, oportunidade em que desenvolvem essas ações com a finalidade de obtenção de dados indispensáveis ao processo decisório, indisponíveis para coleta ordinária em razão do acesso negado por seus detentores.

Na atividade de Inteligência, os valores éticos devem balizar tanto os limites de ação de seus profissionais quanto os de seus usuários. A adesão incondicional a essa premissa é o que a sociedade espera de seus dirigentes e servidores.

3.2 AS COMUNIDADES DE REDE

As tecnologias virtuais que concentram todo esse conhecimento seleto desenvolvido por poucos que dominam uma rede de conectores capazes de se fazer conhecido aquilo que jamais o foi, e de integrar o ocidente ao oriente em questão de milésimos de segundos, cada dia mais se capacitam e se especializam com o intuito de dominar e disseminar esse conhecimento entre as pessoas, responsáveis por essa interação virtual entre comunidades, deu origem a comunidades que se comunicam virtualmente, as comunidades em rede, ou de rede.

Uma comunidade virtual estabelece relações através de meios de comunicação à distância. Caracteriza-se pela aglutinação de um grupo de indivíduos com interesses comuns que trocam experiências e informações em ambiente virtual, e o que as caracteriza é justamente a dispersão geográfica de seus membros.

No entanto o uso de tecnologias da informação e da comunicação vêm minimizando esta dificuldade, que vimos relacionar-se ao tempo e espaço, ocasião em que promovem o compartilhamento de informações e a criação de todo um conhecimento coletivo, capaz de integrar um grupo ou vários grupos detentores de interesses comuns.

As redes estão abertas às novas participações e são alimentadas pela entrada e saída permanente de informações nas trocas com o ambiente externo e são renovadas internamente por emergências e conversações, observa-se que quem modela sua estrutura é o fluxo de informação na rede, e por isso ela é dinâmica, célere e instável.

As redes virtuais policêntricas possuem diversos centros de iniciativa, que derivam de ações autônomas de seus membros e estes não são fixos, nem permanentes. Estes centros funcionam como nós da rede, pontos de irradiação, de distribuição de informação, de conexões de redes dentro de redes e também como pontos de atração, onde as informações fluem pelo sistema indo e vindo sem que sofram interrupção, nem congestionamento.

Essas tecnologias dos sistemas de informação que permeiam todo o mundo globalizado, apesar de se apresentarem supostamente presentes no dia a dia do ser humano, tem também uma estratégia de alcance virtual assaz intrigante e que não se pode mensurar pelas facilidades que oferecem, e pelo perigos que apresentam, pois através desses sistemas virtuais, onde todos se conectam sem nenhuma restrição, sem preocupação iminente, há uma grande probabilidade de ser tornarem presas fáceis a uma invasão visceral de dados criptografados e a captação de informações pessoais disponibilizadas e de fácil acesso nas redes que hoje se encontram conectadas virtualmente, basta a quebra de uma senha, ou o acesso a informações simples, mas consideradas aos analistas de rede, fáceis de captação e extremamente privilegiadas.

A violação destes campos agravou-se mais ainda após os ataques do 11 de setembro de 2001, e do caso Snowden, ex técnico da CIA, que sentiu a obrigação em denunciar ao mundo, mesmo tendo que expor a um custo pessoal muito alto, os

poderes de vigilância acumulados pelo governo do Estados Unidos da América em relação a outros países. A partir de então, o que era tido como seguro, modificou seus paradigmas, ampliando as possibilidades de intrusão através de sistemas, e já não se ouve mais falar em segurança e nem privacidade, mas em exposição, invasão de informações e dados onde são violados direitos, particularidades e interesses de pessoas. Não há confidencialidade, a proteção de dados e a neutralização são temerárias, e a vigilância e a visibilidade são constantes.

Há uma desagregação de valores morais e virtuais onde uma sociedade que pensa estar segura, tem sua liberdade de expressão tolheda pelo fato de não poder mais se manifestar e nem expor sua opinião em quaisquer sistemas virtuais que se apresentem, correndo o risco iminente de ser invadida por *fishings*, podendo ser vigiada por vinte e quatro horas ininterruptamente, bastando acessar dados ou metadados pessoais, fazer uma ligação através de um celular ou acessar seu e-mail pessoal.

Os integrantes dessas comunidades de rede talvez podem até ser os supostos responsáveis por toda esta intrusão, pois detém o conhecimento e dominam a interface do sistema, sendo capazes de consultar qualquer tipo de oceano de matéria bruta constante neste sistema virtual, pesquisar e classificar o que vale ou não à pena para ser extraído. E se o que você tiver a oferecer for de seu interesse ou veiculação, tenha certeza que sua vida pessoal e particular será incessantemente investigada.

As comunidades de rede, através de uma combinação de privacidades e de seus credenciamentos diferenciados, têm acesso a quaisquer tipos de informações privilegiadas. Há uma verdadeira organização de monitoramento que administra esse fluxo de informações e revelações dispostas pelos seus interlocutores que se disponibilizam dessa rede sistêmica e virtual.

Todos os dias, e em todos os momentos, essas comunidades espionam milhares de e-mails e ligações de milhões de brasileiros em todo o mundo, capazes de introduzir *backdoors* que quebram os protocolos de criptografia e decodificam as informações que supostamente seriam inviáveis ao conhecimento de pessoas comuns.

Essa intrusão ocorre através de programas secretos do governo de monitoramento, que extraem áudios, vídeos, fotos, *e-mails*, documentos, registros de conexão, a partir do momento em que você se conecta aos servidores centrais da *Microsoft, Yahoo, Google, Facebook, Aol, Skype, Youtube, Apple*, e outros, e há

profissionais ou analistas responsáveis por esse rastreamento em relação as ações de uma pessoa quando se utiliza da rede, ou de várias pessoas, dentro do seu contexto de tempo. Os poderes dessas comunidades são amplos. Não há proteção e nem segurança.

Na sociedade de consumo de hoje, tudo é transformado em mercadoria e vendido. Isso inclui a informação. Mas a informação, só existe na mente das pessoas. Como não se possui a mente de outra pessoa, não podemos comercializar informações, a não ser que sejam livremente disponibilizadas.

Cada vez mais interagimos com o ambiente que nos cerca através da *internet*, de dispositivos digitais – como celulares, *tablets*, computadores, relógios – e, é claro, por meio das redes sociais, no entanto, muito antes da *internet*, as redes sociais já estavam presentes em nosso cotidiano.

3.2.1 O comportamento complexo dessas comunidades de rede

Redes de relacionamento virtual (*on-line*), que substituem as interações primárias, face a face, e ao mesmo tempo deslocam os critérios informais e lucrativos das organizações e instituições modernas. Este comportamento entre os sistemas de rede, nós e pontos se concentram ao longo de uma série de pontos lógicos e ilógicos, responsáveis pela interligação de conectividades que mudaram sobremaneira os rumos da humanidade. Conexões e comportamentos que mudaram o rumo normal da vida cotidiana. Se é que se pode chamar algo não estático e adepto constantemente a mudanças consideráveis de normal. Depende de quem detém a sua análise.

Comportamentos que fizeram toda a diferença com um único intuito, o de revelar aquilo que até então não havia sido revelado. Aquilo que o mundo virtual não pode controlar, que perpassa os limites da razão e transcende o inimaginável. O que nunca havia sido explorado pelas pessoas comuns, mas que através do conhecimento tecnológico, e por outras pessoas quase comuns, pode ser desenvolvido e especializado, em um nível que pudesse ser utilizado não apenas pelos analistas e especialistas em sua área, mas por todos que têm o mínimo de discernimento para desvendar o mundo virtual de redes e sistemas de informação.

A complexidade de comportamentos, necessariamente começa a aparecer não como inimigo a ser eliminado, mas como um desafio a ser enfatizado, permeando com certeza, uma noção ampla, mas leve, que guarda a incapacidade de determinar e autodefinir certos comportamentos. Eles se apresentam e aparentemente parecem o

que queremos ver e não o que realmente o são, e as vezes, nem o que pensamos ser se correlaciona a essa maneira de inter-relacionamento virtual.

Essa genialidade perceptível nas comunidades de rede é capaz de proceder mudanças tão substanciais a ponto de não mais se poder viver sem estar conectado, sem estar virtualmente participando do mundo que não o cerca, mas que o interliga a outros, que pode transformar sua singela segurança virtual em insegurança em uma questão de milésimos de segundos.

Reconhecer traços de comportamentos complexos nos levam a diversidade de ações, a uma completa desordem a nosso ver, mas que para algumas comunidades, como as comunidades de rede, significa uma ordem inversa capaz de alinhar os seus pensamentos e ações aleatórias.

Há leis e regramentos seguidos por essas comunidades que dizem respeito a sua concepção de respeito dentro da própria comunidade que constituem traços de sua estrutura organizacional virtual, transformando o pensamento complexo em comportamento complexo, pelo fato de suas ações não serem corriqueiras e nem tampouco previsíveis, mas invasivas ao ponto de desconstruir o que se teria como algo estruturado, se é que se existe alguma coisa nesse sentido nos dias atuais, analisando dentro do parâmetro da desconstrução.

Percebe-se que a complexidade do comportamento dos membros da comunidade de rede, em determinado momento já retratada nos conceitos de comunidade na visão de Tönnies acerca da instância da vizinhança, levam-nos a observar que essas comunidades de rede como na vizinhança têm uma vida em comum entre seus vizinhos no entorno de um território partilhado, onde cada um tem sua especialidade e domina uma área de interesse, onde acontece também o compartilhamento de hábitos desses membros como se uma família fosse, estando fortemente ligados, não por laços de amizade, mas por nós entre as redes de conexão.

Da mesma forma, o termo complexidade já não é mais perseguido na consciência científica. A ciência clássica dissolvia a complexidade aparente dos fenômenos para revelar a simplicidade oculta das imutáveis Leis da Natureza. Certamente que essa imutabilidade não mais se sustenta. Esses comportamentos complexos são culturalmente explicáveis diante de suas atividades na interface de qualquer sistema e que lhes propicia essa acessibilidade e mutação continuada.

O controle do sistema de rede por essa comunidade ocorre através de programas de descompressão que auxiliam o acesso supostamente inacessível, mas

utilizado para quebrar o sistema e o sigilo de dados ao infectarem a rede pelo "vírus da paranoia", sendo capazes de monitorar bilhões de telefones móveis e várias sessões de internet simultaneamente, inclusive monitorar sua *webcam*.

A magnitude de interferência e intrusão desses profissionais ou analistas pertencentes a essas comunidades de rede permite o acesso pessoal a milhões de registros de várias pessoas e em todo o mundo, indiscriminadamente, com um nível mínimo de suspeita pelos órgãos de segurança.

3.3 AS DIFERENÇAS ENTRE COMUNIDADES DE INTELIGÊNCIA E COMUNIDADES DE REDE

Os profissionais de inteligência e as agências possuem características que, em conjunto, formam um aspecto relevante para a atividade que é a cultura organizacional, a qual é compreendida como os distintos padrões de cultura e minicultura existentes dentro de uma organização. Cada agência de inteligência possui suas peculiaridades dependendo de seu ramo de atuação fazendo com que a cultura da inteligência não seja igual, mas que tenha alguns pontos em comum em quase todas as organizações de inteligência (HERMAN, 1996).

O ambiente em que ocorre a atividade de inteligência, cuja principal razão de existência é o processamento eficiente de informações complexas, tende a deixar os envolvidos mais vulneráveis a esses mecanismos cerebrais simplificadores devido às pressões contextuais, tais como a incerteza, ambiguidade, stress e rápidas mudanças de objetivos.

As comunidades de inteligência funcionam como um ente dentro de uma organização Institucional limitada a regras e que seguem toda uma hierarquia na cadeia de comando. Apesar do termo comunidades parecer algo onde se criam laços para a vida toda, onde se possa ter segurança para o seu bem-estar, necessariamente não se limita apenas a essas definições, alcançando uma delimitação bem maior, onde se pode adequar a um grupo de indivíduos que congregam os mesmos ideais e se alinham em obediência a uma hierarquia funcional, sob uma coordenação que segue algumas regras e conceituações para que possa atingir seus objetivos e resultados, onde regras são estabelecidas e objetivos são determinados para o alcance de resultados, visando sempre o bem comum e a segurança de seus entes.

Essa nomenclatura atribuída a essa "comunidade de inteligência" estaria atraindo para si uma restrição quanto à sua real constituição, pelo fato de se limitar ao que prescrevem as normas legais, fugindo a uma contextualização de predefinição que alguns autores fazem acerca de "comunidades" e "sociedades".

Esse termo "comunidade" de inteligência, a *contrario senso*, nos reporta a ideia de "sociedade", que especifica tratar-se de uma relação social que se apoia em um acordo racional, onde se visam objetivos a alcançar com determinados fins profissionais, lembrando que Tönnis nos remete em sua compreensão sobre "sociedade", usada também como critério formalizador para o atingimento de suas funções.

Pauta-se, ainda, a comunidade de inteligência, pela conduta ética, que pressupõe um conjunto de princípios orientadores do comportamento humano em sociedade. A sua observância é requisito fundamental aos profissionais de qualquer campo de atividade humana. No que concerne ao comportamento dos profissionais de Inteligência, representa o cuidado com a preservação dos valores que determinam a primazia da verdade, sem conotações relativas, da honra e da conduta pessoal ilibada, de forma clara e sem subterfúgios, analisando-se que esse comportamento se inclui como o que integra uma comunidade voltada aos interesses de uma organização, ou instituição.

Estes dois tipos de vontade explicam a existência de dois tipos fundamentais de grupos sociais ou de "sociedades". Um grupo pode existir e manter-se porque a simpatia entre os seus indivíduos os leva a sentir que essa relação é um "bem em si mesma", ou pode nascer como instrumento para conseguir alcançar um "fim determinado". Ao primeiro tipo de grupo, expressão da vontade essencial, Tönnies chama comunidade *(Gemeinschaft)*, e ao grupo que deriva da vontade arbitrária, sociedade *(Gesellschaft)*.

A comunidade como sendo uma forma social caracterizada por relações pessoais, intenso espírito emocional, e constituída pela cooperação, pelos costumes e pela religião, pode ser parcialmente aplicada as "comunidades de redes", onde se agrupam indivíduos que visam o bem comum de uma sociedade, interligam-se entre nós virtuais de conexões, e dispõe-se a fazer toda uma diferença sistêmica, sendo capazes de quebrar sigilos e fontes, com apenas uma finalidade, abrir um campo de informações a outras pessoas para que as mesmas possam se beneficiar de conhecimentos antes restritos e sigilosos apenas a alguns. Essa visão de comunidade

de rede veio desmistificar o que antes se pensava inimaginável, ou inexecutável aos olhos humanos, pois a mente e a informação não podem ser tolhedas a ponto de não serem transmitidas por um único clique na ponta de um nó do sistema, interligado a uma rede de conexão virtual.

O conceito de comunidade na rede social seria mais apropriado porque permite o alargamento geográfico dos laços sociais. Além disso, a metáfora da rede também é importantíssima porque enfatiza a estrutura da rede, que é onde será encontrada a comunidade virtual. Assim, o território da comunidade pode estar associado com algum espaço institucionalizado no próprio espaço virtual ou mesmo restrito a um elemento de identificação. Um canal de chat, por exemplo, pode constituir um espaço onde as interações são mantidas (RECUERO, 2002). O mesmo pode acontecer com um conjunto de *weblogs* (RECUERO, 2003). A compreensão de um espaço onde as interações podem ser travadas é, assim, fundamental para que os atores saibam onde interagir.

Entretanto, é preciso compreender que estudar redes sociais na Internet é estudar uma possível rede social que exista na vida concreta de um indivíduo, que apenas utiliza a comunicação mediada por computador para manter ou criar novos laços. Não se pode reduzir a interação unicamente ao ciberespaço, ou ao meio de interação.

A comunicação mediada por computador corresponde a uma forma prática e muito utilizada para estabelecer laços sociais, mas isso não quer dizer necessariamente que tais laços sejam unicamente mantidos no ciberespaço. A redução da interação ao ciberespaço, portanto, serve apenas para fins de estudo, já que se pressupõe que uma grande parte dela acontece principalmente através da mediação pelo computador. Garton, Haythornthwaite e Wellman (1997, p. 11) alertam para o mesmo problema, os autores salientam que “redes de computadores são apenas um método de manutenção de laços e as redes sociais não são restritas a um meio”. Por causa disso, os autores explicam que é fundamental observar em que medida há indícios de laços que são mantidos fora e dentro das redes de computadores, apesar da redução das interações à observação em um determinado recorte.

3.4 QUEM SÃO OS *HACKERS*

Os *hackers* não são o que a mídia diz que são. Não são uns irresponsáveis viciados em computador empenhados em quebrar códigos, penetrar em sistemas ilegalmente, ou criar o caos no tráfego de computadores. Os que se comportam assim são chamados "*crackers*", e em geral são rejeitados pela cultura *hacker*, embora ele pessoalmente considere que, em termos analíticos, os *crackers* e outros cibertipos são culturas de um universo *hacker* muito mais vasto e, via de regra, não destrutivos. (CASTELLS, 2003, p. 38).

Um *hacker* geralmente é um analista que detém o conhecimento da área de tecnologia da informação. De maneira geral, os *hackers* são pessoas que conseguem alterar programas, arquivos e até componentes de computador. A alteração pode incluir novas funções no programa ou aparelho ou pode ser uma mudança de uma função já existente.

Hackers são aqueles que a cultura *hacker* reconhece como tais. Quanto cultura *hacker*: ' Há uma cultura compartilhada, de peritos em programação e bruxos da interconexão cuja história remonta, através de décadas, aos primeiros microcomputadores de tempo compartilhado e aos primeiros experimentos da Arpanet. (RAYMOND, 1999, p. 231).

Para os *hackers* será que tudo tem que ser dito? Ou tudo necessariamente precisa ser divulgado? Não há infidelidade documental que os desafie frequentemente. Os códigos de acesso, as senhas e as confidencialidades, tudo isso se torna um desafio contínuo para os *hackers*.

Esse indivíduo com conhecimentos de informática extensa pode ou não violar o uso ou a segurança do desvio da internet. Ele quebra um sistema de computador ou rede com intenção maliciosa de realizar trabalhos de *hacking* malicioso ilegal ou não. Eles são *hackers* de segurança de computadores que invadem computadores e redes, ou também podem criar vírus de computadores.

A cultura *hacker* dominante vê os *crackers* com muita apreensão, uma vez que eles denigrem toda a comunidade com o estigma da irresponsabilidade, amplificado pela mídia. De uma perspectiva analítica, porém, devemos reconhecer a diversidade do mundo dos *hackers* enfatizando ao mesmo tempo o que une todos os seus membros acima de divisões ideológicas e comportamento pessoal: crença compartilhada no poder da interconexão de computadores e a determinação de manter esse poder tecnológico como um bem comum - pelo menos para a comunidade dos *hackers*. (CASTELLS, 2003, p.46).

Por outro lado, o termo *cracker* é utilizado com o sentido de indicar a pessoa que consegue quebrar um sistema de segurança. Ambas as palavras são utilizadas para pessoas que possuem grandes habilidades com computadores. No entanto, cada uma delas tem um sentido diferente, já que o *hacker* age de maneira diferente do *cracker* e vice-versa.

Em relação à postura, o grande diferencial é que o *hacker* não utiliza nenhum método para agir de forma ilegal, enquanto o *cracker* é o criminoso virtual, que pratica roubos e dissemina vírus na internet. Sendo assim, na grande maioria das vezes, chama-se de *hacker* o que deveria ser chamado de *cracker*.

Tratados coletivamente como "*Hackers*", este grupo é subdividido normalmente em duas categorias [Wilhelm, 2009]: *Black Hat Hackers* – indivíduos que executam ataques não autorizados contra sistemas de informação, motivados por ganho material ou financeiro, por mera curiosidade, ou ainda por questões políticas e religiosas. Seja qual for o motivo, entretanto, todos estão sujeitos a ações legais por parte daqueles que foram alvo de seus ataques; *White Hat Hackers* – indivíduos que executam avaliações de segurança com base em contratos formais, trabalhando em companhias responsáveis pela melhoria das características de segurança dos ambientes computacionais de seus clientes ou procurando vulnerabilidades que poderiam ser exploradas em ataques maliciosos.

A diferenciação de conceitos, porém, é questionada até mesmo dentro da área de tecnologia. Muitos especialistas afirmam que o melhor seria chamar os *hackers* e *crackers* conforme o que fazem, designando-os por *Black hat hacker* (chapéu preto), *White hat hacker* (chapéu branco) e *Gray hat hacker* (chapéu cinza).

O *White Hat hacker* tem por objetivo a segurança digital e costuma usar as suas habilidades somente para o bem, de forma totalmente ética. Embora muitas vezes eles comecem como hackers de chapéu preto, os hackers de chapéu branco, por vezes, são pagos como consultores ou funcionários regulares de uma empresa que precisa de seus sistemas protegidos.

Outros tipos de *hackers* incluem: *hackers* de chapéu azul e *hackers* de chapéu cinza. *Hackers* de chapéu azuis são profissionais de segurança que são convidados pela Microsoft para expor as vulnerabilidades nos produtos do Windows. E os *hackers* de chapéu cinza são hackers que realizam ambas as atividades maliciosas.

3.4.1 *Hacker* visto como "celebridade"

Para ser um *hacker,* é preciso mais do que gostar de computadores. Um verdadeiro invasor precisa ter um gosto especial pelos desafios. Quanto mais difícil se torna a entrada numa rede, maior é o seu prazer.

O *hacker* em geral é muito esperto e se destaca em várias áreas por motivos muito parecidos. Geralmente se sobressai porque domina os diversos recursos da informática, sendo tal domínio comum apenas aqueles que são mais dedicados, pacientes, aventureiros e curiosos.

Ainda que a acepção original do termo *hacker*[1] refira-se positivamente aos indivíduos habituados com a exploração quase inquisitiva de equipamentos e sistemas de informação (LEVY, 1984), não é absurdo afirmar que a mídia disseminou uma imagem idealizada do *hacker*: um indivíduo brilhante e autônomo, porém recluso e inescrupuloso, normalmente movido por razões pouco nobres. Mesmo na literatura acadêmica sobre o assunto, os autores parecem se dividir em torno do denuncismo ou da apologia aos *hackers*. Para alguns, os *hackers* possuem uma ética particular, comprometida com a liberdade de informação, meritocracia e desconfiança nas autoridades formais. Outros descrevem os *hackers* como jovens cuja fixação patológica pela internet os leva a buscas obsessivas por conhecimento, golpes complexos e verdadeiras competições em torno da violação de sistemas de computador (COLEMAN; GOLLUB, 2008).

De todo modo, convém salientar que as análises costumam referir-se aos *hackers* como membros de um grupo social, mais ou menos coeso, que partilha de um determinado padrão de interação, ética ou cultura.

Os *hackers* modernos que aderem à ética *hacker*, especialmente os mais ativos, são geralmente adeptos ao software livre e ao código aberto. Isso ocorre porque o software livre e o código aberto permitem aos *hackers* acessar o código-fonte usado para criar o software, permitindo que este seja melhorado ou reutilizado em outros projetos. O ponto chave da ética é o livre acesso a informações e melhoria da qualidade de vida.

Há na cultura *hacker* um sentimento comunitário, baseado na integração ativa a uma comunidade, que se estrutura em torno de costumes e princípios de

[1] O termo *hacking* – ou seja, a atividade dos hackers – muitas vezes é entendido como um conceito "guarda-chuva". Para alguns, engloba também as atividades dos ativistas de software livre e código aberto. Para outros, estende-se às atividades de ativismo pela liberdade de informação e ao terrorismo e vandalismo digital (*cracking)*. (RAYMOND, 2000; COLEMAN; GOLLUB, 2008).

organização social informal. As culturas não são feitas de valores nebulosos. São enraizadas em instituições e organizações. Há uma organização desse tipo na cultura hacker, mas ela é informal; isto é, não é imposta pelas instituições da sociedade. Na comunidade Linux, por exemplo, há "veteranos tribais" (a maioria com menos de 30 anos), sendo Linus Torvalds a autoridade suprema. Eles são proprietários/mantenedores de cada projeto; por exemplo, Linux possui e mantém o núcleo Linux, porque criou sua origem. (CASTELLS, 2003, p. 43).

Eles olham os computadores como se fossem a lâmpada de Aladim, que eles podem controlar. Eles acreditam que toda a sociedade pode se beneficiar ao experimentar esse poder, caso todos pudessem interagir com os computadores da forma como os eles o fazem, a ética hacker penetraria toda a sociedade e os computadores melhorariam o mundo, pois essa utilização do computador na sociedade dá abertura a um mundo ilimitado.

Observa-se que o sentimento que tem o *hacker* ao conseguir invadir sistemas que contenham informações pessoais de terceiros, e cuja veiculação o façam tornar-se conhecido sistematicamente, tanto nas redes quanto na mídia de uma forma geral, o deixam extremamente satisfeito e lhe enchem o ego por ter sido "descoberto" e se tornar uma celebridade, mais famosa que a pessoa cujas informações pessoais, fotos, *emails* ou outros foram divulgadas e expostas ao compartilhamento de todos.

Outros *hackers* reconhecem-se nos personagens "*cyberpunk*" da literatura de ficção científica. Fundam sua autonomia social na Internet, lutando para preservar sua liberdade contra a intrusão de quaisquer tipos de poderes, inclusive a tomada de controle de seus provedores de serviços de Internet pelas corporações da mídia. (CASTELLS, 2003, p.46).

Isso denota que não há receio e nem qualquer sentimento de medo quanto a esta divulgação de informações de terceiros pelos *hackers*, pois seu entendimento acerca do que deveria ser confidencial para alguns que se utilizam das redes sociais, em sua visão de padrões do que se veicula nas redes e em sistemas tem por melhora entre a sociedade, o compartilhamento.

Talvez isso não seja entendido pelas mentes humanas normais, mas esse comportamento complexo e diferenciado de um *hacker* tem feito a diferença, inclusive quanto a divulgações de supostos segredos que não poderiam jamais ser divulgados a sociedade, listados como confidenciais pelos governos dos países, e que alargaram

sobremaneira o campo visionário populacional, permitindo o conhecimento e a visão de forma ética e coerente acerca do mundo virtual.

3.4.2 Diversidade da cultura *hacker* no ambiente virtual

A internet é o alicerce organizacional da cultura *hacker*. A comunidade *hacker* em geral é global e virtual. Embora haja momentos de encontro físico, conferências e feiras, a maior parte da comunicação é eletrônica. Em geral os *hackers* só se conhecem pelo nome que usam na Internet. Não porque ocultem sua identidade. O que ocorre é que a identidade deles como *hackers* é o nome divulgado na Net. Embora o grau mais elevado de reconhecimento costume ser associado a identificação por nomes reais, via de regra informalidade e a virtualidade são essenciais da cultura *hacker* - características que diferenciam nitidamente da cultura acadêmica e de outras manifestações da cultura meritocrática. Por isso que os pesquisadores da ARPA, embora praticassem o *hacking* (programação criativa, de fonte aberta) tenham sido os criadores da Internet, não eram *hackers* no sentido cultural. (CASTELLS, 2003, p.44).

De toda forma, não se deve traçar um panorama idealizado de democratização ilimitada da informação. Primeiro, porque o acesso aos meios eletrônicos é desigual e abarca áreas das sociedades e das regiões do mundo, criando zonas de marginalização, com acesso tardio aos desenvolvimentos tecnológicos. E, mais importante, se por um lado a liberdade de comunicação e de expressão se alargou imensamente, num cenário em que as pessoas compõem seus próprios noticiários e programas de entretenimento a partir de múltiplas fontes, ordenadas em horários e frequências definidas por elas (e não mais ficam em frente à televisão à espera de ver o mundo pelo jornal das oito), por outro lado, os emissores das grandes redes de televisão e jornal estão cada vez mais concentrados, a partir de megafusões de redes de comunicação em vários países. Com a internet e a sociedade em rede, vivemos um momento paradoxal em que o público é segmentado, diferenciado e seletivo, não mais se apresentando como uma audiência maciça, simultânea e homogênea. Por outro lado, os emissores dos grandes canais de televisão, ao verem suas audiências despencarem, vêm procedendo a alianças estratégicas e fusões, e hoje são mais comerciais e oligopolistas do que em qualquer outro momento da história. Nesse contexto complexo, tudo indica, como o que caracteriza o novo sistema de comunicações é sua capacidade de incluir e abranger todas as expressões culturais [...]. Devido à sua diversificação, multimodalidade e versatilidade o novo sistema de

comunicação é capaz de abarcar e integrar todas as formas de expressão, inclusive a dos conflitos sociais, bem como a diversidade de interesses, valores e imaginações. (CASTELLS, 2001: p.491).

Um outro mito poderoso, muitas vezes propalado por ícones dos próprios *hackers*, é que a cooperação, a liberdade e a cultura do dom só podem ser desenvolver sob as condições do novo e imaterial sistema de produção que se cria numa sociedade da pós-escassez. Segundo essa visão, é somente quando têm suas necessidades básicas atendidas que as pessoas podem se dar ao luxo de dedicar suas vidas à criatividade intelectual, e só então podem praticar a cultura do dom. (CASTELLS, 2003, p.45).

Nas margens dessa subcultura *hacker* rebelde, emergem os *cracker*s. Em sua maioria, são indivíduos, com frequência muito jovens, que tentam provar sua perícia, em geral, com conhecimento técnico limitado. Outros, como Kevin Mitnik, misturam habilidade técnica com uma estratégia de sabotagem política em seus esforços para vigiar o mundo que os vigia. Esse comportamento deve ser diferenciado do cibercrime - a prática de roubos pela Internet para lucro pessoal-, o velho hábito do "crime do colarinho branco" executado mediante novos meios tecnológicos. Os crackers mais políticos constroem redes de cooperação e informação, com todas as devidas precauções, muitas vezes, difundindo o código de tecnologia de criptografia que permitiria a formação dessas redes fora do alcance das agências de vigilância. As linhas de batalha estão se deslocando do direito que têm as pessoas de codificar (contra o governo) para o direito que elas têm de decodificar (contra as corporações) (LEVY, 2001; PATRICE RIEMENS, comunicação pessoal, 2001).

O aspecto cultural no presente trabalho se justifica, pois apesar do rápido desenvolvimento de meios de tecnologia da informação, o aspecto cultural do profissional de inteligência interage com a cultura da agência e com os meios que ele precisa para exercer sua atividade. As características peculiares do profissional de inteligência e das agências especializadas formam o que se chama cultura organizacional, a qual possui uma importância muito grande para a integração da atividade de inteligência. (HERMAN, 1996, p. 327).

Muitos dos princípios e dogmas da ética *hacker* contribuem para um objetivo comum: as Práticas Imperativas. "*Hackers* acreditam que as lições essenciais podem ser aprendidas sobre os sistemas —sobre o mundo— separando as coisas, vendo

como elas funcionam, e usar esse conhecimento para criar coisas novas e mais interessantes." (LEVY, 1984, p.32).

Empregar as Práticas Imperativas requer livre acesso, informação aberta e partilha de conhecimento. Para um verdadeiro *hacker*, se as Práticas Imperativas são restritas, então os fins justificam os meios para fazê-lo sem restrições para que as melhorias possam ser feitas. Quando esses princípios não estão presentes, os *hackers* tendem a contorná-los.

Por exemplo, quando os computadores do MIT[2] foram protegidos por travas físicas ou programas de *login*, os *hackers* trabalharam sistematicamente em torno deles, a fim de ter acesso às máquinas. Os *hackers* assumiram uma "cegueira intencional" em busca da perfeição. Este comportamento não era de natureza maliciosa: os *hackers* do MIT não procuraram prejudicar os sistemas nem seus usuários (embora brincadeiras ocasionais foram feitas utilizando sistemas de computador). Isto contrasta profundamente com o moderno, a mídia incentivou a imagem do *hacker* que quebra sistemas de segurança, a fim de roubar informações ou completar um ato de vandalismo cibernético. O acesso a computadores - e qualquer outro meio que seja capaz de ensinar algo sobre como o mundo funciona - deve ser ilimitado e total. Toda a informação deve ser livre.

Esse preceito sempre se refere ao imperativo "mão na massa". Isto é, se um *hacker* precisa enviar várias mensagens para celulares sem pagar, ao invés de entrar várias vezes na interface web e enviar uma mensagem por vez, ele descobrirá como a *interface web* funciona e fará um programa automático para o envio de mensagens de forma mais ágil e com menos desperdício de tempo.

O *hacker* busca a informação diariamente e tem prazer em passá-la para quem quer "pensar" e "criar" coisas novas. Um *hacker* não aceita os famosos argumentos de autoridade e não acredita na centralização como forma ideal de coordenar esforços.

---

[2] MIT-*Massachusetts Institute of Technology.*

4 O MEIO AMBIENTE VIRTUAL

Podemos entender a internet como uma rede de computadores interconectados, em que se utilizam de milhares de redes menores, em que se comunicam entre si através de protocolos comuns, por sistemas de comunicação. E diante dessa concepção virtual desconhecer os limites de território, não há que se falar em território de forma ficta, e passamos a entender e falar em território no ciberespaço, ou seja, um território que não se visualiza, mas existe no meio ambiente virtual.

A *internet,* por sua vez, foi criada durante a Guerra Fria, no decorrer da década de 60. O experimento financiado pelo Departamento de Defesa dos Estados Unidos e desenvolvido pela *Advanced Research Projects Agency* (ARPA), através de um de seus departamentos, o *Information Processing Techniques Office* (IPTO), resultou na primeira forma de comunicação eletrônica entre computadores. Denominada ARPANET, a tecnologia interligou primeiramente os centros universitários da Universidade da Califórnia, em Santa Bárbara, e da Universidade de Utah, possibilitando a comunicação *on-line*. (FIORILLO, 2013, p. 12).

Observa-se, desde então, a preocupação em se criar um território virtual que necessariamente funcionasse me um meio ambiente virtual até então não muito conhecido e dominado pelos profissionais da área.

O legislador constituinte definiu o meio ambiente de maneira genérica, recepcionando o conceito da Política Nacional do Meio Ambiente nos seguintes termos: “Todos têm direito ao meio ambiente ecologicamente equilibrado, bem de uso comum do povo e essencial a sadia qualidade de vida, impondo-se ao Poder Público e a coletividade o dever de defendê-lo e preservá-lo para as presentes e futuras gerações” (Art. 225, *caput*, CF).

> Art. 225. Todos têm direito ao meio ambiente ecologicamente equilibrado, bem de uso comum do povo e essencial à sadia qualidade de vida, impondo-se ao Poder Público e à coletividade o dever de defendê-lo e preservá-lo para as presentes e futuras gerações.

Segundo Paulo Peixoto, o conceito legal não deve ser interpretado de forma literal, e sim sistemática, para que esteja em consonância com o artigo 225 da CF/88, visto que o direito ambiental possui uma necessária visão antropocêntrica.

Assim, a proteção da vida em todas as suas formas se dá na medida em que garante a sadia qualidade de vida do homem, destinatário da lei e do direito ambiental. “A proteção do meio ambiente visa favorecer o próprio homem e, de forma oblíqua, as demais espécies”, não importando se essa proteção de se no campo físico, propriamente dito, ou se ocorra no campo, ou mundo virtual.

Ao nos referirmos ao meio ambiente virtual, interligado por meio de fios e conexões lógicas que se decodificam sem que se possa tocar, verificamos uma complexidade quanto a aplicação das normas existentes em sede de Constituição, como quando da aplicação de leis ordinárias que tentam disciplinar um campo multipolar e em rede, visto que sua amplitude vai muito além do território usual propriamente conhecido, ou território ficto, atingindo um território conhecido como virtual ou ciberespaço.

Com o advento da Internet, e com ele, do ciberespaço, a concepção clássica do território transfigurou-se, posto que esta possibilitou o tráfego rápido e eficiente de informações, bem como uma interação num espaço que desconhece os limites impostos por fronteiras. Não existe separação de lugar na rede. A noção de lugar passa a ser qualquer ponto da rede em que se possa ter acesso a informação. (FIORILLO, 2013, p. 161).

Verifica-se, que a informação se torna dinâmica e volátil, diante da rapidez que chega e atinge os mais variados pontos, das mais variadas formas, através de várias pessoas de culturas diferentes, e o meio ambiente virtual, passa a ser visto como algo que se necessitava disciplinar para que se pudesse resguardar direitos e obrigações atinentes ao seu alcance e responsabilidade.

E como conter um nível de informação tão desenfreada, onde o conhecimento por intermédio de dados se faz ilimitado diante de um clique em um computador ou *notebook*, diante de uma mensagem através do *Facebook* ou *Whatsapp.*

Não há mais barreiras de comunicação entre as pessoas, e que são prontamente resolvidas através do *Google* tradutor, para aqueles que ainda têm dificuldade em se comunicar em outro idioma. Mas porque se falar em idiomas ou dificuldade de comunicação, se a linguagem é universal quando da conexão em ambiente virtual.

No Brasil, a utilização da Internet ocorreu inicialmente no meio acadêmico, especificamente na Universidade de São Paulo. No ano de 1988. Oscar Sala, professor da USP, desenvolveu um projeto de interação entre universidades, em

âmbito internacional, para que houvesse a troca de informação por meio de uma rede de computadores. Contudo, a autorização da disseminação da Internet para a população, autorizando-se o uso comercial da rede, só foi dado pelos Ministérios das comunicações e da Ciência e Tecnologia sete anos depois. A incidência direta da Internet nas relações humanas exige a tutela jurisdicional para as informações veiculadas na rede, bem como para as mais diversas relações jurídicas realizadas por meio virtual, mas dotadas de todos os riscos e garantias das relações firmadas no "mundo real". (FIORILLO, 2013, p. 14).

No século XXI, o avanço das denominadas redes sociais (*Facebook e Twitter*, por exemplo) bem como o serviço de sites de compras coletivas destinados a fazer a intermediação entre consumidores e empresas indica a enorme modificação cultural por que passou e continua passando o Brasil e todo o planeta em face dos modos de se expressar, criar, fazer e viver (art. 216 da CF). (FIORILLO, 2013, p. 16).

Portanto, observa-se que tal veículo de informação, fundamentado constitucionalmente, reveste-se de tutela jurídica do meio ambiente cultural, pela necessidade de manifestação, por meio da internet, do pensamento, da criação, expressão e informação, e dentro da atualização midiática crescente, onde sofre impactos da cultura da convergência, mais conhecida como meio ambiente digital ou virtual.

Em 2014, a lei nº 12.965 de 23 de abril, estabeleceu direitos e deveres para o uso da internet no Brasil, em seu artigo 5º e incisos, conforme transcrito *ipsis litteris:*

> Art. 5º Para os efeitos desta Lei, considera-se:
>
> I - internet, o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes.
>
> II - terminal: o computador ou qualquer dispositivo que se conecte à internet;
>
> III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
>
> IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;
>
> V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

> VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
>
> VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
>
> VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço Ip.

Dessa maneira, mais assemelhado a uma peça publicitária, o denominado Marco Civil da Internet (Lei 12.965/2014), ao pretender estabelecer princípios, garantias, direitos e deveres vinculados à manifestação do pensamento, à criação, a expressão e à informação (meio ambiente cultural), por meio do uso da internet no Brasil (meio ambiente digital), procura de qualquer forma tentar organizar parâmetros jurídicos específicos no âmbito infraconstitucional destinados a tutelar o conteúdo da comunicação social e mesmo dos deveres fundamentais da pessoa humana por meio do uso de computadores no Brasil em redes interligadas visando, ao que tudo indica, destacar a importância da tutela jurídica da internet no século XXI em nosso país.(FIORILLO, 2015, p.17).

4.1 A VIOLAÇÃO DA SEGURANÇA NA INTERNET

Nos primeiros dias da internet, os libertários proclamaram que a "informação quer ser livre" e retrataram a internet como o fim dos controles do governo e a "morte da distância". Na prática, os governos e as jurisdições geográficas continuam a desempenhar um papel importante, mas o domínio é também marcado pela difusão do poder. (NYE JR, 2003, p. 162).

A área da informática foi a que mais evoluiu nos últimos anos exigindo do campo do direito o devido acompanhamento das mudanças ocorridas na sociedade, especialmente em relação à prática de novos ilícitos fisionomicamente alterados pela sofisticação tecnológica.

Em decorrência deste avanço, e por consequência da Internet das Coisas (IoT) os riscos de segurança foram demasiadamente ampliados, tornando a neutralidade da rede em sistemas cada vez mais complexo, pelo fato do poder de computação embarcado que apresentam novos desafios a integridade, confidencialidade e controle de dados dos sistemas de informação.

A elasticidade da internet a torna particularmente suscetível a intensificar as tendências contraditórias presentes em nosso mundo, uma vez que a volatilidade, a insegurança, a desigualdade e a exclusão social andam de mãos dadas com a criatividade, a inovação, a produtividade e a criação de riqueza nesses primeiros passos do mundo baseado na Internet.

A Internet é uma expressão de nós mesmos por intermédio de um código de comunicação específico, que necessitamos compreender e entender se quisermos mudar nossa realidade. Esse conceito de segurança nos permite estar mais atentos e conectados ao mundo virtual para que a confidencialidade de informações possa estar guardada e protegidas por códigos criptografados e softwares específicos, capazes de proteger e neutralizar quaisquer tipos de ciberataques, que podem violar a segurança da *internet*.

Alguns princípios devem ser observados quanto a disciplina do uso da internet no Brasil, como a preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas e a responsabilização dos agentes de acordo com suas atividades, nos termos da lei, diante de riscos contínuos quanto ao uso de algoritmos com a finalidade de automatizar processos que visam coletar, armazenar e manipular dados de pessoas e organizações, e serviços de e-governo.

O Estado de Direito é responsável pela preservação da ordem pública e da incolumidade das pessoas e do patrimônio. No exercício dos seus poderes, compete-lhe investir nos órgãos de segurança, dotando-os de armamento moderno e de máquinas e aparelhos de alta tecnologia, para investigação. Por outro lado, deve assegurar ao seu pessoal condições sociais condignas e treiná-los devidamente para o exercício das funções. (ROCHA, 2003, p.40).

A responsabilidade funcional em manter a ordem pública faz com que ser policial não seja apenas um ofício, e sim uma causa. Percebe-se que, para a maioria das pessoas, a distância dos riscos e dos perigos é uma necessidade. Já para os policiais isso é uma profissão, e por ser uma profissão, precisa acompanhar as mudanças contínuas que vem ocorrendo em relação a diversos comportamentos criminais, inclusive aos cometidos quando da utilização e quebra de sigilo das redes virtuais, para que o serviço de investigação e a colheita de informações, feitos de forma sigilosa, possam ser obtidos com qualidade mediante pesquisas em sistemas informatizados de levantamento e acesso a banco de dados.

No segmento da segurança pública tais comportamentos não poderiam se diferenciar, mas extrapolar as conectividades que, por falta de recursos e de uma séria aplicação de política públicas não conseguem acompanhar a evolução tecnológica necessária e primordial para tolher as invasões contínuas ao sistema de segurança e de certa forma diminuir ou equalizar o número de ocorrências de *cibercrimes* registrados no sistema e que figuram nas estatísticas policiais.

Os criminosos que se utilizam da Internet para o cometimento de crimes virtuais, se beneficiam de um vasto campo de propagandas comerciais indesejadas, que praticamente são enviadas e recebidas diuturnamente por todos os usuários da rede, ocasião em que são introduzidas mensagens contendo anexos contaminados ou links para páginas maliciosas.

Os usuários mais leigos, tem dificuldade em diferenciar o que de fato é propaganda comercial e o que faz parte de mensagens maliciosas, oportunidade em que se tornam fáceis presas para os criminosos, sendo disponibilizadas na caixa de entrada de seus e-mails, sem que tenham sido classificadas como *spams.*

Esses atacantes (criminosos) enviam suas mensagens maliciosas, e tentam disfarçá-las como mensagens comerciais comuns (*spams*), simulando ser mensagens originadas por instituições conhecidas, tais como órgãos do governo, bancos ou empresas comerciais conhecidas, para milhões de usuários da Internet, sabendo que estatisticamente, uma pequena parcela dos usuários que receberem as mensagens vão acessá-las indiscriminadamente sem saber o risco que correm.

O *phishingscam* é um procedimento realizado por esses criminosos virtuais que analisam a "engenharia social" destas vítimas, utilizando-se de uma técnica utilizada para levantar informações de qualquer pessoa desconhecida, realizando os mais variados tipos de fraudes, obtendo dados valiosos tais como informações pessoais e senhas bancárias.

Essas mensagens lançadas como iscas no meio virtual, sempre contêm algo chamativo como notícias e boatos de grande audiência da moda, promessas de grandes lucros, fotos de celebridades, avisos de dívidas, multas, apelos sexuais, entre outros, onde não há limite para a criatividade desses criminosos virtuais.

No momento em que o usuário acessa essa mensagem enviada pelo criminoso virtual, ela infecta o sistema através de um *malware*, e se instala por meio de ações da vítima que pressupõe estar recebendo um “presente” e aceita fazer algumas ações

tais como abrir anexos contaminados ou clicar em links que levam à infecção e captura de informações de seu sistema.

Allor acredita que a indústria da segurança cibernética trava uma luta de proporções apocalípticas contra o mal. " é uma corrida armamentista. Para mim, é um caso de espada contra escudo. No submundo, eles têm uma espada cada vez mais afiada - os codificadores mal-intencionados-, e você precisa pesquisar todos para ter um escudo capaz de impedir todos os golpes daquela espada. Quando você consegue detectar algo que não está funcionando corretamente, uma vulnerabilidade em seu sistema, sabe que está diante de um grande problema - se você descobriu uma vulnerabilidade, pode apostar que o submundo também vai descobrir, se é que já não o fez. Hoje em dia, o submundo leva 48 horas para detectar uma vulnerabilidade. Quanto tempo leva até que uma empresa a detecte e produza uma atualização capaz de corrigi-la? As mais rápidas fazem isso em trinta dias. A maioria leva de trinta a sessenta dias. E o usuário doméstico? Será que chega a se dar conta disso? (GLENNY, 2008. p. 320).

Atualmente, grande parte das pessoas depende de seus dispositivos informáticos (computadores, discos externos, *smartphones*, celulares comuns, *tablets*, *pendrives e outros*), onde são armazenados dados e informações pessoais (contas e senhas bancárias, fotos, vídeos, arquivos de áudio, correspondências em geral) que estão cada vez mais sujeitos a violações criminosas.

Como o roubo tornou-se o objetivo principal dos programas mal-intencionados, o usuário comum de computador tornou-se mais vulnerável do que era antes. " O único computador seguro é o que está desligado", me assegura Kau, um brasileiro descendente de lituanos especialista em testar segurança, o que está passando no cinema, mas se usar a rede para qualquer outra coisa, é só uma questão de tempo até que o seu computador seja infectado - mesmo que você atualize o seu antivírus regularmente.(GLENNY, 2008. p. 322).

Na colocação acima podemos observar que o exemplo contextualizado como "roubo" conforme destacado, criminalmente, trata-se de um "furto de dados virtual" feito através de um software mal-intencionado que capta senhas do usuário, quebra o sigilo de dados e furta as informações que lhe interessam.

As possibilidades de cometimento de crimes virtuais são tremendas, e em sua grande maioria cometidas por pessoas que detém o conhecimento técnico de manipulação de redes e quebra de sigilos em programas, inclusive bancários, que

chegam a desviar quantidades em dinheiros de contas de clientes, apresentando a mente brilhante para a decodificação de sistemas e para o cometimento de crimes.

Para o cliente, o *internet banking* é tentadoramente confortável. Para os bancos representa uma economia monumental, porque derrubou seus custos com a mão-de-obra. Para os dedos-leves, é uma fonte de renda irresistível. E, para a polícia, é um enorme desafio. Basicamente, a internet não pode ser policiada sem ajuda substancial do setor privado - e, mesmo assim, como destaca um integrante da Divisão de Repressão a Crimes Cibernéticos em Brasília, " estamos sempre atrasados correndo atrás dessa gente. Eles conseguem burlar novas atualizações de segurança horas depois que elas são instaladas em uma rede". (GLENNY, 2008. p. 320).

Manuel Castells, enfatiza que a periferia do mundo industrial subdesenvolvido sofre estes efeitos dos fluxos e da atualização hegemônica do ciclo sistêmico que a articula aos blocos capitalistas. Pergunta-se então, como pode uma economia emergente, que se evidencia num ciclo completamente diferente do normal, criar a desterritorialização constante de pessoas e bens, tanto de serviços quanto de capital e continuar a implementar e aplicar o capital econômico em algo estático, cujo processo de crescimento certamente não acompanharia o desenvolvimento dessas comunidades de rede policêntricas.

A confidencialidade, a integridade e a disponibilidade formam uma tríade da segurança da informação clássica, conhecida mundialmente como *CIA* (*confidentiality, integrity and availability*).

4.2 CONECTIVIDADE E CONTROLE DO RISCO VIRTUAL

Para Latour (2000), as conexões estabelecidas entre os atores de uma rede, as negociações que, dessa forma, têm lugar e a própria comunicação se dão lugar a lógica da "Tradução". Traduzir é fazer conexão, é se ligar a. Se há comunicação há tradução. A tradução supõe também percepção, interpretação e apropriação, de forma que estão envolvidas nessa dinâmica tanto a " possibilidade de equivalência", quanto a "transformação" (Law, 1992). Através desse conceito, o que os autores querem afirmar são exatamente as transformações que se dão nos enunciados e tudo mais que circula na rede. Os atores se conectam pela tradução, permitindo-nos, afirmar que eles próprios traduzem a sis mesmos e aos demais e, ao mesmo tempo, são traduzidos. (CASTRO, p.38).

Em uma comunidade virtual, cada um de seus membros torna-se emissor e receptor de conhecimentos, crítico de informações compartilhadas, disseminador de experiências, professor e aluno, ou seja, seus membros são tradutores de sua história e conhecimentos cibernéticos. A internet é um meio de comunicação e conhecimento. No entanto, ao utilizarmos este meio ficamos bastante expostos, por ser um campo bem frágil e ao mesmo tempo bem ágil, no momento em que se permite o acesso de outros usuários concomitantemente.

Ao se conectar à internet, e acessar os mais diversos sites, o usuário acaba disponibilizando informações pessoais a esses sites, fato este que gera uma certa insegurança jurídica pela possibilidade deste usuário vir a ser vítima de crimes cometidos pela utilização dos seus dados pessoais, ocasião em que sofre uma violação de direitos e privacidade.

Atualmente, a internet tem sido utilizada para inúmeras finalidades, seja para realizar negociações comerciais, buscar conhecimento, conhecer pessoas, manter relacionamentos, produzir atividades de marketing pessoal, buscar diversão e, em alguns casos, promover transtornos para outras pessoas, incluindo prejuízos financeiros das vítimas.

Essa utilização tem sofrido um aumento exponencial a cada ano que passa, muito em virtude da evolução tecnológica e do barateamento dos computadores e dispositivos móveis de acesso à rede mundial, o que facilita os milhões de acessos por segundo pelo mundo inteiro. Uma comunicação conectada e ao mesmo tempo descentralizada em razão da distância das redes lógicas, ligadas apenas por conexões virtuais em pontos distintos e onde informações se cruzam em milésimos de segundos.

O poder cibernético pode ser definido como um conjunto de recursos que se relacionam à criação, ao controle e à comunicação de informações eletrônicas e baseadas em computador -- infraestrutura, redes, *softwares,* habilidades humanas. Isso inclui não somente a internet dos computadores ligados à rede, mas também intranets, tecnologias de telefonia celular e comunicações via satélite. Definido do ponto de vista comportamental, o poder cibernético é a capacidade para obter resultados preferidos mediante o uso dos recursos de informação eletronicamente conectados do domínio cibernético. O poder cibernético pode ser usado para produzir resultados preferidos *dentro* do espaço cibernético, ou pode usar instrumentos

cibernéticos para produzir resultados preferidos em outros domínios *fora* do espaço cibernético. (NYE JR, p.163).

Pelo fato do homem contemporâneo ter se tornado cada vez mais consciente de seus direitos, e, de reivindicar a capacidade de agir segundo a própria convicção e com liberdade responsável, não forçado por coação, mas levado pela consciência do dever, e que começa a exigir também que o poder público seja juridicamente delimitado, para que a liberdade das pessoas não seja restringida indevidamente.

Conforme preceitua a Lei nº 12.965 de 23 de abril de 2014, foram estabelecidos princípios que instruem acerca do uso da internet no Brasil, conforme disciplina o art. 3°, e seus incisos, transcrito *ipsis litteris*:

> Art. 3 °. A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II - proteção da privacidade;
>
> III - proteção dos dados pessoais, na forma da lei;
>
> IV - preservação e garantia da neutralidade de rede;
>
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

A gestão do risco de segurança da informação, de acordo com a ISO/IEC de 2007 é um processo sistemático, adotado na gestão da segurança da informação, que realiza a identificação dos eventos potencialmente negativos para a segurança de uma organização, chamados de riscos de segurança, e em seguida formula um ou mais planos que permitam o tratamento destes riscos de forma custo-efetiva, por meio da adoção de controles e outras ações gerenciais.

A análise e avaliação de riscos é uma atividade do processo de gestão de riscos em que são identificados os riscos e seus componentes ativos, as ameaças, as vulnerabilidades e consequências.

A probabilidade de ocorrência do cenário de risco e suas consequências são avaliadas, resultando em um nível de risco. Esse risco é então avaliado segundo critérios pré-definidos que determinarão a sua importância para a organização.

A ideia da sociedade de risco segundo Renato Nunes Bittencourt:

> Se por um lado a tecnologia dá aos usuários ampla liberdade e máxima igualdade individual, por outro lado ela lhes retira a habilidade de distinguir as

> pessoas com as quais se relacionavam virtualmente, além de lhes restringir a capacidade de diferenciar a sensação de segurança da ideia de segurança como realidade. (BITTENCOURT, 2010, p. 60).

No mesmo passo que a evolução dos recursos tecnológicos, as ameaças praticadas via computador se aprimoram com o passar dos anos. Com a popularização de dispositivos utilizados para o acesso à internet, também surgiram novos meios para a difusão de ameaças.

Atualmente a questão da segurança dos usuários no ambiente virtual é um problema sério, e as maiores vítimas são as crianças e adolescentes, pois, no momento em que utilizam a internet não conhecem os perigos a que estão sendo expostas.

Os riscos individuais são reais e as redes tradicionais e a segurança de computadores não estão preparadas para lidar com esses riscos, cujos dados uma vez expostos podem ser furtados (quebra de confidencialidade), modificados (quebra de integralidade) e bloqueados, impedindo a sua utilização (quebra de disponibilidade);

4.3 A IMPORTÂNCIA DO SIGILO E DO SEGREDO DAS INFORMAÇÕES.

Para elucidar um caso misterioso ou para descobrir alguma coisa, o primeiro movimento de um serviço de investigação é obter informações. Esse trabalho de pesquisa deve ser feito de forma sigilosa. O agente não pode revelar sua identidade, só o fazendo quando for necessário. Deve agir com discrição, evitando que sua missão seja percebida ou conhecida, quando penetra ou se infiltra em determinados lugares, na abordagem de pessoas ou em conversas, mesmo com seus familiares. (ROCHA, 2003, p.39).

No entanto, a cada dia que passa o ser humano contemporâneo se encontra mais refém do acesso fácil à informação, principalmente no que diz respeito à veiculada no âmbito virtual. Em razão das tantas mutações sistêmicas é salutar que também possa estar seguro, de certa forma, para que possa acompanhar essas mudanças sem que passe ou sofra interferências e intrusões desnecessárias em sua maneira de informar-se e expressar-se.

O direito à informação é previsto constitucionalmente no artigo 5º, inciso XIV da Constituição da República, sendo definido por Pedro Lenza, na obra Direito

Constitucional Esquematizado, como sendo "assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional. Trata-se do direito de informar e de ser informado".

Infelizmente, o legislador pátrio, tecnologicamente, não consegue evoluir e criar dispositivos com a mesma celeridade dos acontecimentos ocorridos na sociedade em suas transformações, decerto, acaba pecando em relação à celeridade em que oferece o devido amparo legislativo.

As autoridades administrativas que detém competência legal para a requisição dessas informações, devem atender as medidas e procedimentos de sigilo e segurança, sendo informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos governamentais.

A lógica cultural da modernidade tardia, marcada pela insegurança, repõe a questão da alteridade cultural, pois o culto da liberdade individual e o desdobramento da personalidade passam ao centro das preocupações. Rompe-se a consciência coletiva da integração social. Vivemos uma situação de incerteza fabricada, na qual há uma pressão contínua para desmantelar as garantias socialmente construídas. Trata-se de uma ruptura do contrato social e dos laços sociais, provocando fenômenos de desfiliação e de ruptura nas relações de alteridade, dilacerando o vínculo entre o eu e o outro (CASTELLS, 1998; BAUMAN, 1998).

As mídias locativas ameaçam a vida privada e o anonimato, vigiando controlando e monitorando praticamente tudo que nos cerca. A privacidade pode ser definida como o controle e a posse de informações pessoais, bem como o uso que se faz posteriormente delas. Anonimato, por sua vez, implica a ausência de informação sobre um indivíduo e também o controle sobre a coleta de informações pessoais (GOW, 2005).

A privacidade é um pilar das sociedades democráticas já que:

> empodera as pessoas para controlar as informações sobre si mesmas, protege as pessoas contra problemas indesejados, ou o direito de ser deixado em paz; (...) relaciona-se à dignidade nas obrigações recíprocas de revelações entre partes; (...) e é também um agente regulador podendo ser usado para equilibrar e fiscalizar o poder daqueles capazes de coletar dados (LESSING; GOW, 2005, p.7).

O "*Secure the Internet*" cita que a criptografia, o anonimato e os conceitos de segurança a ele relacionados, oferecem a privacidade e segurança necessárias para o exercício do direito de liberdade de opinião e de expressão na era digital, acordo o Relator Especial das Nações Unidas para a Liberdade de Expressão.

A soberania tecnológica promove, por sua vez, o direito de acesso e controle dos recursos e inclui a dimensão social da promoção da autonomia e da cooperação. A invasão da privacidade dos internautas é uma realidade que precisa ser pensada do ponto de vista jurídico, no sentido de coibi-la. As empresas administradoras de sites e redes sociais devem assumir sua responsabilidade pela guarda e segurança dos dados fornecidos por seus usuários.

A questão da privacidade está ligada diretamente a segurança jurídica e a liberdade do usuário, e esse domínio corresponde à esfera secreta, ocasião em que o indivíduo tem o direito de ser deixado tranquilo, sendo-lhe assegurado o direito à indenização por dano moral ou material decorrente de sua violação.

A regulamentação que vem disciplinar um padrão de segurança adequado, no sentido de primar pelo equilíbrio das relações virtuais quanto ao grau de proteção, veio efetivar esse direito dos usuários através do Marco Civil da Internet.

A preservação da intimidade, da vida privada e da imagem das partes envolvidas foi disciplinada no art. 10 da Lei 12. 965 de 2014, na Seção II que trata da proteção aos registros, dados pessoais e comunicações privadas.

Quem ficar responsável como provedor pela guarda desses registros será obrigado, mediante ordem judicial, a disponibilizá-los de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, respeitado o disposto nos incisos II e III do art. 7º do mesmo diploma legal.

A lei do Marco Civil da internet em seu artigo 10 trata da questão da privacidade, ao estabelecer que os dados pessoais, as informações de acesso e os registros do usuário devem preservar a intimidade e a vida privada do usuário, não admitindo, portanto, a divulgação de dados pessoais de usuários, preservando-se dessa forma a privacidade do usuário e a manutenção pela segurança jurídica da internet como um todo.

As políticas de segurança e privacidade de um serviço devem ser de fácil compreensão. É necessário explicar quais dados são coletados dos usuários, por que

são necessários, como serão usados, quando serão deletados e se serão repassados a terceiros.

Como na vida em sociedade, o meio cibernético também deve ser protegido, e resguardado. No artigo 7º da lei do Marco Civil da internet é assegurado o direito de inviolabilidade da vida privada, e em que sendo violada, pode resultar em danos materiais ou morais, como também é assegurado o sigilo das comunicações, podendo ser quebrados, salvo por ordem judicial.

A preservação da privacidade, intimidade, honra e imagem são direitos fundamentais dentre tantos outros previstos e ditos invioláveis na nossa constituição federal. A todo e qualquer instrumento legal que venha a reger determinada temática ou ramo do direito há que se embasar em princípios gerais da nossa carta maior, tal como o Marco Civil o faz principalmente no seu artigo 7º, tomando como parâmetro o Artigo 5 º, X da Carta Magna.

O uso da imagem e a privacidade na Internet também são alvos de decisões do STJ. Numa recente decisão, o relator do Agravo de Instrumento (Ag) 1.347.502, ministro João Otávio de Noronha negou o pedido do Google Brasil Internet Ltda., que recorria contra decisão do Tribunal de Justiça do Rio de Janeiro (TJRJ). O tribunal fluminense, com base no Código de Defesa do Consumidor (CDC), decidiu que a empresa é responsável pela publicação de um perfil falso num sítio de relacionamento e deve indenizar a pessoa atingida.

O Google foi parte em outro processo, relacionado ao mesmo sítio de relacionamento. Só que nesse caso, o Resp 1.193.764, relatado pela ministra Nancy Andrighi na Terceira Turma, a decisão foi favorável à empresa. No caso, conteúdos publicados no sítio de relacionamento foram considerados ofensivos e a empresa foi processada.

Os números falam por si só quão relevante é garantir àqueles que usufruem dos meios virtuais, seja para que atividade for, e que para tanto necessitam expor informações particulares valiosas. E ainda mais importante que proteger tais informações é necessário também formular atividades para que a prática dessa proteção seja real e não só teórica.

Mesmo os dados que não são públicos ficam de certa maneira disponíveis para quem estiver mal-intencionado. Da mesma forma que se rouba um objeto material, informações preciosas podem ser roubadas – basta que essas informações estejam digitalizadas em alguma máquina ou dispositivo eletrônico.

Podemos destacar que a segurança e a proteção de dados das redes é de extrema importância e são aspectos essenciais a serem verificados quando se lida com comunidades virtuais, devendo tais informações serem protegidas contra perdas acidentais ou violações propositais na rede do sistema.

O exposto nos artigos citados é de fundamental importância para frear, a princípio, as altas taxas de crime cibernéticos no país. Dados de 2013 estimam que o Brasil perdeu entre 7 e 8 bilhões de dólares devido a crimes dessa natureza; mais recentemente, em 2015, relatório da ONU divulgado coloca o Brasil entre os 5 países no mundo com as maiores taxas de crimes pela internet.

4.4 AS TENTATIVAS DE INTRUSÕES NOS SISTEMAS VIRTUAIS DO SISTEMA DE SEGURANÇA PÚBLICA PELAS COMUNIDADES DE REDE

A rede é o sangue de qualquer companhia. Quilômetros de cabos elétricos e de fibras ópticas estão nas paredes de qualquer empresa, agindo como sistema circulatório que fornece sangue rico em oxigênio ao cérebro. Mas a configuração original de uma rede local ou de uma longa distância (LAN ou WAN, respectivamente) corporativa típica é menos do que segura. Suas vulnerabilidades não são irrelevantes, pois uma vez que um atacante entre em sua rede, ele invade toda a companhia. (MCCLURE; SCAMBRAY; KURTZ, 2000, p.288).

Atualmente, as redes Ethernet modernas não se parecem em nada com as versões mais antigas. Em redes Ethernet antigas, as estações eram conectadas por longos cabos coaxiais que enviavam o tráfego de destino a todos os nós do segmento, e a todos os dispositivos da rede. Nas redes modernas se usa cabeamento de par trançado ou fibra ótica para conectar as estações em um padrão radial. As redes comutadas substituem a mídia compartilhada utilizada pela Ethernet antiga por um segmento dedicado para cada estação, onde o pacote chega através de um *switch* ao destino pretendido, ou seja, a estação final, enviando e recebendo dados ao mesmo tempo, sem a ocorrência de colisão de informações.

Para o invasor do sistema, a descoberta dos dispositivos de rede, devido a falhas de projeto, o leva a começar a varredura de portas, procurando marcas reveladoras, identificando os dispositivos, ante uma segurança digital mal feita, vazando ou alterando as informações, gerando uma vulnerabilidade das mais difíceis de serem entendidas.

Vários incidentes se destacam como exemplo clássico de *hacking* de rede, nos anais das atividades de *hacker,* é o ataque no dia de Natal de 1994, supostamente lançado pelo famoso hacker Kevin Mitnick contra o computador pessoal do renomado especialista em segurança Tsutomu Shimomura em San Diego, Califórnia (EUA); o furto de fotos de celebridades do iCloud da Apple em 2014; a violação do portal Ashley Madison em 2015; o roubo de dados de cerca de 83 milhões de cliente do Banco JPMorgan Chase em 2014; a violação de dados do Escritório de Administração de pessoal do governo dos EUA, Provavelmente pela China em 2015.

O ex-técnico da CIA Edward Snowden, de 29 anos, é acusado de espionagem por vazar informações sigilosas de segurança dos Estados Unidos e revelar em detalhes alguns dos programas de vigilância que o país usa para espionar a população americana – utilizando servidores de empresas como *Google, Apple e Facebook*– e vários países da Europa e da América Latina, entre eles o Brasil, inclusive fazendo o monitoramento de conversas da presidente do Brasil com seus principais assessores. Snowden teve acesso às informações que vazou para a imprensa quando prestava serviços terceirizados para a Agência de Segurança Nacional (NSA) no Havaí, fato que deixou o mundo todo em constante alerta diante da ameaça cibernética e acesso aos dados pessoais e sigilosos de pessoas do mundo inteiro.

Supõe-se que a adoção de sistemas computadorizados na administração pública forneça um considerável apoio ao aperfeiçoamento da gestão pública, seja devido à transparência na qual se ofertam seus serviços, seja no apoio a operações em volume e extensão geográfica compatíveis com as dimensões populacional e territorial brasileiras.

Tais medidas, quando combinadas com ações de formação de recursos humanos, podem produzir um ciclo virtuoso, que aumenta o desempenho e estimula novas demandas por atuação do governo, especialmente necessárias no atendimento à redução das desigualdades sociais ainda muito grandes no país.

Durante uma conversa informal com a Analista de Negócios da PRODAM/DPRON/AM, a mesma nos relatou em 10 de maio de 2017, como se desenvolve a infraestrutura de dados do Sistema de Segurança em relação ao suporte de rede que é disponibilizado pela PRODAM.

> A Sociedade de Economia Mista, Processamento de Dados do Amazonas S/A-PRODAM é um órgão de informática do Estado. A Prodam concentra todas as informações da maioria dos segmentos do Estado. Nós prestamos

> serviços de TI (Tecnologia da Informação) a todas as Secretarias e órgãos do Estado. Nós temos uma rede de fibra óptica na cidade chamada Metromao, e essa rede de fibra óptica, todos os órgãos ou a maioria dos órgãos do estado estão ligados nela. A Secretaria de Segurança até pouco tempo quando estava no prédio da Torquato Tapajós, ela estava dentro desta rede, agora que foi para o Shopping Via Norte, está com um link de fibra direto de uma Empresa chamada Eisenware que é nossa contratada e que tem, e que faz também uma rede conosco. (R. J., Analista de Negócios). Pesquisa realizada em 10.05.2017.

Informalmente, falamos sobre os *ciberataques* que vem ocorrendo na rede mundial de computadores, lembrando que esse último *ciberataque* tratou-se de uma aparente campanha de *ransomware* – em que computadores foram infectados com um vírus que codificou e "sequestrou" os arquivos. Os invasores, então, pediram um "resgate": ameaçaram destruir (ou tornar públicos) os arquivos caso não recebessem dinheiro.

O *WannaCryptor,* vírus utilizado no ataque, funcionou apenas em computadores com o Windows, e indagamos a analista, como ocorre o procedimento de proteção e neutralização em razão desses ataques repentinos no sistema, e se relatos ou tentativas de invasão pelas comunidades de rede no meio virtual do ambiente de dados do sistema de segurança pública, ocasião em que ela nos reporta o que segue:

> **Então a gente tem um perigo bastante minimizado em relação à invasão, mas não é que não exista, hacker faz qualquer negócio,** mas diminui bastante essa vulnerabilidade do sistema em relação a invasões.Todas as Delegacias e todos os órgãos que compõem a parte de Segurança Pública, na Polícia Militar, no Corpo de Bombeiros, como na Polícia Civil, todos eles estão ligados a Prodam através de uma fibra, então é um canal direto, ninguém sai pra Internet, então esse perigo diminui bastante em função disso. E o que se fez foi desenvolver um Sistema Integrado para eles, e a gente nunca teve até agora nenhum problema de invasão. (R. J., Analista de Negócios). Pesquisa realizada em 10.05.2017.

Continuo indagando a analista se há ou não a possibilidade de intrusão, e se há algum controle de dados em relação a essa situação no concernente as tentativas de intrusões pelas comunidades de rede no meio virtual do ambiente de dados do sistema de segurança pública.

> complementa a senhora...que o Sistema deles é via internet mas na verdade ele não sai pra internet, ele trafega só na rede do Estado. A Secretaria Executiva Adjunta de Inteligência/SEAI trabalha com outro Sistema também, além desse interno deles lá, que a gente desenvolveu há muito tempo atrás, tem uma tecnologia bastante antiga mas como ela está num ambiente

> fechado, então fica bastante difícil de invadir, observa-se que existe mecanismos de segurança da informação ou privacidade no ambiente virtual do sistema de dados da Secretaria de Segurança. (R. J., Analista de Negócios). Pesquisa realizada em 10.05.2017.

Pressupondo-se que literalmente essas comunidades de rede consigam invadir os sistemas de dados da secretaria de segurança, há algum mecanismo de software específico para segurança da informação ou privacidade existente no ambiente virtual para proteger e neutralizar a ação desses *hackers.*

> Em relação ao suporte que está sendo dado à Secretaria de Segurança a Gestora de Negócios da Prodam relata que já tem bastante tempo que trabalha com eles, mas a partir de 2011 e 2012 desenvolveram esse Sistema de Segurança Pública Integrado. Eles já trabalhavam com outros isolados, mas não entravam integrados. Hoje se trabalha desde a denúncia do BO (Boletim de Ocorrência) até o processo ir para o Judiciário.
>
> R.J. explica também que quanto aos mecanismos de segurança ou softwares específicos para a proteção e neutralização de dados dos Sistema de Segurança, que não tem nada na Secretaria de Segurança, tudo fica na PRODAM. " Na Prodam nós temos os sistemas de Hardware, de softwares bastante robusto que protege todo o ambiente do Estado. Na verdade não é específico para a Secretaria de Segurança, protege todo o ambiente do Estado. **A gente tem cerca de 60.000 (sessenta mil) tentativas de invasões por dia.** Então já faz bastante tempo que a gente não tem nenhum tipo de invasão em nenhum órgão. Não é só dentro da Secretaria de Segurança. (R. J., Analista de Negócios). Pesquisa realizada em 10.05.2017.

Observa-se então que os ataques ocorrem, e que o número desses ataques é bem significativo, e que vem sendo monitorados e controlados pela Prodam, através de Softwares específicos para a proteção e neutralização desses ataques nos sistemas de informação. No entanto ainda indago a analista se, o sistema de segurança pública, através das comunidades de inteligência, os analistas da Prodam, tem conseguido tolher essa invasão pelas comunidades de rede nos sistemas de informação.

E ela complementa:

> Na verdade a proteção é em cima de todos os dados que estão contidos aqui, não é especificamente para um ou para outro, tanto que a gente trabalhou agora nos Jogos Olímpicos, trabalhamos também nas Olimpíadas junto com o Exército e a gente não teve nenhum problema, a gente ligou a nossa rede à rede do Exército, nesse dois grandes eventos, a gente disponibiliza para a Polícia o aparto para todos os grandes eventos aqui de Manaus, Carnaval, a operações grande e a gente nunca teve problema.
>
> A Prodam tem equipamentos e softwares que fazem isso, e o nosso pessoal é que cuida disso aí. Isso não quer dizer que a Prodam nunca vá ser invadida. A gente nunca tem 100% (cem por cento) de segurança. Mas a gente tem uma segurança bastante boa que até agora a gente não teve nenhum

> problema. Toda a segurança da rede é feita na Prodam, nós temos os spywares[2], a gente tem os DBS[3], funcionam todos aqui. A gente tem o suporte de outras empresas, mas tudo é coordenado por aqui, sendo coordenado pelo Setor de Segurança. E tem o pessoal que cuida dessa parte, da segurança de tecnologia, segurança dos dados, dados mesmos. (R. J., Analista de Negócios). Pesquisa realizada em 10.05.2017.

Certifica-se, então que os testes de invasão têm por objetivo verificar a resistência dos sistemas em relação aos métodos de ataque existentes. Diariamente são descobertas novas falhas nos mais variados sistemas, por isso é de fundamental importância a realização de auditorias preventivas, e especificamente, estes testes de invasão podem dar um diagnóstico fidedigno sobre a segurança dos sistemas em questão.

R.J. esclarece que:

> a Prodam tem ainda uma parceria com o pessoal de tecnologia da Secretaria de Segurança que cuida da parte mais operacional da rede, se pintar um problema, essas coisas todas, mas assim, falando em termos de segurança, desde a implantação do Sistema de Segurança, a gente nunca teve problema de invasão.
>
> A Secretaria Executiva Adjunta de Inteligência/SEAI tem outros sistemas que funcionam lá e que são ligados a Brasília, e que a gente não tem ligação. (R. J. Analista de Negócios). Pesquisa realizada em 10.05.2017.

Para controlar, recuperar e monitorar o sistema, observar as vulnerabilidades e restaurar os arquivos há a necessidade do acompanhamento de profissionais qualificados para o desempenho dessa tarefa, e em relação a essa situação pergunto a analista se há especialistas ou profissionais responsáveis pela segurança da rede da secretaria de segurança na Prodam, e quais as formações acadêmicas e qualificação específica desses profissionais.

> em relação aos especialistas e profissionais responsáveis pela segurança da rede da Secretaria de Segurança, há um setor dentro da Prodam composto por quatro ou cinco pessoas que só cuidam da área de segurança, sendo todos formados na área de tecnologia, e todos são especialistas na área de segurança da informação. (R. J. Analista de Negócios). Pesquisa realizada em 10.05.2017.

A Vulnerabilidade é uma falha, também conhecida como *bug,* presente na segurança de um elemento do sistema, que pode ser utilizada por um atacante para deturpar o comportamento esperado deste elemento, normalmente um componente de software, sujeitando o sistema afetado a problemas como indisponibilidade,

obtenção indevida de acessos privilegiados e controle externo por indivíduos não autorizados.

A partir do momento em que ocorrem interconexões entre os sistemas, as vulnerabilidades em um deles, podem levar a ataques contra outros, podendo propagar-se a outros sistemas, onde ninguém percebe ou é responsável pela mitigação.

4.4.1 O inconstante estado de segurança e o suposto direito de liberdade

O surgimento das polícias modernas transformou, pois, a maneira de relacionamento do Estado com a sociedade, dividindo-se em duas grandes áreas: administrativa (polícia preventiva, ou ostensiva), e polícia judiciária (polícia de investigação), conforme o Artigo 144 e §§ da Constituição da República de 1988.

O Estado se revela incapaz de controlar a economia nacional e conter os limites da legalidade do Estado de Direito, constrangendo-se a tolerar atividades informais ou ilegais, e perdendo completamente o controle democrático da situação, e como agravante se depara com essa rápida difusão do crime, principalmente quanto às atividades como o narcotráfico e comércio de armas, perdendo, assim, também o controle efetivo da violência endêmica da sociedade civil, e de suas forças repressivas.

Quanto ao envolvimento da mídia retratando a segurança pública como objeto de análise, significa refletir sobre o fato de que cada um desses polos têm sua maneira de construção. No primeiro a realidade social por meio dos sentidos e das narrativas que supostamente representam a "realidade" da violência e, no outro, a violência como a própria realidade.

Sacrifica-se a liberdade com o controle, a autonomia com a repressão, e entramos em uma nova ditadura, a da sobrevivência, a da necessidade que usa a tecnologia como arma.

Verifica-se que apesar de iminente o perigo e de se estar presenciando continuamente fatos violentos, a mídia tende a arriscar os seus profissionais, e a colocar em risco as pessoas envolvidas nestes fatos, por simplesmente expor suas vidas, histórias e realidades.

Em outras palavras, se a realidade é apresentada através de narrativas e imagens de guerra ou de paz, os efeitos sobre possíveis formas que orientam a condutas desses atores sociais serão igualmente distintos, e para tanto as vezes uma

imagem mal colocada ou mal contextualizada pela mídia pode desmistificar os poderes da polícia, levando a uma análise pessoal e subjetiva das pessoas, sobre seus entes e acerca da sua atuação.

Essas tendências, expostas muitas vezes nas ocorrências policiais do cotidiano, refletem tensões da sociedade pós-moderna, praticamente em toda parte do mundo. E independente do lugar a que você se desloque ou se distancie, pode-se reconhecer, ao lado dos eventos costumeiros e tradicionais que inflam os indicadores de criminalidade, a existência de certas tendências contemporâneas desafiadoras da atuação policial, da gestão da segurança pública e da justiça.

As questões que as tendências contemporâneas se mostram na segurança pública e junto ao sistema de justiça criminal requerem respostas mais sistêmicas, integrais e integradas, capazes de articular ações repressivas e urgentes a outras de natureza mais mediatas e preventivas. Significa agir sobre as causas imediatas do crime, ainda que superficial e mesmo topicamente, como também promover outras intervenções de caráter mais profundo e estrutural.

Assim a polícia é entendida como um grupo de profissionais que executam atividade de segurança pública, exercendo um mandato direcionado prioritariamente para o controle do crime e da manutenção da ordem, não deixando de realizar algumas funções negociáveis de caráter social, a polícia é essencial para a ordem social e sem esta força pública a sociedade se tornaria um caos. Encontra-se sob a responsabilidade da segurança pública, representada, também, pela instituição policial.

Podemos então deduzir que a atividade de polícia é, portanto, política, uma vez que diz respeito à forma como a autoridade coletiva exerce seu papel. A partir desta concepção moderna de polícia, é possível encontrar várias definições que possibilitam um melhor entendimento do significado do termo na atualidade.

Apesar de tudo, para que de fato ocorra algo substancial é necessária uma mudança drástica nos segmentos da segurança pública, como a prevenção do crime situacional e na comunidade a que se encontra o infrator, fazendo-se precípua a implementação de ações estruturais e de ações imediatas ou urgentes, preventivas e repressivas, vez que o crime se rearticula com certa celeridade, incorporando medidas de superação às ações utilizadas para evitá-lo, e das providências adotadas para combatê-lo.

Maria Sylvia Zanella Di Pietro, adota um conceito moderno, onde "o poder de polícia é a atividade do Estado que consiste em limitar o exercício dos direitos individuais em benefício do interesse público".

> O conceito jurídico de ordem pública não se confunde com incolumidade das pessoas e do patrimônio (art. 144 da CF/1988). Sem embargo, ordem pública se constitui em bem jurídico que pode resultar mais ou menos fragilizado pelo modo personalizado com que se dá a concreta violação da integridade das pessoas ou do patrimônio de terceiros, tanto quanto da saúde pública (nas hipóteses de tráfico de entorpecentes e drogas afins). Daí sua categorização jurídico-positiva, não como descrição do delito nem cominação de pena, porém como pressuposto de prisão cautelar; ou seja, como imperiosa necessidade de acautelar o meio social contra fatores de perturbação que já se localizam na gravidade incomum da execução de certos crimes. Não da incomum gravidade abstrata desse ou daquele crime, mas da incomum gravidade na perpetração em si do crime, levando à consistente ilação de que, solto, o agente reincidirá no delito. Donde o vínculo operacional entre necessidade de preservação da ordem pública e acautelamento do meio social. Logo, conceito de ordem pública que se desvincula do conceito de incolumidade das pessoas e do patrimônio alheio (assim como da violação à saúde pública), mas que se enlaça umbilicalmente à noção de acautelamento do meio social. (**HC 101.300**, rel. min. **Ayres Britto**, julgamento em 5-10-2010, Segunda Turma, **DJE** 18-11-2010.).

Se não tivermos o direito à privacidade como se poderá ter um debate livre e aberto e de que servirá o direito à liberdade de expressão de cada indivíduo se não há espaço e nem respeito ao direito à liberdade de expressão.

A intrusão pelos *hackers* aos dados de pessoas necessita que se atente para o estado democrático de direito, onde cada pessoa constitucionalmente tem direito ao resguardo e respeito aos seus direitos individuais, mais ainda quando se referem a direito à privacidade.

Não há proteção. Há um efeito paralisante aos comportamentos que se diferenciam desses comportamentos de inteligência. Não existe segurança em lugar algum, vive-se um ambiente de insegurança não apenas físico, mas incisivamente virtual, que em determinados momentos agrega comunidades com o intuito de prejudicar enquanto em outro segmento desagrega pessoas pela falta de privacidade e segurança.

5 PREVISÃO DO ORDENAMENTO JURÍDICO PARA COIBIR A INVASÃO PELAS COMUNIDADES DE REDE EM RAZÃO DOS CRIMES CIBERNÉTICOS REGISTRADOS NO SISTEMA DE SEGURANÇA

No novo contexto tecnológico, qualquer infração penal em que o autor utilize um recurso tecnológico como meio para a prática do delito é tratado como “crime cibernético”. O termo é reconhecidamente o mais apropriado e mais utilizado no meio policial, embora comumente sejam utilizados os nomes “crimes digitais”, “crimes eletrônicos”, “crimes informáticos”, “e-crimes”, “crimes virtuais”, que importam nas menções às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, difusão de pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito), *ciberbullying,* terrorismo, falsificação de dados, estelionatos eletrônicos, racismo e xenofobia (difusão de imagens, ideias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica, injúria e ameaças qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade), entre outros.

Fato é que os meios eletrônicos e, especialmente, a Internet, têm facilitado a perpetração de condutas penais comuns, bem como possibilitaram o surgimento de novas condutas criminosas, mais complexas, pela disseminação de ferramentas de alta tecnologia. Essa nova era tecnológica, que abarca a Sociedade da Informação, propiciou o surgimento de novas espécies de criminosos, responsáveis por grande parte dos prejuízos ocasionados por intermédio da Internet, pela disseminação de vírus, desvendando códigos ou outras informações pessoais. Nos dizeres de Miranda Rosa:

> Todos os tipos de criminalidade, ou quase todos, prestam-se para que sejam cometidos pela via "virtual", ou seja, pela rede eletrônica montada em todos os países. Essa rede está se propagando em grande velocidade, até mesmo pela parente, ou não, simplicidade de seu uso". (FIORILLO, 2013, p.146).

Para que se pudesse proteger esses dados virtuais, e informações sigilosas constantes deste meio ambiente cibernético, houve a necessidade de regulamentação

deste tipo de crime cujo comportamento mostra-se complexo quando praticado por comunidades de rede em razão de diversas ações ilícitas realizadas no ambiente virtual.

O legislador buscou sancionar não apenas o comportamento criminoso da pessoa que faz a instalação do software delituoso, mas também o sujeito ativo que desenvolveu, ofereceu, distribuiu, comercializou ou difundiu o programa.

O crime de invasão de dispositivo informático, conectado ou não a rede de computadores, conforme previsão no artigo 154-A do Código Penal Brasileiro, visa possibilitar e garantir aos operadores do direito a aplicação do dispositivo legal e para que se possa efetivamente, fazer valer os direitos de inúmeras vítimas que sofrem violação criminosa de seus dados ou informações armazenadas em seus computadores, *smartphones*, *tablets*, *pendrives e outros*.

Ainda mais insidioso é o tipo destinado ao mercado internacional. *E-mail*: contendo mensagens do tipo " Alguém te ama!" " Descubra quem é" estimulam o internauta a clicar num *hiperlink* que levam a um *website.* Assim que a tela se abre*,* um leitor de teclado se instala no seu computador, diz o *SuperGeek* e você está ferrado. Um programa leitor de teclado monitora tudo o que você digita e envia as informações a quem quer que o tenha instalado ali. Usando esses dados, o *cibercriminoso* consegue extrair suas senhas, entrar em sua conta bancária e raspar até o último centavo. O *SuperGeek* me conta que cada remessa de 50 mil e-mails garantia ao Aprendiz cerca de duzentas infecções _ isto é, duzentos computadores que criminosos podiam controlar a vontade. Embora represente apenas 0,4% dos e-mails enviados, esse número permite o roubo em quantias fenomenais e explica por que o *cibercrime* é tão atraente. De acordo com a Polícia Federal, o Aprendiz e suas dezenas de cúmplices conseguiram roubar 33 milhões de dólares antes de serem apanhados pela Operação Pégasus. O esquema fraudulento funcionou poucos meses, e no ano anterior, 2004, uma fraude ainda maior rendera aos criminosos 125 milhões de dólares. (GLENNY, 2008, p. 321).

Toda essa violação indevida de mecanismo de segurança, com a finalidade de obter, adulterar ou destruir dados, ou o acesso dessas informações sem autorização expressa ou tácita, ou o ato de instalar vulnerabilidades para obter vantagem ilícita, constitui pena de detenção de três meses a um ano, e multa, com redação de inclusão pela alteração da Lei nº 12.737 de 2012, respondendo o infrator ainda pela

qualificadora caso produza, ofereça, distribua, venda ou difunda dispositivo ou programa de computador com o intuito único de permitir a prática da violação.

A pena é agravada, e passa a ser de reclusão, se dessa invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, de segredos comerciais ou industriais, informações sigilosas, ou de controle remoto não autorizado deste dispositivo invadido, aumentando-se ainda a pena, caso haja divulgação, comercialização ou transmissão a terceiros dos dados ou informações obtidas.

Se este crime for cometido contra Presidente da República, Governadores, Prefeitos, Presidente do Supremo Tribunal Federal da Câmara dos Deputados, do Senado Federal, da Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal, aumenta-se a pena de um terço até a metade.

Os crimes definidos no artigo supra, somente se procedem mediante representação, salvo se o crime for cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Segundo dados da Gerência de Estatística da Secretaria Executiva Adjunta de Inteligência, tendo como fonte o Sistema Integrado de Segurança Pública/SISP, foram registrados no ano de 2013, 835 delitos de Crimes Cibernéticos, dentre ameaças, difamações, injúrias, calúnias, perturbações da tranquilidade, apropriações indébitas, falsas identidades, invasões de dispositivo informático e outras ocorrências; em 2014, 1015 delitos de Crimes Cibernéticos; e em 2015, 548 delitos de Crimes Cibernéticos.

Tabela 1 - Crimes cibernéticos no Amazonas – 2013 a 2017 Fonte: SISP (Adaptada pela autora).

NATUREZAS DE MAIOR INCIDÊNCIA	2013	2014	2015	2016	2017
AMEAÇA	204	248	106	409	252
DIFAMACAO	199	273	84		363
INJURIA	194	199	81	346	236
CALUNIA	61	58	28	122	123
PERTURBACAO DA TRANQUILIDADE	13	24	11	53	26
APROPRIACAO INDÉBITA	4	5	4		
CONSTRANGIMENTO ILEGAL	4	3	4	5	
FALSA IDENTIDADE	3	2	5	8	28
INVASAO DE DISPOSITIVO INFORMÁTICO		3	6	11	14
OUTRAS NATUREZAS	22	29	11	42	22
TOTAL	**835**	**1015**	**548**	**996**	**1064**

Interessante destacar que, conforme observado nos registros do Setor de Estatística é que determinadas apreensões se registram em maior ou em menor número conforme o ano, pois não nos foi disponibilizado os meses das ocorrências para que fosse feita uma análise mais apurada quanto aos índices de referência.

Portanto, parece-nos límpido observar que, apesar das inúmeras ocorrências registradas no Sistema de Segurança Pública, ainda se mostra precário o suporte para acompanhamento das investigações dos crimes nominados como virtuais ou cibernéticos, pela falta de suporte logístico e humano, pois não há no Estado do Amazonas, Delegacia Especializada em Crimes Cibernéticos ou Virtuais, e um contingente suficiente e especializado de profissionais para integrá-la.

O que se presencia hoje, são os registros realizados através da Delegacia interativa da Polícia Civil, através da internet, onde esses crimes recebem uma nomenclatura diferenciada na referida delegacia, que não é especializada para que se possam gerar os dados estatísticos capazes de agrupar os delitos cometidos em redes virtuais ou nos ambientes virtuais, como podemos melhor explicitar.

Por se mostrarem os registros muito discretos ao longo dos anos, não há possibilidade de uma análise comparativa quanto à redução ou aumento de indicadores de criminalidade no Estado do Amazonas em relação aos crimes em questão.

Nota-se, no entanto, que o ano de 2015 houve uma redução quanto aos números dos anos anteriores, e de forma geral e bem substancial, não se sabe ao certo se esses registros definem o quantitativo correto de ocorrências, ou pela falta de

desconhecimento de alguns agentes que operam o sistema, os referidos crimes teriam sido registrados como ocorrências comuns pela dificuldade em discernir, se pela sua origem ou tipificação, seriam agrupados entre os crimes virtuais, ou não.

Quanto as ocorrências registradas de janeiro a dezembro de 2016, e filtradas pela Gerência de Estatística da Secretaria Executiva Adjunta de Inteligência, tendo como fonte o Sistema Integrado de Segurança Pública/ SISP, foi-nos informado o quantitativo de 1158 ocorrências de Crimes Cibernéticos, e no ano de 2017 foram registradas 1121 ocorrências de Crimes Cibernéticos.

Tomando como parâmetro os anos de 2013, 2014, 2015 2016 e 2017 foram computados e registrados junto ao Sistema Integrado de Segurança Pública do estado do Amazonas um total de 4.677 crimes virtuais.

As mudanças legislativas não conseguem acompanhar os passos largos da evolução tecnológica, responsável pelas transmutações do conhecimento científico, não mais estático, mas virtual e transepistêmico, e que pode modificar pensamentos e comportamentos em todo o mundo conectado em questão de milésimos de segundos, quebrando as barreiras virtuais do impossível.

Resta-nos relembrar um fato de grande repercussão na mídia televisiva que envolveu a exposição de fotografias íntimas da atriz e modelo Carolina Dieckmann, criando um misto de indignação e falta de respeito, e que deu um impulso à regulamentação da lei que já tramitava há anos. O incidente ocorreu quando a atriz levou seu computador pessoal para conserto junto a uma loja especializada e as fotografias inseridas no disco rígido de seu computador foram veiculadas na mídia digital, situação que lhe causou um grave constrangimento e decepção.

Os crimes cibernéticos estão divididos nas categorias “próprios” e “impróprios”. O segundo é formado crimes comuns que porventura são realizados por todo e qualquer meio, inclusive pela internet como, por exemplo, a injúria.

A ocorrência de crime virtual financeiro de maior valor ocorrido em Manaus, até o momento, envolve a loja de eletroeletrônico Mirai Panasonic, ocorrida em meados de 2017. A empresa criou um e-commerce em abril deste ano e até agosto vendeu, aproximadamente, 250 *smartphones* - 95% deles *iPhones* -, mas não recebeu o crédito de quase R$ 450 mil do pagamento por meio da operadora Cielo, que alegou “suposta fraude” nas vendas, após uma série de contestações de donos de cartões de crédito. A operadora Cielo foi até a Mirai e ficou durante uma semana fazendo cerca de 10 mil testes no site, para saber se se tratava de uma plataforma segura.

A maior parte das vítimas do delito informático é constituída de cidadãos comuns, que em geral não compreendem corretamente o meio em que estão, nem as dificuldades e os prejuízos que podem lhes ser impingidos, pelo meio eletrônico, causado por outro usuário.

O uso indevido dos computadores e da tecnologia em geral constitui verdadeira ameaça global. “Cibercrimes”, “Crimes Cibernéticos”, “Crimes Digitais”, “Crimes Informáticos”, “Crimes Eletrônicos”, são termos para definir os delitos praticados contra ou por intermédio de computadores (dispositivos informáticos, em geral).

No Brasil, os ataques a computadores brasileiros quase triplicaram em 2011 em relação ao ano anterior. No ano de 2012 foram 399.515 registros de problemas com vírus, códigos maliciosos ou tentativas de fraude, enquanto em 2010 eram 142.844.

A Lei nº 12.737 de 2012, também alterou a redação dos artigos 266 e 298 do Código Penal para adequá-los a realidade cibernética.

O artigo 266 teve a sua titulação alterada para inserir a interrupção quanto aos serviços informáticos. Em seu contexto esse dispositivo trata do seguinte delito “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública”.

Em relação ao artigo 298, no parágrafo único, o legislador equiparou como documento particular os cartões de crédito e débito no delito de falsificação de documento.

Essa nova lei classifica como crime justamente casos semelhantes, em que há a invasão de computadores**,** *tablets* ou *smartphones*, conectados ou não à internet, “com o fim de obter, adulterar ou destruir dados ou informações”. Ou seja, uma legislação que resguarda nossa intimidade, porém sem garanti-la de fato.

Cyberbullying é a intimidação e a violência na internet**.** O veículo mais utilizado para esta prática são as redes sociais. Em tempos de internet, *o bullying* ignora fronteiras, assim como suas vítimas e executores.

A exposição de adultos e crianças em cenas de nudez e sexo como forma de ganhar dinheiro com o *cibercrime*, se prolifera pela internet à medida que crianças e jovens aparecem cada vez mais conectados às redes sociais. Isso ocorre em razão do somatório da internet aos antigos veículos de comunicação.

Em relação à criação e produção, os filmes e fotos de sexo envolvendo crianças ainda se prendem às técnicas próprias dessas mídias antigas, no entanto, somadas

ao veículo internet tudo muda. O primeiro fator introduzido pela internet é o anonimato, porque sem uma investigação profunda é difícil saber quem produz ou distribui esses conteúdos criminosos na rede.

Outro comportamento que vem se expandindo na internet é o *sexting*, resultado da união das palavras em inglês: *sex* (sexo) e *texting* (envio de mensagens), e se resume na prática em que pessoas usam seus celulares, câmeras fotográficas, e-mail, chats, mensagens instantâneas e redes sociais para produzir e enviar fotos sensuais de seu corpo nu ou em trajes íntimos. Também se enquadram neste conceito os textos eróticos (em dispositivos móveis ou internet) com convites e insinuações sexuais para namorados, pretendentes ou amigos, sendo certamente uma grande porta que os usuários da internet disponibilizam.

O aliciamento de menores é um crime de grande incidência nas cidades brasileiras e as autoridades fazem constantes apelos para que as famílias fiquem bem atentas à ação dos criminosos. As redes de cafetões agora recrutam pessoas em redes sociais, fazem falsas propostas de trabalho como modelo ou manequim e utilizam as vítimas para recrutar outras jovens.

Ao navegar pela internet**,** crianças e adolescentes podem se deparar com sites que procuram adeptos por meio da pregação da violência contra homossexuais, mulheres, negros, nordestinos, judeus e outros, além da incitação a crimes.

Geralmente o aliciador fala com as crianças por meio de mensagens de celular e procura marcar encontro em um local de grande circulação de pessoas. Nesse primeiro contato, a intenção do aliciador não é cometer abuso, mas ganhar a confiança da vítima para marcar outros encontros em locais mais reservados.

Quadrilhas procuram sinais de ostentação na web. Golpistas, entre eles chantagistas e ladrões, necessitam de informações para cometer seus crimes. Antigamente, os criminosos se valiam de informantes que atuavam muito próximo a suas futuras vítimas: amigos, colegas de trabalho, empregados ou outros, e quando não podiam contar com informantes, os criminosos partiam para um longo processo de observação dos hábitos da vítima.

Esses métodos não foram abandonados nos dias de hoje, mas, com a internet, a partir da difusão do uso de redes sociais, esse trabalho de obtenção de informações foi extremamente facilitado. Suas informações são visíveis em tempo real.

A rede mundial de computadores mostra um cenário em que os usuários potenciais vítimas são, em diversos casos, os condutores de seu próprio rumo e

destinos virtuais. Não são somente as crianças e os adolescentes que estão sujeitos a serem vítimas de crimes na internet; mas também os adultos.

O caráter subsidiário do Direito Penal deve ser sempre buscado, especialmente com medidas preventivas de inclusão digital, educando e conscientizando as pessoas quanto ao uso racional dos meios informáticos.

5.1 CONTROLE DA SEGURANÇA PELAS COMUNIDADES DE INTELIGÊNCIA E AS INTERFERÊNCIAS VIRTUAIS NO SISTEMA DE SEGURANÇA PÚBLICA PELAS COMUNIDADES DE REDE

Uma organização não detém, nem jamais deterá, controle pleno sobre os eventos do seu ambiente, sejam o interno ou o externo. Portanto, sujeita-se aos riscos. Decorre da exposição ao risco a necessidade de ações que consistem em observar os eventos passados e as condições da situação presente; estimar as chances de eventos potenciais no futuro (riscos) que influenciem a organização de forma negativa (riscos de segurança) ou positiva; e adotar decisões e controles para neutralizar os riscos negativos, garantindo o alcance de condições desejáveis no futuro.

Dá-se o nome de gestão da segurança a este conjunto de ações, quando realizadas de forma intencional, planejada, organizada, monitorada e controlada.

O criminoso informático pode cometer mais de uma conduta lesiva ao mesmo tempo, estando em diversos lugares simultaneamente, e conta com a vantagem de haver poucos profissionais de segurança pública capacitados para investigar sua ação, analisar as provas e os indícios. Sem contar a vantagem de o agente não fazer qualquer esforço e agir de forma transnacional com facilidade ímpar.

Para que isso aconteça, além dos diversos setores dentro do Sistema de Segurança Pública, ocasião em que fizemos uma levantamento de informações em 17 de maio de 2017 por meio de roteiros informais, oportunidade em que destacamos neste momento a Secretaria Executiva Adjunta de Inteligência que é um órgão integrante da Secretaria de Estado de Segurança Pública do Amazonas.

> Informa-nos o representante da Secretaria Executiva Adjunta de Inteligência/ SEAI que a mesma foi criada por meio da lei delegada n° 63/2007 e nos termos do seu artigo 3º possui como atribuições:
>
> I - auxiliar diretamente o Secretário de Estado nos assuntos inerentes às atividades de Inteligência Policial dos órgãos integrantes do Sistema Estadual de Segurança Pública;

> II - centralizar a coleta dos dados obtidos pelos Órgãos de Inteligência do Sistema;
>
> III -acompanhar e classificar a difusão das informações, criando mecanismos de proteção de dados, bem como disponibilizando, permanentemente, dados de interesse para as investigações e operações policiais;
>
> IV - manter intercâmbio com a Comunidade de Informações, Instituições de Bancos de Dados, Órgãos Auxiliares do Sistema e congêneres, preservando sempre o grau de confiabilidade mútua;
>
> V - filtrar, em todos os níveis, as informações obtidas, compartimentando-as;
>
> VI - participar das investigações e operações policiais, dando o suporte necessário;
>
> VII - acompanhar todas as atividades de Inteligência Policial do Sistema, fornecendo suporte técnico-operacional, quando requisitado;
>
> VIII - concentrar e alimentar, permanentemente, bancos de dados e informações de interesse policial;
>
> IX - fiscalizar a utilização e difusão dos dados obtidos, via Comunidade de Inteligência;
>
> X - executar outras atividades que lhe sejam determinadas ou delegadas pelo Secretário de Estado.
>
> XI - requisitar diretamente de qualquer órgão estadual informações, certidões, cópias de documentos ou volumes de autos relacionados com investigações em curso sem o pagamento de quaisquer taxas, custos ou emolumentos.

Observamos ainda a diversidade de profissionais que apesar de policiais integram a referida Secretaria, e indagamos que profissionais especialistas fazem parte dessa Comunidade de Inteligência e que hoje ocupam os quadros da SEAI, o que nos foi relatado que

> os servidores da SEAI são oriundos dos diversos órgãos integrantes do Sistema de Segurança Pública do Amazonas (PC, PM e Bombeiros), além de outros com experiência nas Forças Armadas e Sistema Penitenciário, além disso possuem formação na área de inteligência através de cursos realizados pela Secretaria Nacional de Segurança Pública, Agência Brasileira de Inteligência e Forças Armadas. (Representante da SEAI). Pesquisa realizada em 17.05.2017.

Efetivamente, o representante da Secretaria Executiva Adjunta de Inteligência nos informa que trabalho vem sendo desenvolvido pelos agentes.

> Ao longo de dez anos como órgão central do Sistema de Inteligência de Segurança Publica do Estado do Amazonas, a SEAI realizou inúmeras operações com o suporte dos órgãos integrantes do sistema, notadamente em combate a organizações criminosas e ao narcotráfico. (Representante da SEAI) Pesquisa realizada em 17.05.2017.

E os meios são utilizados para o desenvolvimento desse trabalho são: técnicas operacionais previstas na doutrina de inteligência tais como: Entrevista, Estoria-Cobertura, Vigilância, coletas de informações, bancos de dados e outros. (Representante da SEAI).

Indaga-se ainda se os recursos empregados são os necessários para atingir os fins da ação policial, e o representante nos esclarece que "A SEAI dispõe de meios adequados para a consecução de seus objetivos, com constante aprimoramento de suas ferramentas tecnológicas." (Representante da SEAI). Pesquisa realizada em 17.05.2017.

Complementa ainda o Representante da SEAI que, quanto ao grau de hierarquia de veiculação de informações,

> esses conhecimentos produzidos pela SEAI possuem natureza sigilosa, sendo difundidos conforme a necessidade de conhecer das autoridades ou órgãos de inteligência receptores*"* Que dada a natureza sigilosa de suas atividades, todos os setores da SEAI necessitam da aplicação de medidas de segurança previstas em seu plano de segurança orgânica, em razão de proteção e controle diuturnos, mais especificamente a Gerência de Sistema de Informação –GSI. E que o grau de hierarquia quanto a veiculação de informações, encontra-se previsto na Lei Nº 12.527/2011 que trata do Acesso a Informação

Informou-nos, também, o Representante da SEAI, que são utilizados como procedimentos para evitar invasão por *hackers* a estrutura de software Fail2ban e essa estrutura é desenvolvida com Firewall através do sistema Linux, utilizando-se, ainda, o controlador de domínio com firewall do windows, em razão das tentativas diárias de invasões por comunidades de rede *(hackers)* na rede dos sistemas de informação da SEAI. Havendo um controle de dados por intermédio dos *log's* do sistema.

Esclareceu-nos o Representante da SEAI que os mecanismos de softwares específicos para segurança da informação ou privacidade existentes no ambiente virtual do sistema de dados da secretaria de segurança para proteger e neutralizar a ação dos "hackers são realizados através do Fail2ban*"*, que é responsável por fazer bloqueio após 3 tentativas de invasões, sendo a Gerência de Sistemas de Informação da SEAI a responsável por inibir e neutralizar essas invasões ao sistema.

5.2 ORGANIZAÇÃO DO MONITORAMENTO E CONTROLE VIRTUAL EFETUADOS PELO SISTEMA DE SEGURANÇA PÚBLICA

A organização da estrutura de monitoramento e controle possui vantagens, sendo uma delas a diminuição do risco a que está sujeito o cidadão, nela incluindo-se o policial em sua ação cotidiana, cuja agilização quanto a ação policial no cometimento da infração por parte do infrator estar sendo controlada e monitorada, o que sobremaneira diminui os riscos de um maior atingimento de pessoas (vítimas) e capaz de promover um pouco mais de segurança.

Para redução dos riscos se faz também necessário melhorar as percepções, atitudes, capacidades técnicas e ações gerenciais dos servidores públicos no que concerne ao valor estratégico da informação e da comunicação públicas, e aos cuidados com a gestão da segurança dessas informações, de suas tecnologias de suporte, e tais competências devem ser combinadas com o contínuo alinhamento ao interesse público, inclusive quanto à transparência.

A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto na Lei nº 9296/96 e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça, e no parágrafo único, sua disposição aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

A interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento, da autoridade policial, na investigação criminal, do representante do Ministério Público, na investigação criminal e na instrução processual penal.

Explica o Analista de Informação do Departamento em Repressão ao Crime Organizado/DRCO, em pesquisa realizada em 20 de junho de 2017, que o monitoramento realizado pelo Sistema de Segurança, ocorre quando: *".....*

> os terminais que estão no mandado, os chips e os imeis são cadastrados no sistema de gravação digital, e após oficializar as operadoras de telefonia... é feito o inicio da operação e ficamos ouvindo as gravações em tempo real, monitorando os alvos.. temos também uma equipe operacional que acompanha, caso aconteçam alguns encontros para tirar fotos, fazer filmagens, fazendo esse monitoramento de todos os alvos em tempo real. "

Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada, conforme preceitua a lei de interceptação.

A gravação que não interessar à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada, e o procedimento para que o sistema desse criminoso virtual seja interceptado funciona assim, complementa o analista de informação

> após o término determinado do mandado judicial para monitorar os terminais alvos, onde foram feitas as gravações das descobertas e também as degravações .. é feito um relatorio identificando todos os alvos que geraram conversas relevantes bem como a sua transcrição, sugerindo uma nova prorrogação ou indiciamento dos envolvidos, para que a autoridade policial faça o relatório final do Inquérito Policial." Pesquisa realizada em 20.06.2017.

Por constituir crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei de que maneira é realizada a interceptação telefônica dos criminosos (alvos) considerados virtuais, que cometem os crimes via sistema de informática/ telemática, e o analista de informação nos explana que:

> após recebermos o mandado judicial que autoriza a interceptação das comunicações, nós verificamos que no corpo do mandado tem as linhas telefonicas, os imeis dos aparelhos, e também pode haver os ip's das máquinas que foram utilizadas nas comunicações telemáticas. Para a interceptação da comunicações dos telefones, nos fazemos a programação no nosso gravador digital e enviamos para as operadoras de telefonias os numeros dos terminais que estão nos mandados.. já em referencia aos ip's nós mandamos para as empresas para que forneçam os dados cadastrais de quem utilizou aquele ip num determinado dia e hora e minuto, e após começarmos o monitoramento, ficamos gravando todas as conversas e consequentemente fazemos toda a degravação dos audios, normalmente num período de 15 dias." Pesquisa realizada em 20.06.2017.

E continua explicando que

> quanto ao gravador digital que grava todas as conversas dos telefones e imeis interceptados, acompanhamos em tempo real a "plataforma vigia" de cada operadora de telefonia, onde nesse vigia constam as informações da ligações efetuadas e recebidas das mensagens sms, bem como o endereço onde é feita a ligação gerando a ERB (Estação Rádio Base de cada ligação) dos envolvidos que utilizam naquele momento as chamadas efetuadas e recebidas.Os procedimentos referentes a todos os envolvidos identificados durante a interceptação, através das conversas, do dados cadastrais dos telefones, de dados que passam por mensagem sms, e tambem quanto ao ip, facilita a localização da lan house, onde foi cometido o ilícito e a autoridade policial diante dos elementos probatórios pode solicitar os pedidos de prisão, mandados de busca e apreensão e finalizar o inquérito policial com o

relatório. (Analista de Informação do DRCO). Pesquisa realizada em 20.06.2017.

6. CONSIDERAÇÕES FINAIS

No Estado do Amazonas, em razão de sua dimensão territorial e da concentração populacional na cidade de Manaus, os cenários da violência não são diferentes. A violência contra a propriedade, contra a vida e todos os outros atos de transgressão contra a ordem social é onde a mídia traz seus enfoques e os sentimentos da população se manifestam com mais frequência.

É exatamente no centro da pluralidade que conforma o mundo da violência, nas suas múltiplas manifestações que será tomado como referência para as reflexões que aqui se seguem, já que estamos em contínuo crescimento e o Sistema de Segurança Pública necessita como Instituição e como força policial da criação de uma Delegacia Especializada em Crimes Virtuais.

Verificamos, em pesquisa nos outros estado brasileiros, que já foram criadas e encontram-se em pelo funcionamento a Delegacia Especializada em Crimes Virtuais e Delitos praticados por Meios Eletrônicos, em São Paulo, a Delegacia de Repressão aos Crimes de Informática (DRCI) no Rio de Janeiro, a Delegacia de Repressão a Crimes Eletrônicos (DRCE), no Espírito Santo, a Delegacia Especializada de Investigações de Crimes Cibernéticos em Minas Gerais- DEICC, a Nuciber da Polícia Civil do Paraná, a Delegacia de Repressão aos Crimes Informáticos (DRCI/DEIC) no Rio Grande do Sul, a Delegacia de Repressão aos Crimes Tecnológicos no Pará, a Gerência de Inteligência da Polícia Civil em Goiás, a Gerência de Combate a Crimes de Alta Tecnologia – GECAT no Mato Grosso – Cuiabá, e a Delegacia de Repressão a Crimes Cibernéticos (DRCC) em Sergipe/ Aracaju.

Poderemos aqui, com base na observação e pesquisa feitas que a hipótese para se compreender o fenômeno da violência, imaginar uma polícia sem recursos financeiros no intuito de acompanhar as mudanças que se efetivaram na sociedade e que ganham sustentação quando relacionadas a um conjunto de processos sociais que permitem compreender, em profundidade o aumento significativo da explosão da violência, seja urbana, virtual ou rural, enquanto transgressão da lei e das normas sociais, registrando que, de forma isolada podem não explicar os fenômenos de violência, mas, articulados, passam a fornecer as bases mais concretas da explicação da violência, originária no campo social, e que se não forem tolhedos e até prevenidos por força de uma ação policial preventiva e preparada conforme o crescimento tecnológico, ficará fadada ao descrédito e ao caos.

Por não haver Delegacia Especializada em combate e Repressão a Crimes Virtuais na cidade de Manaus, a vítima de qualquer crime virtual, seja qual for a modalidade, necessita registrar sua ocorrência em qualquer outra Delegacia, que provavelmente não o registrará com a definição e especificidade necessária para que se prossiga com fundamentação e acompanhamento adequado o referido procedimento policial, supostamente envolvendo crimes cibernéticos.

As ações criminosas na sociedade: furto, roubo, estelionato, contrabando, tráfico de drogas, crimes cibernéticos, prostituição infantil, desvios de recursos públicos, sequestro e outros, tornaram-se frequentes na vida urbana, virtual e no interior.

Urge, neste momento, que se propaguem mudanças radicais para que retorne à população, a credibilidade há muito perdida quanto a sua integridade e defesa de seu patrimônio.

Essa intenção política para o sistema, nos diz, porque fazer, considerando que, em caso contrário, continuaremos reféns do crime organizado, por termos negligenciado um instrumento do estado de defesa social, que é o sistema de segurança pública.

Isso evidencia o crescimento que nos leva hoje ao atendimento da demanda, rápido e eficaz, cuja intenção é a de resgatar a eficiência e eficácia da prestação de serviço público na proteção individual e coletiva do povo e sua propriedade, sendo irrelevante, o custo que venha ter, pois o bem maior que é a vida do ser humano, vê-se em primeiro plano, já que há um resgate face ao servidor que trabalha tanto na área meio, quanto na área fim da segurança pública buscando melhorias estruturais e, consequentemente a geração de melhorias que beneficiem a categoria policial como um todo.

Portanto, para que se possa vislumbrar crescimento, propõe-se a criação de uma Delegacia Especializada em Crimes Virtuais sendo de extrema necessidade e pertinente a área da Segurança Pública, para melhor solucionar os crimes cometidos no ambiente virtual.

Desde 2012, tramita na Assembleia Legislativa do Estado do Amazonas (Aleam) um projeto de lei (PL) do governo do Amazonas, que trata da criação da delegacia especializada para que responda por esse segmento de crimes cibernéticos.

A proposta, que tinha previsão inicial de aprovação em 90 dias, mudou para 2015, e com os cortes de despesas do governo, puxados pela crise econômica, não deixaram o Projeto de Lei sai da gaveta.

Enquanto a delegacia especializada não é criada, encontra-se assumindo o papel em fase experimental a Delegacia Interativa e já conta inclusive com procedimentos cartorários que se fazem necessários para qualquer tipo de investigação.

A Delegacia Interativa tem cerca de 72 casos em andamento acerca de Crimes Cibernéticos, entre impróprios e próprios. A grande parte deles partem de requisições judiciais, representações do Ministério Público do Estado do Amazonas (MPE-AM), ficha crime e representação por parte de vítima.

Para que isto ocorra e funcione de maneira eficaz, faz-se necessária a alteração junto a Lei Delegada n° 87 de 18 de maio de 2007, que dispõe sobre a Polícia Civil do Estado do Amazonas, e que define suas finalidades, competências e mais especificamente a estrutura organizacional, para que ocorra a criação da Especializada, com suas atribuições e especificidades inerentes ao seu potencial desenvolvimento.

Destarte, como produto ao Mestrado Profissional de Segurança Pública, Cidadania e Direitos Humanos, e após toda a pesquisa realizada, sugerimos a alteração pontual no item 4. da Lei Delegada n° 87 de 18 de maio de 2007, que dispõe sobre a Polícia Civil do Estado do Amazonas, em seu Capítulo III, da Estrutura Organizacional, no Artigo 3º, inciso IV, que trata dos Órgãos da Atividade Fim, incluindo-se às Delegacias Especializadas, e acrescentando-se para composição do quadro de especializadas, o item 4.17, incluindo-se no rol das delegacias já existentes, a Delegacia Especializada em Combate e Repressão a Crimes Virtuais/DECRCV, com sua respectiva nomenclatura.

Quanto aos seus cargos de provimento em comissão, transcritos no Anexo I da referida Lei Delegada, sugiro a criação de mais uma Titularidade de Delegacia (AD-2) passando de 128 (cento e vinte e oito) cargos, para 129 (cento e vinte e nove), 1(uma) Chefia de Cartório (FG-3), passando de 60 (sessenta) existentes para 61(sessenta e uma) funções gratificadas, e 1(uma) Chefia de Investigação (FG-3), passando de 60 (sessenta) existentes para 61(sessenta e uma) funções gratificadas, e para visualização melhor da modificação, foram realizadas a seguir as alterações sugeridas na Lei Delegada n° 87 de 18 de maio de 2007 (Anexo D).

Em relação às atribuições da Delegacia Especializada em Combate e Repressão a Crimes Virtuais/DECRCV, propõe-se a investigação em casos especiais de crimes que ocorrem no meio cibernético, como invasão de dispositivos móveis, crimes contra o patrimônio em meio virtual sem autoria, crimes contra a honra ou liberdade individual e pesquisas avançadas em redes sociais, com atendimento direto ao público, e apoio a outras delegacias e entidades de investigação que requisitem auxílio.

Além da tecnologia, que não deve em hipótese alguma ser descartada, para que haja investimento na Polícia Civil, necessitamos, também de servidores capacitados e especializados na área cibernética e crimes virtuais, comprometidos com a sua profissão, honrados, com um nível de satisfação pelo que fazem, e que venham corresponder à sua qualidade de vida para que possam trazer respostas aos clamores da sociedade.

Por todo o exposto, somos sabedores que a eficiência e a eficácia do sistema não dependerão, somente, dos organismos criados e dos mecanismos disponibilizados, mas temos a certeza de que sem eles nada poderemos fazer, ou ficaremos andando engessados.

Dependerá também dos recursos humanos alocados nas funções certas, capazes, indicados pela sua competência e qualificação, não por meios outros, visto que a área de abrangência da segurança pública, por ser uma atividade de ponta com a sociedade, não permitirá conceder espaços a incompetência, a negligência e muitas vezes a corrupção, sem que isso venha, de forma muito forte, comprometer o Poder Executivo, com resultados políticos desastrosos para a administração.

No entanto, os recursos financeiros não podem faltar para o crescimento de uma Instituição forte que tem uma perspectiva otimista e visionária para a aplicação de projetos e investimentos em seu efetivo, e obviamente, gerando um retorno positivo à população, pelo fato da tecnologia avançar a passos largos, e a polícia por ser um órgão precípuo do Sistema de Segurança Pública necessitar sempre de aperfeiçoamento para estar à frente das novas modalidades de crime.

REFERÊNCIAS

BACHELARD, Gaston. **A formação do espírito científico**: contribuição para uma psicanálise do conhecimento. Tradução de Estrela dos Santos Abreu. Rio de Janeiro: Contraponto, 1996.

BITTENCOURT, R. N. **A sociedade de transição** (Resenha do livro A sociedade de risco: rumo a uma outra modernidade de Ulrich Beck). Filosofia (São Paulo), v.53, p.60, 2010.

BAUMAN, Zygmunt. **Comunidade: a busca por segurança no mundo atual.** Tradução de Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2003.

BOLTANSKI, Luc. **Enigmas y complos - Una investigacion sobre las investigaciones**. Buenos Aires: Fondo de Cultura Economica, 2016.

BOURDIEU, Pierre. **A Miséria do Mundo**. Petrópolis/RJ: Vozes, 2007.

BRASIL. Código Penal Brasileiro de 1940 e alterações. Disponível em: <Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm>. Acesso em: 05 nov. 2016.

_____. Constituição (1988). Constituição da República Federativa do Brasil, 1988. Brasília, DF: Centro Gráfico do Senado Federal, 1988. Disponível: www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acessado em 05.11.2016.

_____. Decreto nº 8.793, de 29 de junho de 2016, fixa a política nacional de inteligência. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8793.htm>. Acesso em: 05 nov. 2016.

_____. Lei nº 12.965/2014 - Estabelece princípios, garantias e deveres para o uso da internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 05 nov. 2016.

_____. Lei nº 9.296/1996 - Regulamenta o inciso XII, parte final do Art. 5º da Constituição Federal- Interceptação Telefônica. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em: 05 nov. 2016.

BRUNO, Fernanda, KANASHIRO, Marta, FIRMINO, Rodrigo. **Vigilância e Visibilidade-espaço, tecnologia e identificação**. Porto Alegre: Sulina. 2010.

CALDWELL, H. **Basic Law Enforcement**. Santa Mônica, CA: Goodyear, 1972.

CASTELLS, Manuel. **A galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Tradução de Maria Luiza X. de A. Borges. Rio de Janeiro: Korge Zahar, 2003.

CASTELLS, Manuel. **A sociedade em rede:** na era da informação. 10. ed. Paz e Terra, 2001.

CITIZEN FOUR. (Documentário). Direção: Laura Poitras. Annaud, Produção: Mathilde Bonnefoy, Laura Poitras, Dirk Wilutzky, Steven Soderbergh. EUA: HBO Films, 2014.

COLEMAN, G. E.; Golub, A. Hacker practice: Moral genres and the cultural articulation of liberalism**. Anthropological Theory**, v.8, n.255, 2008.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo**. 12.ed. - São Paulo: aTLAS, 2000.

DURKHEIM, Émile. As regras do método sociológico. In: Durkheim, Émile. **Durkheim – Os pensadores**. São Paulo: Abril Cultural, 1978a.

_____. Da divisão do trabalho social. In: Durkheim, Émile**. Durkheim – Os pensadore**s. São Paulo: Abril Cultural, 1978b.

_____. Uma resenha de Ferdinand Tönnies, Gemeinschaft und Gesellschaft: abhandlung des communismus als empirischer kulturformen. In: MIRANDA, Orlando de. **Para ler ferdinand tönnies**. 1. ed. São Paulo: EdUSP, 1995. p. 113-118.

FERNANDES, Florestan. **Comunidade e Sociedade:** leituras sobre problemas conceituais, metodológicos e de aplicação. São Paulo: USP, 1973.

FILHO, Jayme Teixeira. **Comunidades Virtuais**. Rio de Janeiro: SENAC Rio, 2002.

FIORILLO, Celso Antonio Pacheco. Conte, Christiany Pegorari. **Crimes no meio ambiente digital**. São Paulo: Saraiva, 2013.

_____. **O marco civil da internet e o meio ambiente digital na sociedade da informação/ Comentários a Lei nº 12.965/2014.** São Paulo: Saraiva, 2015.

GARTON, L.; Haythornthwaite, C. e Wellman, B. Studying Online Social Networks. **Journal of Computer Mediated Communication**, v. 1, n. 3, 1997.

GOLDSTEIN,H. **Policing a Free Society**. Cambridge, MA: Ballinger, 1977.

GLENNY, Misha. **MacMáfia. Crime sem Fronteiras**. Tradução Lucia Boldrini. São Paulo: Companhia das Letras, 2008.

GRECO, Marco A., MARTINS, Ives Gandra. **Direito e Internet, Relações Jurídicas na sociedade informatizada.** São Paulo: Revista dos Tribunais, 2001.

GREENE, Jack R. **Administração do trabalho policial**: questoes e analise. Tradução de Ana Luisa Amendola Pinheiro. ed. 1. Reimp. Sao Paulo: USP, 2007.

HERMAN, Michael. **Intelligence power in peace and war**. Cambridge: University Press, 1996.

LÉVY, Pierre. **As tecnologias da inteligência**. O Futuro do pensamento na era da informática; tradução de Carlos Irineu da Costa. - Rio de Janeiro: Ed.34, 1999. Coleção TRANS.

_____. **Cibercultura**. Tradução de Carlos Irineu da Costa. São Paulo: Ed. 34, 1999.

_____. **Heroes of the Computer Revolution**. New York, NY: Dell/Doubleday, 1994.

LENZA, Pedro. **Direito constitucional esquematizado**. 16.ed.rev.atual. e ampl- São Paulo: Saraiva , 2012.

VASCONCELLOS, Marcio J. A**. A internet e os *hackers*: ataques e defesas**. 5. ed. São Paulo: Chantal, 2000.

MCCLURE, Stuart; SCAMBRAY, Joel. **hackers Expostos**. São Paulo: Makron *Books* do Brasil, 2000.

NETO, Mário Furlaneto; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. **Crimes na internet e inquérito policial eletrônico (Crimes contra a Honra, Furto e Estelionato, Criança e Adolescente, Perturbação da ordem, Questões Penais e Processuais Penais controvertidas)**. São Paulo: Edipro, 2012.

NISBET, Robert. **The sociological tradition**. 1. ed. London: Heinemann, 1967.

PRICE,B.R. **Police Profiessionalism**. Lexington.MA: D.C.Heath, 1977.

RECUERO, R. C. **Comunidades em Redes Sociais na Internet: Uma proposta de estudo**. 2005. Disponível em: <http://www.raquelrecuero.com/seminario2005.pdf>. Acesso em: 09 jan. 2018.

_____. **Comunidades Virtuais no IRC**: o caso do Pelotas. Um estudo sobre a Comunicação Mediada por Computador e a estruturação de comunidades virtuais. 2002, 165 f. (Dissertação)-Programa de Pós-Graduação em Comunicação e Informação, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2002.

_____. **Comunidades em Redes Sociais na Internet**: Um estudo de uma rede pró-ana e pró-mia. 2005. Disponível em: <http://www.ufrgs.br/limc/PDFs/ana_mia.pdf>. Acesso em: 09 jan. 2018.

REISS, A.J. Professionalization of the Police. In BRANDSTATTER, A.F. e RADELET. **Police and Community Relations**. Beverly Hills: C.A.Glencoe Press, 1968.

SKOLNICK, J.H. **Justice Without Trial**. New York: John Wiley, 1966.

SPODE, C. B. & MERLO, A. R. C. Trabalho policial e saúde mental: uma pesquisa junto aos Capitães da Polícia Militar. **Psicol. Reflex. Crit**. [online]. 2006, vol.19, n.3, pp.362-370.

TÖNNIES, Ferdinand. Comunidade e sociedade. In: MIRANDA, Orlando de. **Para ler Ferdinand Tönnies**. 1. ed. São Paulo: EdUSP, 1995a. p. 231-352.

TÖNNIES, Ferdinand. Ferdinand. Uma resenha de La division du travail social, de Emile Durkheim. In: MIRANDA, Orlando de. **Para ler Ferdinand Tönnies**. 1. ed. São Paulo: EdUSP, 1995b. p. 118-120.

TONRY, Michael. MORRIS, Norvan. **Policiamento Moderno**. Tradução Jacy Cardia Ghirotti. Sao Paulo: NEV USP, 2000.

WEBER, Max. **Conceitos básicos de Sociologia**. São Paulo: Editora Moraes, 1987.

WEINER, N.L. **The Role of the Police in Urban Society:** Conflicts and Consequences. Indianapolis: Bobbs-Merrill, 1976.

WILHELM, Wilhelm, T. Professional Penetration Testing, Burlington, MA: Syngress, 2010.

ANEXO A - LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012

Presidência da República

Casa Civil

Subchefia para Assuntos Jurídicos

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

“Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

"Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."

Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266. .....

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (NR).

"Falsificação de documento particular

Art. 298. .....

Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito." (NR).

Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.

DILMA ROUSSEFF

José Eduardo Cardozo

ANEXO B - LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

I - o reconhecimento da escala mundial da rede;

II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI - a finalidade social da rede.

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

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

I - do direito de acesso à internet a todos;

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

III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

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

Art. 5º Para os efeitos desta Lei, considera-se:

I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal: o computador ou qualquer dispositivo que se conecte à internet;

III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço Ip.

Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e

costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

CAPÍTULO II
DOS DIREITOS E GARANTIAS DOS USUÁRIOS

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

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

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

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

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

V - manutenção da qualidade contratada da conexão à internet;

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

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

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

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

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

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

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

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput**, tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

CAPÍTULO III
DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I
Da Neutralidade de Rede

Art. 9º 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.

§ 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.

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no **caput** deve:

I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil;

II - agir com proporcionalidade, transparência e isonomia;

III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Seção II
Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

§ 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País.

Subseção I
Da Guarda de Registros de Conexão

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput**.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput**.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Subseção II

Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão

Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

Subseção III

Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput**, observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Seção III
Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

§ 1º A ordem judicial de que trata o **caput** deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5ºda Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos

de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no **caput** deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Seção IV

Da Requisição Judicial de Registros

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

CAPÍTULO IV

DA ATUAÇÃO DO PODER PÚBLICO

Art. 24. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil:

I - estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica;

II - promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil;

III - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

IV - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;

V - adoção preferencial de tecnologias, padrões e formatos abertos e livres;

VI - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VII - otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VIII - desenvolvimento de ações e programas de capacitação para uso da internet;

IX - promoção da cultura e da cidadania; e

X - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos.

Art. 25. As aplicações de internet de entes do poder público devem buscar:

I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;

II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;

IV - facilidade de uso dos serviços de governo eletrônico; e

V - fortalecimento da participação social nas políticas públicas.

Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:

I - promover a inclusão digital;

II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e

III - fomentar a produção e circulação de conteúdo nacional.

Art. 28. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da internet no País.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.

Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no **caput**, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

Art. 30. A defesa dos interesses e dos direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei.

Art. 31. Até a entrada em vigor da lei específica prevista no § 2º do art. 19, a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

Art. 32. Esta Lei entra em vigor após decorridos 60 (sessenta) dias de sua publicação oficial.

Brasília, 23 de abril de 2014; 193º da Independência e 126º da República.

DILMA ROUSSEFF
José Eduardo Cardozo
Miriam Belchior
Paulo Bernardo Silva
Clélio Campolina Diniz

ANEXO C - LEI Nº 9.296, DE 24 DE JULHO DE 1996

Presidência da República

Casa Civil

Subchefia para Assuntos Jurídicos

LEI Nº 9.296, DE 24 DE JULHO DE 1996.

Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.

Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:

I - não houver indícios razoáveis da autoria ou participação em infração penal;

II - a prova puder ser feita por outros meios disponíveis;

III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.

Art. 3° A interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento:

I - da autoridade policial, na investigação criminal;

II - do representante do Ministério Público, na investigação criminal e na instrução processual penal.

Art. 4° O pedido de interceptação de comunicação telefônica conterá a demonstração de que a sua realização é necessária à apuração de infração penal, com indicação dos meios a serem empregados.

§ 1° Excepcionalmente, o juiz poderá admitir que o pedido seja formulado verbalmente, desde que estejam presentes os pressupostos que autorizem a interceptação, caso em que a concessão será condicionada à sua redução a termo.

§ 2° O juiz, no prazo máximo de vinte e quatro horas, decidirá sobre o pedido.

Art. 5° A decisão será fundamentada, sob pena de nulidade, indicando também a forma de execução da diligência, que não poderá exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova.

Art. 6° Deferido o pedido, a autoridade policial conduzirá os procedimentos de interceptação, dando ciência ao Ministério Público, que poderá acompanhar a sua realização.

§ 1° No caso de a diligência possibilitar a gravação da comunicação interceptada, será determinada a sua transcrição.

§ 2° Cumprida a diligência, a autoridade policial encaminhará o resultado da interceptação ao juiz, acompanhado de auto circunstanciado, que deverá conter o resumo das operações realizadas.

§ 3° Recebidos esses elementos, o juiz determinará a providência do art. 8° , ciente o Ministério Público.

Art. 7° Para os procedimentos de interceptação de que trata esta Lei, a autoridade policial poderá requisitar serviços e técnicos especializados às concessionárias de serviço público.

Art. 8° A interceptação de comunicação telefônica, de qualquer natureza, ocorrerá em autos apartados, apensados aos autos do inquérito policial ou do processo criminal, preservando-se o sigilo das diligências, gravações e transcrições respectivas.

Parágrafo único. A apensação somente poderá ser realizada imediatamente antes do relatório da autoridade, quando se tratar de inquérito policial (Código de Processo Penal, art.10, § 1°) ou na conclusão do processo ao juiz para o despacho decorrente do disposto nos arts. 407, 502 ou 538 do Código de Processo Penal.

Art. 9° A gravação que não interessar à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada.

Parágrafo único. O incidente de inutilização será assistido pelo Ministério Público, sendo facultada a presença do acusado ou de seu representante legal.

Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

Pena: reclusão, de dois a quatro anos, e multa.

Art. 11. Esta Lei entra em vigor na data de sua publicação.

Art. 12. Revogam-se as disposições em contrário.

Brasília, 24 de julho de 1996; 175º da Independência e 108º da República.

FERNANDO HENRIQUE CARDOSO

Nelson A. Jobim

ANEXO D – LEI DELEGADA N.º 87, DE 18 DE MAIO DE 2.007

LEI DELEGADA N.º 87, DE 18 DE MAIO DE 2.007

DISPÕE sobre a POLÍCIA CIVIL DO ESTADO DO AMAZONAS, definindo suas finalidades, competências e estrutura organizacional, fixando o seu quadro de cargos comissionados e estabelecendo outras providências.

O GOVERNADOR DO ESTADO DO AMAZONAS

FAÇO SABER a todos os habitantes que, no exercício da delegação que me foi conferida pela **Resolução Legislativa n.º 408**, de 27 de dezembro de 2.006, com a modificação de prazo promovida pela **Resolução Legislativa n.º 415**, de 02 de maio de 2.007, edito a seguinte

< LEI DELEGADA >:

CAPÍTULO I

DAS FINALIDADES E DAS COMPETÊNCIAS

CAPÍTULO II
DA ESTRUTURA ORGANIZACIONAL

.Art. 3.º Dirigida pelo Delegado Geral de Polícia, com o auxílio de um Delegado Geral Adjunto, a Polícia Civil do Estado do Amazonas tem a seguinte estrutura organizacional:

IV - ORGÃOS DE ATIVIDADES-FIM

4. Delegacias Especializadas em:

4.1. Homicídios e Seqüestros

4.2. Roubos, Furtos e Defraudações

4.3. Roubos e Furtos de Veículos

4.4. Ordem Política e Social

4.5. Crimes Contra a Fazenda Pública Estadual

4.6. Capturas e Polícia Interestadual - Polinter

4.7. Crimes Contra o Consumidor

4.8. Acidentes de Trânsito

4.9. Crimes Contra a Mulher

4.10. Assistência e Proteção à Criança e ao Adolescente

4.11. Apuração de Atos Infracionais Cometidos por Crianças e Adolescentes

4.12. Crimes Contra o Idoso

4.13. Crimes Contra o Meio Ambiente e Urbanismo

4.14. Crimes Contra o Turista

4.15. Delegacia Interativa

4.16. Delegacia Especializada em Combate ao Furto de Energia, Água, Gás e Serviços de Telecomunicações

SUGESTÃO DE ALTERAÇÃO

4.17. Delegacia Especializada em Combate e Repressão a Crimes Virtuais

CAPÍTULO V

DOS CARGOS DE PROVIMENTO EM COMISSÃO E DAS FUNÇÕES GRATIFICADAS

Art. 7.º Os cargos de provimento em comissão da Polícia Civil do Estado do Amazonas são os especificados no **Anexo I**desta Lei, extintos os cargos constantes do **Anexo I da < Lei Delegada >** n.º 60, de 29 de julho de 2.005.

Parágrafo único. Os cargos a que se refere este artigo serão ocupados, preferencialmente, por servidores da Polícia Civil do Estado do Amazonas.

Art. 8.º O Delegado-Geral da Polícia Civil poderá atribuir exclusivamente aos servidores da Instituição, através de ato próprio, Função Gratificada (FG) pelo exercício de encargo de chefia, assessoramento ou direção, nos termos do **Anexo II** desta Lei, extintas as funções gratificadas constantes do **Anexo II da < Lei Delegada >** n.º 60, de 29 de julho de 2.005.

GABINETE DO GOVERNADOR DO ESTADO DO AMAZONAS, em Manaus, 18 de maio de 2.007.

ANEXO I

REDAÇÃO ORIGINAL

CARGOS DE PROVIMENTO EM COMISSÃO

QUANT.	CARGO	SIMBOLOGIA
128	Titular de Delegacia	AD-2

SUGESTÃO DE ALTERAÇÃO

CARGOS DE PROVIMENTO EM COMISSÃO

QUANT.	CARGO	SIMBOLOGIA
129	Titular de Delegacia	AD-2

ANEXO II

REDAÇÃO ORIGINAL

FUNÇÕES GRATIFICADAS DA POLÍCIA CIVIL

QUANT.	FUNÇÃO	SIMBOLOGIA	VALOR
60	Chefia de Cartório	**FG-3**	**R$1.240,00**
60	Chefia de Investigação	**FG-3**	**R$1.240,00**

SUGESTÃO DE ALTERAÇÃO

FUNÇÕES GRATIFICADAS DA POLÍCIA CIVIL

QUANT.	FUNÇÃO	SIMBOLOGIA	VALOR
61	Chefia de Cartório	**FG-3**	**R$1.240,00**
61	Chefia de Investigação	**FG-3**	**R$1.240,00**