ASSOCIAÇÃO CARUARUENSE DE ENSINO SUPERIOR – ASCES
BACHARELADO EM RELAÇÕES INTERNACIONAIS

CASO DE JULIAN ASSANGE E CRIMES CIBERNÉTICOS: UMA ABORDAGEM SOB A SEGURANÇA NA INTERNET

THIAGO ANTONIO MACIEL DA SILVA

CARUARU

2014

ASSOCIAÇÃO CARUARUENSE DE ENSINO SUPERIOR – ASCES
FACULDADE ASCES
BACHARELADO EM RELAÇÕES INTERNACIONAIS

CASO DE JULIAN ASSANGE E CRIMES CIBERNÉTICOS: UMA ABORDAGEM SOB O ENFOQUE DA TUTELA PENAL DAS RELAÇÕES DIPLOMÁTICAS

THIAGO ANTONIO MACIEL DA SILVA

Trabalho de conclusão de curso, apresentado à Faculdade ASCES, Curso de bacharelado em Relações Internacionais, sob orientação do Prof. Dr. Bruno Viana.

CARUARU
2014

BANCA EXAMINADORA

Aprovado em: __/__/__.

Presidente: Prof. Dr. Bruno Viana

Primeiro avaliador.

Segundo avaliador.

DEDICATÓRIA

Aos meus pais. E à todos aqueles que contribuíram para a minha formação pessoal e acadêmica.

AGRADECIMENTOS

RESUMO

O ser humano sempre prezou em suas negociações na tomada de decisão a transparência entre todas as partes envolvidas. Na república é imprescindível a transparência e a responsividade do estado em relação aos seus cidadãos. Isto porque, a transparência das políticas externas e internas tomadas por um estado é utilizada para que a população possa analisar e julgar os atos para melhor escolher seus futuros dirigentes. A internet é uma ferramenta e, por si só, não garante o desenvolvimento social, a intensificação da democracia ou a promoção de justiça social. Nesse sentido, o dever estatal da educação deve abarcar o uso da internet como ferramenta de exercício de cidadania e promoção da cultura. este trabalho buscou apresentar contribuições para o combate aos crimes virtuais fazendo um estudo dos crimes cibernéticos a partir dos acontecimentos que desencadearam a reflexão sobre a necessidade de proteção internacional contra a espionagem virtual e outros delitos: o caso de Julian Assenge.

Palavras-chave: Transparência. Cyberativismo. Julian Assange. Crimes digitais. Direito Internacional.

ABSTRACT

The human beeing has always taken in consideration, transparency as a importante key by all members envolved. In the republic it is necessary tranparency and responsiveness of the state towards its citizens. That is said because the transparency on international affairs and inside the state are taken by the state in order to analyse and judge their governos. The internet is a tool, and alone, can not garante social development, neither the intensification of democracy nor the promotion of social justice. In this way, the state's educational duty, should be to use the internet as a tool do express its citizenship and to promote its cultura. This project has seeked to present contributions of the war on digital crimes making a reflexion of digital crimes and events that initiated the need of international protection against virtual espionage and other crimes related: The case of Julian Assange

Key-words: Transparency. Cyberactivism. Julian Assange. Digital Crimes. International Law.

SUMÁRIO

INTRODUÇÃO..... 08
CAPÍTULO I – HISTÓRIA DE JULIAN ASSANGE E A ERA DOS CRIMES DIGITAIS..... 10
1.1 Perfil de Julian Assange..... 10
1.2 Os crimes Cibernéticos..... 13
1.3 Entendendo o ciberespaço..... 16

CAPÍTULO II - CONFIDENCIALIDADE E SIGILO NAS RELAÇÕES DIPLOMÁTICAS E DOMÉSTICAS DO GOVERNO..... 20
2.1 Segurança e Defesa cibernética..... 20
2.2 Incidentes cibernéticos..... 23
2.3 Registros de incidentes de espionagem mundial..... 28

CAPÍTULO III – MARCO DA PROTEÇÃO CIVIL DA INTERNET..... 31
3.1 Os Direitos individuais e coletivos..... 31
3.2 A responsabilidade dos atores..... 36
3.3 Diretriz governamental..... 39

CONSIDERAÇÕES FINAIS..... 42
REFERÊNCIAS BIBLIOGRÁFICAS..... 44

INTRODUÇÃO

Este trabalho busca fazer uma abordagem sobre os crimes de internet a partir dos escândalos desencadeados pelo vazamento de dados wikileaks por Julian Assange, refletindo sobre a necessidade de se estabelecer medidas seguras para que os internautas possam transitar na rede com segurança.

A sociedade vive um novo momento histórico desencadeado pela era da informação. Trata-se na verdade de um movimento em que as relações interpessoais cada vez mais são estabelecidas através da internet, por meio de um processo em que linguagens, usos, percepções sensoriais, novas identidades formadas e trocas simbólicas encontram-se emaranhadas em rede, isto sem mencionar o aspecto econômico dessas novas relações.

Neste sentido, a sociedade dos dias atuais encara um novo processo de sociabilidade, uma nova forma de relação em que o espaço e o tempo são aspectos que demarcam a vida dos seres humanos. É um cenário em que os indivíduos se encontram diante de mecanismos de interação em que o espaço físico praticamente não existe.

Ante o exposto, ao mesmo tempo em que saboreia as maravilhas deste espaço em que a informação e as relações interpessoais se multiplicam em uma velocidade assustadora, a sociedade se depara com um dilema, qual seja, a inexistência de marcos legais que disciplinem a disputa pelo domínio desse espaço cibernético, com potencial para suscitar conflitos de proporções e consequências mais danosas à humanidade do que a própria arma nuclear.

Neste contexto é que os eventos relacionados ao ambiente cibernético ocorridos nos últimos anos mostram que há países que já vivem em uma guerra fria cibernética. Começa a se delinear um ambiente de insegurança internacional e que vem ocasionando iniciativas de sistematização de ações para contê-la em várias partes do mundo.

Portanto este estudo buscou também dimensionar o impacto do vazamento das informações secretas norte-americanas para a segurança internacional assim como

também chamar a atenção para a necessidade de transparência dos estados e suas políticas públicas direcionadas à seus cidadãos.

A metodologia utilizada para a concretização do trabalho elaborado de conclusão de curso, foi a análise bibliográfica de obras a respeito do tema escolhido, trazendo a contribuição de diversos autores e fazendo um debate teórico capaz de conduzir ao melhor entendimento da temática em estudo.

Assim, no primeiro capítulo faz-se uma abordagem sobre a história de Julian Assange assim como também apresenta um estudo mais detalhado no tocante aos crimes praticados no ambiente virtual.

O segundo capítulo apresenta uma reflexão sobre o sigilo nas relações diplomáticas do governo, apontando alguns casos de incidentes cibernéticos que se tornaram famosos no mundo inteiro.

Por sua vez, o terceiro capítulo é abordado o marco da proteção civil na internet, evidenciando a necessidade de estabelecer mecanismos legais especifico de combate ao crime cibernético apesar da existência de alguns dispositivos constitucionais que servem para dar proteção à possíveis vitimas desses crimes.

Por fim, faz-se uma releitura de todas as ideias trazidas no corpo do trabalho para apresentar a conclusão a que o estudo chegou.

CAPÍTULO I – HISTÓRIA DE JULIAN ASSANGE E A ERA DOS CRIMES DIGITAIS

1.1 Caso Julian Assange

Não faz muito tempo que diversos organismos da mídia nacional e internacional focalizaram as suas atenções para o, até então, pouco conhecido, site especializado na divulgação de arquivos secretos dos Estados Unidos da América, sobre a Guerra do Afeganistão e a Guerra do Iraque: WikiLeaks.

> No dia 04 de Outubro de 2006, foi fundado, na Suécia, o site WikiLeaks, feito sob a plataforma de MediaWiki, similar ao da Wikipédia, entretanto, seu conteúdo possui edição restrita a um seleto grupo de editores, onde se destaca o seu principal editor, o jornalista e ciberativista australiano Julian Assange, que tornou-se famoso em 2010, assim como o site WikiLeaks, com a divulgação de arquivos secretos dos Estados Unidos da América, sobre a Guerra do Afeganistão e a Guerra do Iraque, muitos estes denunciando graves violações aos direitos humanos.[1]

Observando-se o contexto dos acontecimentos de outubro de 2006, bem como a repercussão que a divulgação dos arquivos secretos americanos provocou no mundo inteiro, urge buscar entender não apenas o motivo da imprensa ter se escandalizado com a divulgação de tais informações, mas, sobretudo, o discurso que se projetou a partir de então sobre a transmissão de informações no meio digital.

Entender a importância que a polêmica adquiriu para a sociedade contemporânea parece ser tão importante quanto buscar conhecer a história do responsável por todos esses acontecimentos: o australiano Julian Assange.

> Fundador, editor e porta-voz do site WikiLeaks, o jornalista, programador e ativista da internet **Paul Julian Assange** nasceu na cidade de Townsville, na Australia, em 03 de julho de 1971. Como seus pais eram donos de uma companhia de teatro itinerante, Assange viajou por toda a Australia durante sua infância e adolescencia.
> Aos 16 anos, Assange tornou-se membro de um grupo de hackers internacionais – os *International Subversives* (Subversivos Internacionais), o que levou a Policia Federal Australiana a invadir sua casa, na cidade de Melbourne, em 1991, acusando-o de invadir computadores de várias organizações. Assange declarou-se culpado das 24 acusações que lhe foram

[1] ESSE, Luis Gustavo; GONÇALVES, José Artur Teixeira. **Wikileaks e a primeira ciberguerra da história da humanidade – uma revolução ou apenas uma manifestação sufocada**?. *In*: Âmbito Jurídico, Rio Grande, XIV, n. 94, nov 2011. Disponível em: <http://ambitojuridico.com.br/site/?artigo_id=10718&n_link=revista_artigos_leitura>. Acesso em nov. 2013.

> atribuídas, e foi libertado por bom comportamento após o pagamento de uma multa.[2]

Observa-se, portanto, que o criador do site apresenta um vasto currículo, bem como desde cedo já havia se envolvido em problemas com a polícia australiana em decorrência da invasão de computadores de organizações, coincidentemente, ou não, seria uma situação semelhante que uma década mais tarde viria fazer com que o seu nome ganhasse notoriedade.

> Julian Assange nasceu em 3 de julho de 1971 em Townsville, no estado de Queensland, no norte da Austrália. Assange foi criado por sua mãe, Christine, uma mulher criada em uma família tradicionalista de renome acadêmico, seu pai que era diretor de uma universidade local, decidiu no século 19, emigrar da Escócia para o norte da Austrália onde a família Assange estabeleceu sua vida.[3]

Em 2003, Assange ingressa na Universidade de Melbourne para concluir seus estudos em Matemática e Física, o jovem hacker acreditava que sua nova vida acadêmica o ajudaria a se distanciar das atividades as quais ele se envolveu e poderiam também proporcionar uma vida mais tranqüila, não imaginava, porém que, muito rapidamente iria desistir da vida universitária ou mesmo que rapidamente estaria trabalhando em projeto que lhe daria reconhecimento internacional alguns anos mais tarde.

> Sua participação no site WikiLeaks lhe renderam reconhecimento e consequentemente, os seguintes prêmios:
> 2008 - Index on Censorship – Concedido pelo The Economist, por promover a liberdade de expressão; 2009 - Amnesty International UK Media Awards – Concedido pela Anistia Internacional, por ter exporto ao mundo os assassinatos no Quênia; 2010 - Sam Adams Award – Concedido pela Sam Adams Associates for Integrity in Intelligence, associação de funcionários aposentados da CIA, pela integridade e ética de suas ações.
> Além dos prêmios em reconhecimento por sua atuação junto a WikiLeaks, Assange foi considerado uma das 50 figuras mais influentes de 2010, segundo a revista britânica New Statesman. Algumas comunidades da internet promovem a indicação de Assange para o Premio Nobel da Paz em 2011, por

---

[2] PACIEVITCH, Thais. **Paul Julian Assange**. In InfoEscola, 2013. Disponível em: http://www.infoescola.com/biografias/paul-julian-assange/. Acesso em 28 out. 2013.

[3] KHATCHADOURIAN, Raffi. **NO SECRETS Julian Assange's mission for total transparency**. The New Yorker, 7 de junho de 2010. Disponível em: <http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian?currentPage=all>. Acesso em 25 out. 2013.

> ter fundado o WikiLeaks.[4]

Em que pese ter ganhado reconhecimento internacional mediante os prêmios recebidos, o seu papel como figura de destaque internacional, ficou comprometido quando o mesmo se viu envolvido nas denúncias e documentos publicados no WikiLeaks, sobretudo as que têm relação com o governo americano e a Guerra do Afeganistão e que conforme já fora aqui destacado desencadearam ações de retaliação de vários governos do mundo.

Apesar do escândalo em que se envolveu, Julian Assange acabou dividindo a opinião das autoridades internacionais, isto porque:

> Se o conteúdo publicado no site WikiLeaks não agradou as mais poderosas instituições do mundo contemporâneo, por outro lado, houve pessoas de grande destaque no cenário mundial que prestou apoio e defendeu Julian Assange e o site WikiLeaks como um instrumento que visa promover a transparência e denunciar abusos, principalmente aos direitos humanos, por parte dos Estados-nacionais, como consta em inúmeras denúncias feitas pelo site, principalmente sobre as guerras no médio-oriente.[5]

Analisando-se, portanto, o contexto desses acontecimentos, inevitável enfatizar que o WikiLeaks revolucionou a história da humanidade, assim como também se constituiu como ferramenta importante de influência para a geração de instrumentos capazes de concretizar a garantia de acesso a informação e outros direitos internacionalmente reconhecidos, entretanto, sob o viés da organização institucional, “tal instrumento fere a ética nas instituições, por outro lado, prova que, no seio dessas instituições, há dissidentes que anseiam mudanças no comportamento por parte das instituições que fazem parte.”[6]

Notabiliza-se gradativamente que, o grande problema do escândalo do site WikiLeaks, surge a partir do instante em que em nome da Liberdade de Expressão, restou ameaçada a integridade, deixando como saldo um relevante prejuízo às relações

---

[4] PACIEVITCH, Thais. **Paul Julian Assange**. In InfoEscola, 2013. Disponível em: http://www.infoescola.com/biografias/paul-julian-assange/. Acesso em 28 out. 2013.
[5] PACIEVITCH, Thais. **Paul Julian Assange**. In InfoEscola, 2013. Disponível em: http://www.infoescola.com/biografias/paul-julian-assange/. Acesso em 28 out. 2013.
[6] PACIEVITCH, Thais. **Paul Julian Assange**. In InfoEscola, 2013. Disponível em: http://www.infoescola.com/biografias/paul-julian-assange/. Acesso em 28 out. 2013.

diplomáticas de muitos países, o que conseqüentemente poderá vir a "desencadear uma série de revolução ao redor do globo, o que tornaria os Estados ineficazes em garantir outros direitos estabelecidos na carta, como o próprio direito de ir e vir (art. XIII) e o direito à segurança e a vida (art. III)."[7]

Importa salientar que, tomando como referência os acontecimentos de outubro de 2006, e tantos outros escândalos virtuais que surgiram nos últimos anos, seja envolvendo personalidades famosas ou mesmo entidades diplomáticas, "o espaço cibernético constitui novo e promissor cenário para a prática de toda a sorte de atos ilícitos, incluindo o crime, o terrorismo e o contencioso bélico entre nações [...]"[8].

Portanto proceder-se-á abaixo a um estudo mais detalhado no tocante aos crimes praticados no ambiente virtual, visando oferecer uma melhor contextualização para a temática aqui proposta.

1.2 Os crimes Cibernéticos

A partir do final da década de 80, com o fluxo crescente de informações e a computadorização dos meios de tecnologia e o acesso de tais máquinas pela classe média mundial, ficou cada vez mais evidente que o ciberespaço deveria organizar regras no espaço digital para que os indivíduos que se comunicam através de meio digitais ou realizam transações, como também, as instituições, pudessem sentir-se menos ameaçados com a crescente presença, de cibercriminosos no espaço digital.

> Essa nova era tem sua melhor caracterização no surgimento da internet, que introduziu novas formas de comunicação e de troca de informações, a velocidades inimagináveis há poucos anos e suportadas por uma miríade de equipamentos e *softwares* distribuídos e operados por pessoas, empresas e governos. Formando uma complexa teia de atores, de equipamentos e de locais aos quais o homem se acostumou e com os quais interage de forma natural, ao realizar atividades cotidianas, tais como assistir à televisão ou a um filme, falar ao telefone ou corresponder-se com amigos, estudar ou fazer pesquisas em bibliotecas, conferir o extrato ou o saldo bancário, pagar tributos ou duplicatas, comprar discos ou livros. Enfim, o homem "conversa", "vai aos bancos",

[7] PACIEVITCH, Thais. **Paul Julian Assange**. In InfoEscola, 2013. Disponível em: http://www.infoescola.com/biografias/paul-julian-assange/. Acesso em 28 out. 2013.

[8] BRASIL. Desafios **estratégicos para segurança e defesa cibernética**. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

> "namora", "trabalha", "compartilha opiniões", para ficar em poucos exemplos, de forma virtual, sem necessariamente conhecer o outro a quem se dirige ou com quem interage. Sem saber por onde trafegam suas informações, expõe sua intimidade, sua privacidade, sua capacidade financeira e econômica, suas atividades profissionais, pressupondo que está seguro nesse ambiente virtual, nesse espaço cibernético.[9]

A acessibilidade digital trouxe-nos benefícios e encurtou distâncias de forma astronômica, entretanto o impacto que o avanço na área tecnológica trouxe implicações também para a área do direito. No ciberespaço, o campo do direito teve que adaptar-se para que as condutas dos utilizadores deste espaço não ferissem direitos de terceiros ou que as condutas dos mesmos não ferissem o interesse comum da população, isto é, os princípios morais e éticos como também a jurisdição vigente.[10]

> A acessibilidade a estes novos equipamentos trouxe para a sociedade diversos impactos, principalmente na seara do Direito. Antigos conceitos legais tiveram de ser reformulados, revestindo-se de uma roupagem mais moderna, de forma que pudessem se enquadrar à nova realidade. Emergiram também novas situações jurídicas, que ensejam dos profissionais do Direito tratamento diferenciado, além de conhecimentos mais específicos sobre as matérias informáticas.[11]

Existem crimes, entretanto, que já são devidamente enquadrados na legislação e jurisdição brasileira, independentemente de serem cometidos em ambiente virtual ou fora dele, como a pedofilia. A única diferença quando um crime é cometido na internet é apenas o seu meio de execução.

Ante estas considerações pode exemplificar que todo ato ilícito praticado no ambiente virtual, pode ser tipificado, ou seja, reconhecido como crime digital ou cibernético. Neste contexto observe-se, por exemplo, que o ato de expor imagens pornográficas de crianças na internet é reconhecido como ato criminoso pelo Estatuto da Criança e do Adolescente em seu art. 241, no entanto, por ser praticado em um

---

[9] BRASIL. Desafios **estratégicos para segurança e defesa cibernética**. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

[10] COLARES, Rodrigo Guimarães. **Cibercrimes: os crimes na era da informática**. Conjur, jul. 2002. Disponível em: http://www.conjur.com.br/2002-jul-26/crimes_informatica. Acesso em: 02 nov. 20013.

[11] COLARES, Rodrigo Guimarães. **Cibercrimes: os crimes na era da informática**. Conjur, jul. 2002. Disponível em: http://www.conjur.com.br/2002-jul-26/crimes_informatica. Acesso em: 02 nov. 20013.

ambiente virtual, pode ser entendido como crime cibernético.[12]

Partindo dessa perspectiva observa-se que, crimes de calúnia, difamação, furto, estelionato, favorecimento da prostituição, incitação ao crime, apologia ao crime ou criminoso e qualquer delito já enquadrado na legislação brasileira, não necessitam de legislação específica no ambiente de ciberespaço, apenas algumas alterações para se adaptarem às práticas dentro da internet.

> Dessa forma, são crimes que podem admitir sua consecução no meio cibernético: calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação ao direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, escrito ou objeto obsceno, incitação ao crime, apologia de crime ou criminoso, falsa identidade, inserção de dados falsos em sistema de informações, adulteração de dados em sistema de informações, falso testemunho, exercício arbitrário das próprias razões, jogo de azar, crime contra a segurança nacional, preconceito ou discriminação de raça-cor-etnia-etc, pedofilia, crime contra a propriedade industrial, interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software.[13]

Por outro lado, existem crimes que quando praticados, causam danos à bens e dados no campo da informática, tais como os vírus que são enviados para a máquina do usuário e que acaba danificando o bem, e que por vezes não se encontram enquadrados na jurisdição atual.

A problemática que surge aqui é que cada vez mais é crescente o número de usuários de diversas plataformas eletrônicas, todavia, é ainda mais crescente o número de indivíduos que se dedicam a encontrar os meios de burlar estas plataformas com o objetivo de acessar os computadores de modo ilegal (invasão), para desta forma, desvendar criptografia, para com isto obter acesso a senhas de cartões de crédito dentre outras atividades ilícitas.

Considerando-se o modo como estes criminosos virtuais atuam, há de se destacar que os crimes praticados pelos mesmos são bastante complexos, tendo em vista que fogem à realidade do que a nossa sociedade e até mesmo as autoridades de

---

[12] COLARES, Rodrigo Guimarães. **Cibercrimes: os crimes na era da informática**. Conjur, jul. 2002. Disponível em: http://www.conjur.com.br/2002-jul-26/crimes_informatica. Acesso em: 02 nov. 20013

[13] COLARES, Rodrigo Guimarães. **Cibercrimes: os crimes na era da informática**. Conjur, jul. 2002. Disponível em: http://www.conjur.com.br/2002-jul-26/crimes_informatica. Acesso em: 02 nov. 20013.

segurança pública estão acostumados a lidar. Isto porque, estes crimes, por vezes não se encontram tipificados, ou seja, inseridos no código penal, muito embora seja notório os danos que decorrem da ação dos cibercriminosos.

1.3 Entendendo o ciberespaço

Entender o conceito de ciberespaço requer um verdadeiro exercício de criatividade e imaginação, uma vez que, este é um espaço ou ambiente que não é visível, não se consegue apalpá-lo, muito embora saibamos que ele existe, ainda que em um lugar indefinido, desconhecido e repleto de possibilidades de interação.

A afirmação de que o ciberespaço encontra-se presente nos computadores, nas redes, desperta ainda mais a curiosidade para desvendar este ambiente, sobretudo porque, a partir desta afirmativa surge um questionamento importante: o que acontece neste "ambiente-mundo" quando as máquinas são desligadas, para onde vai? Assim, é justamente este aspecto fluido, ou seja, sem forma própria, que faz do ciberespaço um mundo virtual.

Neste contexto o ciberespaço pode ser entendido como um mundo virtual em que se encontram disponíveis para a sociedade uma multiplicidade de formas de interação e comunicação.

O conceito de ciberespaço pode ainda ser definido como:

> O ciberespaço, dispositivo de comunicação interativo e comunitário, apresenta-se como um instrumento dessa inteligência coletiva. É assim, por exemplo, que os organismos de formação profissional ou à distância desenvolvem sistemas de aprendizagem cooperativa em rede … Os pesquisadores e estudantes do mundo inteiro trocam idéias, artigos, imagens, experiências ou observações em conferências eletrônicas organizadas de acordo com interesses específicos.[14]

Cumpre ainda esclarecer que distante do que se possa imaginar, o virtual aqui, não é o oposto do real, o ciberespaço não está desconectado da realidade, ou seja:

> O ciberespaço, enfim, é uma grande máquina abstrata (conceito deleuziano), semiótica e social onde se realizam não somente trocas simbólicas, mas transações econômicas, comerciais, novas práticas comunicacionais, relações

[14] LEVY, Pierre. **Cibercultura**. Rio de Janeiro: Ed.34, 1999,p.29

> sociais, afetivas e, sobretudo, novos agenciamentos cognitivos.[15]

Todavia, a territorialização do espaço virtual, traz consigo não apenas benefícios, mas também um conjunto de aspectos negativos.

> Se, por um lado, o uso dessas modernas tecnologias computacionais e de comunicações, que caracterizam a cibernética trouxe grandes benefícios à humanidade, facilitando o trânsito de informações, a interação e a aproximação entre indivíduos, grupos sociais, políticos e econômicos e até entre nações, por outro lado, possibilitou o aparecimento de ferramentas de intrusão nesses sistemas utilizados pelas pessoas no desenvolvimento de suas atividades particulares e profissionais.[16]

Cumpre destacar que no ciberespaço as distâncias e o espaço entre os indivíduos se tornam muito menores e praticamente inexistentes. Neste ambiente as informações percorrem o mundo em fração de segundos e, portanto, o poder que uma determinada informação tem de atingir um grande número de pessoas e também de várias pessoas coletarem dados e utilizarem os mesmos para a construção deste espaço é enorme.

> O ciberespaço (que também chamarei de "rede") é o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infra-estrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo.[17]

Do mesmo modo, há de se chamar a atenção para um aspecto importante neste contexto, qual seja, o fato de que, tem se tornado evidente o uso destas informações por ciberativistas para a prática de ações contra o governo, o que representa uma grande ameaça quando se leva em conta que uma máquina utilizada por um indivíduo pode causar tanto dano às instituições do governo e terceiros, quanto uma arma ou um

---

[15] MONTEIRO, Silvana Dumont. **O que é ciberespaço**. Departamento de Ciência da Informação da Universidade Estadual de Londrina [on line] disponível em: http://departamentocienciadainformacao.blogspot.com.br/2010/05/o-que-e-o-ciberespaco.html. acesso em: 05 dez. 2013.

[16] BRASIL. Desafios **estratégicos para segurança e defesa cibernética**. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

[17] LEVY, Pierre. **Cibercultura**. Rio de Janeiro: Ed.34, 1999,p.17.

objeto real fora deste mundo virtual.[18]

Cumpre destacar que o mundo do ciberespaço é um local onde, aqueles que ali interagem uns com os outros, faz do mesmo, um espaço facilitador de formação de opiniões e que com a ampliação destes espaços e dos seus indivíduos, a comunicação e a sociabilidade entre os mesmos, torna real, a capacidade de reformulação da personalidade desses cidadãos agirem de livre e espontânea vontade, formando sua personalidade dentro da rede e agindo da maneira que julgam ser melhor.

> Esse espaço, em princípio autorregulado e autônomo, permite a troca de informações das mais variadas formas, por pessoas e equipamentos, pessoas que fazem uso de toda essa infraestrutura crítica de informações, sem muitos conhecimentos técnicos de como essa troca se processa e sem clara percepção das suas consequências, como já referenciado. À medida que a sociedade da informação vai-se estabelecendo em um país, inicia-se um processo de construção de verdadeira "nação" virtual, constituída no que se denomina de espaço cibernético.[19]

Esta grande mudança nas últimas décadas se tornou essencial para o cidadão moderno atual, isto porque, na modernidade a qual nos encontramos o cidadão consegue um poder de influência bem maior que as gerações anteriores à ele. O cidadão sai de uma posição onde ele e os outros indivíduos costumam ser expectadores e passam a buscar informações e transformar a realidade em que vivem. Há, portanto, uma integração entre a comunicação e a interatividade, resultando em melhores formas de expressão na realidade em que o indivíduo vive.

> A mediação digital remodela certas atividades cognitivas fundamentais que envolvem a linguagem, a sensibilidade, o conhecimento e a imaginação inventiva. A escrita, a leitura, a escuta, o jogo e a composição musical, a visão e a elaboração das imagens, a concepção, a perícia, o ensino e o aprendizado, reestruturados por dispositivos técnicos inéditos, estão ingressando em novas configurações sociais.[20]

Considerando que a sociedade é constituída pela técnica, Pierri Leby elabora um painel histórico, que compreende o advento da escrita, da enciclopédia e do

---

[18] LEVY, Pierre. **Cibercultura**. Rio de Janeiro: Ed.34, 1999,p.17.
[19] BRASIL. Desafios **estratégicos para segurança e defesa cibernética**. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.
[20] LEVY, Pierre. **Cibercultura**. Rio de Janeiro: Ed.34, 1999, p.17.

ciberespaço. Nesse cenário, situa a simulação como modo de conhecimento próprio da cibercultura. Amparado no conceito de inteligência coletiva, o sociólogo descortina novas formas de organização e de coordenação flexíveis, em tempo real, no ciberespaço. [21]

A sociedade em rede pode ainda ser analisada sob o aspecto da “cibercultura”, sendo, pois, este novo espaço de interações propiciado pela realidade virtual (criada a partir de uma cultura informática). Neste contexto, Pierre Lévy, ao explicar o virtual, a cultura cibernética, em que as pessoas passam pela experiência de uma nova relação espaço-tempo, utiliza a mesma analogia da “rede” para indicar a formação de uma “inteligência coletiva”.[22]

Ante esta realidade, cumpre ainda destacar que a Internet deve ser compreendida como uma rede que congrega diversos grupos de redes. E essas redes não são apenas de computadores, mas também de pessoas e de informação.

Diante deste contexto observa-se que existe uma relação entre o caso Julian Assange e os crimes digitais, no sentido de que, os atos praticados por ele foi considerado como uma ameaça à integridade, além de ser relevantemente prejudicial às relações diplomáticas de muitos países.

A diferença é que os crimes digitais, via de regra, são praticados entre os particulares ao passo que os atos praticados por Julian Assange está diretamente relacionado às relações diplomáticas que as nações possuem entre si, provocando assim danos de natureza internacional.

Nisto entende-se que, o crime praticado por Assange estaria desta forma inserido entre os crimes digitais, mas que devido o dano causado assume natureza internacional, ou seja, o dano causado pela prática do delito estaria diretamente vinculado à segurança internacional.

Neste sentido, alguns crimes já tipificados na legislação nacional e abarcados no rol de crimes cibernéticos apresentam conexão com o caso Assange, dentre os quais é possível destacar: divulgação de segredo, crime contra a segurança nacional.

---

[21] LEVY, Pierre. **Cibercultura**. Rio de Janeiro: Ed.34, 1999.
[22] LEVY, Pierre. **Cibercultura**. Rio de Janeiro: Ed.34, 1999.

CAPÍTULO II - CONFIDENCIALIDADE E SIGILO NAS RELAÇÕES DIPLOMÁTICAS E DOMÉSTICAS DO GOVERNO.

2.1 Segurança e Defesa cibernética.

Considerando o que fora até aqui exposto, é preciso destacar que a estratégia de segurança cibernética tem a missão garantir entre outros aspectos, a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações de interesse do Estado e da sociedade brasileira, aspectos da segurança institucional.

Assim é que, com o surgimento da internet comercial em meados da década de 1990, a questão da manipulação de informações e da sua segurança ganha maior ênfase, pois a grande rede e seus protocolos, especialmente a família TCP/IP, foram construídos sem muita preocupação com a confidencialidade, a integridade, a disponibilidade e a autenticidade.[23]

O TCP/IP é um grupo de protocolos de comunicação que tem como objetivo estabelecer a comunicação entre computadores que estão em rede. O que se observa é que inicialmente pouco se fez no mundo da informática para que esta comunicação pudesse ser estabelecida livre das ameaças de invasão, ou seja, as empresas não se preocuparam em desenvolver protocolos capazes de evitar que o sistema do usuário fosse invadido.

Neste sentido, durante muito tempo os usuários ficaram reféns de uma infinidade de vírus que não obstante tivessem acesso ao computador das pessoas ainda danificava a máquina e roubavam senhas, causando muitas vezes, prejuízos financeiros.

Neste contexto é importante esclarecer que:

> À semelhança do que ocorre em qualquer novo espaço aberto e pouco regulado no mundo físico, como o antigo “velho oeste”, as regiões de fronteiras ou as bordas de expansão agrícola, ainda não perfeitamente demarcadas, pessoas mal-intencionadas sempre buscam obter vantagens ilícitas ou socialmente inaceitáveis explorando a falta de regras.

[23] MANDARINO JUNIOR, Raphael. **Reflexões sobre segurança e defesa cibernética**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.40.

> Assim ocorre na internet, ou melhor, no chamado *espaço cibernético,* em que pessoas e grupos, acobertados pela distância e pelo anonimato, tentam burlar a segurança dos equipamentos e dos sistemas informatizados de qualquer empresa, governo ou indivíduo e extrair benefícios indevidos da exploração desse bem chamado *informação*.[24]

Observa-se, portanto, que o ambiente virtual configura-se como sendo um espaço sem fronteiras. Desta forma, urge chamar atenção para o fato de que uma rede comprometida pode prejudicar outras, sejam elas públicas, privadas, contíguas ou não. Neste sentido, a colaboração e a constante interação entre os mais diversos atores são essenciais para garantir um elevado nível de proteção cibernética para todos, ou seja:

> Isoladamente, nem o governo, nem a academia e nem a indústria conseguirão obter sucesso na proteção das próprias redes. São necessárias ações conjuntas entre estes setores. Portanto, constitui-se um indicativo tanto para a academia quanto para a indústria nacional visando suprir uma demanda iminente por sistemas seguros. Prevenir, identificar vulnerabilidades e preparar-se para situações de risco devem ser questões de Estado e não apenas priorização de governo.[25]

Neste sentido, a defesa cibernética diz respeito ao conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente.[26]

Em que pese não haver nenhum indício de guerra declarada entre grandes potencias mundiais atualmente, a ocorrência de ataques frequentes provocam um clima de desconfiança generalizada. Portanto, as potencias tendem a buscar informações a respeito de seus potenciais rivais, e isto acaba se tornando um fator preocupante, porque “a internet, nossa maior ferramenta de emancipação, está sendo transformada

---

[24] MANDARINO JUNIOR, Raphael. **Reflexões sobre segurança e defesa cibernética**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.40.

[25] CRUZ JUNIOR, Manoel Cesar da. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unido, Rússia e índia para os espaço virtua**l. Instituto de Pesquisa Econômica Aplicada.- Brasília : Rio de Janeiro: Ipea, 2013.

[26] BRASIL. Secretaria de Assuntos Estratégicos – SAE. Desafios estratégicos para a segurança e defesa cibernética. Brasília: SAE, 2011. Disponível em: <http://www.sae.gov.br/site/wp-content/ uploads/Seguranca_Cibernetica_web.pdf>.Acesso em 30 nov. 2013

no mais perigoso facilitador do totalitarismo que já vimos. A internet é uma ameaça à civilização humana".[27]

Este panorama faz surgir os conceitos de defesa e segurança cibernética, devendo, portanto, serem entendidos sob o aspecto de que:

> [...] a segurança cibernética preocupa-se em reduzir ou eliminar vulnerabilidades da sociedade da informação do País e suas infraestruturas críticas da informação e em fazê-las voltar à condição de normalidade em caso de ataque, enquanto a defesa cibernética se preocupa em resguardar de ameaças (externas) e reagir, se for o caso, aos ataques ao "nosso" espaço cibernético.[28]

A fragilidade do espaço cibernético faz ainda surgir o temor de que a modernização tecnológica, especialmente das infraestruturas críticas, possa ser uma porta de entrada para ataques ou sabotagem de possíveis inimigos.[29]

Neste sentido, experimenta-se hoje a nível internacional uma ambiente semelhante ao vivenciado durante a guerra fria, desta vez sob a eminente possibilidade de um ataque virtual, agravado pela dificuldade de identificar o agressor. Portanto:

> A guerra fria cibernética vivida hoje apresenta uma diferença básica do período em que vigorou a guerra fria tradicional. Naquela época, havia um efeito "demonstração" de tecnologias militares que não se vê mais – pelo menos não abertamente como era feito. Praticamente todos os ataques cibernéticos ocorridos até então são apócrifos.[30]

Não restam duvidas de que nos dias atuais uma diversidade de sistemas de informação (sistemas de gestão e controle de infraestruturas críticas, sistemas bancários e sistemas de comando e controle militares) busca gradativamente se modernizarem e alcançar o máximo de sofisticação no ciberespaço. Isso representa,

---

[27] ASSANGE, Julian *et. all*. **Cypherpunks: liberdade e o futuro da internet**. Tradução Cristina Yamagami. São Paulo: Boitempo, 2013, p. 25.

[28] MANDARINO JUNIOR, Raphael. **Reflexões sobre segurança e defesa cibernética**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.45.

[29] CLARKE, Richard; KNAKE, Robert. ***Cyber war***. New York, USA: CCCO, 2010.

[30] MANDARINO JUNIOR, Raphael. **Reflexões sobre segurança e defesa cibernética**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.45.

por um lado, um incremento alarmante das ameaças aos interesses do Estado. Por outro, e como sempre, enseja oportunidades a serem exploradas, pelos mais capazes, naturalmente.[31]

2.2 Incidentes cibernéticos

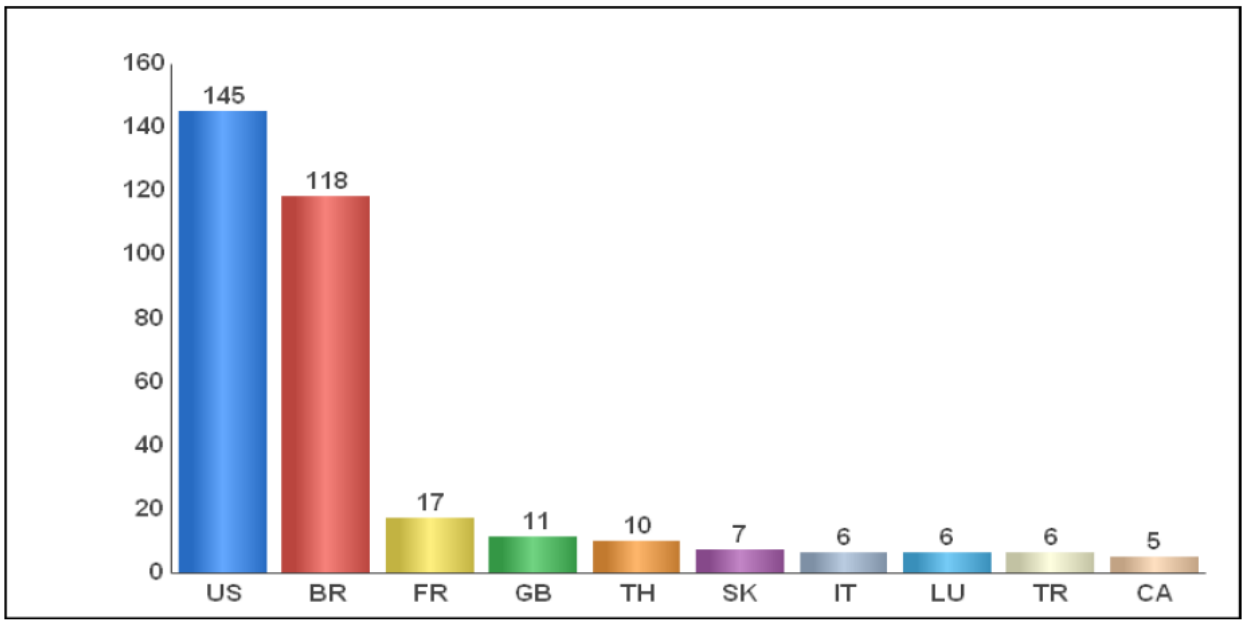
Para se ter uma ideia deste cenário é importante observar as estatísticas do Centro de Tratamento de Incidentes de Rede da Administração Pública Federal, referente ao período de 01/10/2012 a 31/12/2012 e que fazem parte do trabalho de detecção, análise e resposta a incidentes de rede desenvolvido pelo órgão.

Neste sentido o gráfico abaixo vem esclarecer o cenário que se apresenta nos dias atuais, os países destinatários das notificações de incidentes das categorias: Abuso de SMTP, Hospedagem de Malware, Redirecionamento de Malware e Hospedagem de Artefatos. Estados Unidos e Brasil continuam sendo os países destinatários do maior número de notificações de incidentes, com grande diferença para os outros países apresentados.[32]

[31] ZUCCARO, Paulo Martino. **Tendência Global em segurança e Defesa Cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.54.

[32] BRASIL. Gabinete de Segurança Institucional da Presidência da República – GSI/PR. **Estatísticas de incidentes de rede na APF**: 4º trimestre/2012. Brasil: CTIR/DSIC/GSI/PR, 2013. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2012/Estatisticas_CTIR_> Acesso em: 30 nov. 2013.

Gráfico 01: Países destinatários das notificações de incidentes



Fonte: CTIR Gov (2012)

Do ponto de vista internacional, a percepção de que as ameaças cibernéticas vêm-se expandindo exponencialmente com a Internet pode ser corroborada, entre outras formas e fontes disponíveis, pela apreciação do número de incidentes relatados ao Centro de Coordenação do Computer Emergency Readiness Team (CERT/CC), um centro de pesquisa e desenvolvimento na área de segurança de internet, financiado pelo governo norte-americano e operado pela universidade de Carnegie-Mellon.

O estudo desenvolvido por este órgão identificou que no período de 1990 a 2003, esse número elevou-se de 252 a 137.529, ou seja, houve um crescimento exponencial do número de incidentes, destacando-se, portanto, o fato de que, dos quais 55.435 ocorreram em 2003.[33]

Cumpre destacar que de modo diferente ao que ocorre na espionagem humana, física, sua correspondente cibernética é, além de muito difícil controle, tacitamente aceita, à medida que o impedimento do acesso aos conteúdos colocados em

[33] ZUCCARO, Paulo Martino. **Tendência Global em segurança e Defesa Cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.54.

computadores conectados à rede mundial é, fundamentalmente, responsabilidade daqueles que optaram por arquivá-los em um meio que pode, ao menos teoricamente, ser perscrutado de qualquer parte do mundo.

Neste sentido, a problemática que se instala aqui, encontra-se na dificuldade que as autoridades tem apresentado para imputar responsabilidades a invasões de privacidade, à apropriação de conteúdo protegido por direitos autorais ou comerciais e até mesmo de material sensível à segurança nacional, quando o alvo da ação se encontra armazenado em computadores conectados à rede mundial.[34]

> É difícil atribuir a responsabilidade de um ataque a um ou outro país. O ambiente virtual, quando utilizado de maneira inteligente, favorece o anonimato na medida em que os comandos de ataque podem ser distribuídos por servidores espalhados pelo mundo antes de chegar a seu alvo. Frequentemente, redes de países sem acordo diplomático são utilizadas para dificultar uma eventual sequência investigativa. Por esta razão, a maioria dos ataques ocorridos até hoje ainda não foram oficialmente atribuídos a algum país, uma vez que ninguém assume sua autoria.[35]

Outro fator preponderante e que deve ser levado em consideração refere-se ao fato de que:

> Não obstante as ameaças evidenciadas nas ações no ciberespaço, os países tem ainda que se preocupar, também, com as ameaças físicas à própria estrutura material que consubstancia esse espaço. Isto porque, mais de 90% do tráfego da internet passa por fibras óticas em cabos submarinos, os quais, ao longo de seus trajetos, por vezes se concentram perigosamente em alguns pontos de estrangulamento.[36]

Como exemplo do que fora mencionado acima pode-se apontar o largo de Nova Iorque, o Mar Vermelho e o Estreito de Luzon, nas Filipinas, conforme se verifica abaixo.

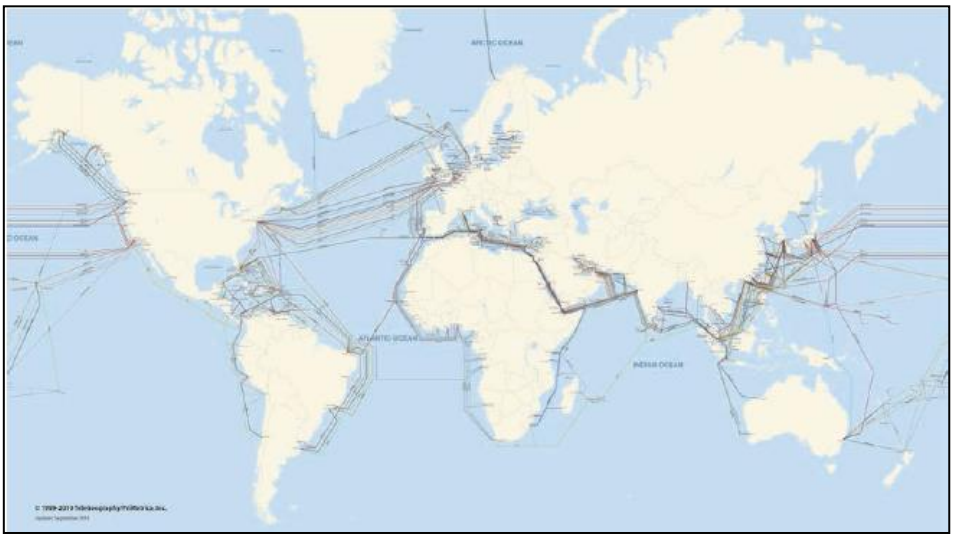
---

[34] ZUCCARO, Paulo Martino. **Tendência Global em segurança e Defesa Cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.54.

[35] CRUZ JUNIOR, Manoel Cesar da. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unido, Rússia e índia para os espaço virtua**l. Instituto de Pesquisa Econômica Aplicada.- Brasília : Rio de Janeiro: Ipea, 2013, p.10.

[36] CRUZ JUNIOR, Manoel Cesar da. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unido, Rússia e índia para os espaço virtua**l. Instituto de Pesquisa Econômica Aplicada.- Brasília : Rio de Janeiro: Ipea, 2013, p.10

Figura 01: Distribuição dos cabos Submarinos de Fibra Ótica



Fonte: WAR (2010)/Brasil(2011)

Fazendo-se uma análise bem próxima da realidade brasileira é possível trazer como exemplo, os fatos recentes em que o Brasil se viu envolvido, uma vez que apareceu em destaque nos mapas do Programa *Fairview* da norte-americana NSA.[37]

Portanto, observa-se que o Brasil assim como outros países (China, Rússia, Irã e Paquistão), surge como alvo prioritário no monitoramento de tráfego de telefonia e de dados. Tomou-se conhecimento ainda de que a capital Brasília constituiu um pedaço de uma rede composta de 16 bases direcionadas à coleta de informações. Mas não apenas o território continental brasileiro teria sido alvo: os escritórios da embaixada do Brasil em Washington e a representação brasileira junto às Nações Unidas também foram objetos das ações da NSA.[38]

O caso mencionado acima ganhou notoriedade e vem sendo objeto de muita discussão no cenário internacional, especificamente porque a partir de então o mundo tomou conhecimento do sistema de vigilância americano sobre a internet e que tem no centro dos escândalos, o ex-funcionário da Agência Nacional de Segurança dos EUA.

---

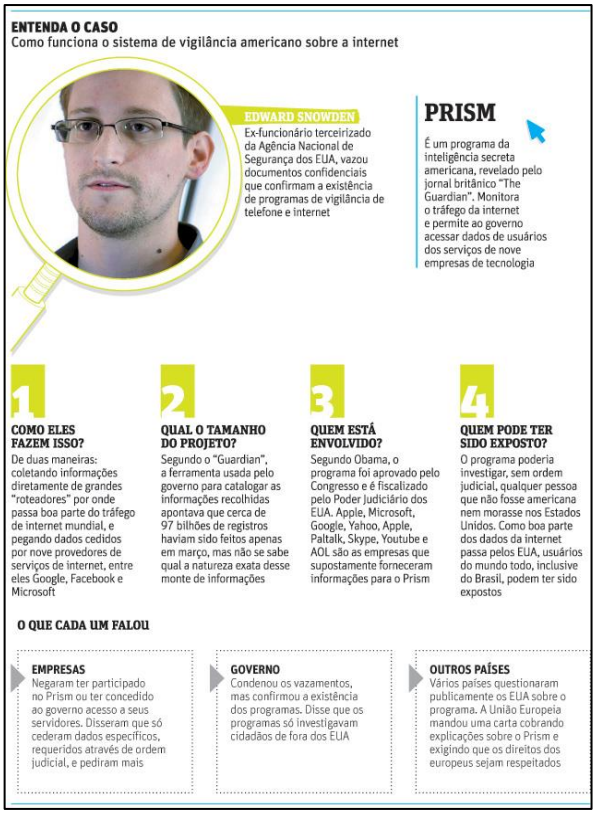
[37] GREENWALD, Glenn; KAZ, Roberto; CASADO, José. "EUA **espionaram milhões de e-mails e ligações de brasileiros**". *O Globo*, 06 jul. 2013. Disponível em: <http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934>. Acesso em 02 nov. 2013.

[38] KAZ, Roberto; CASADO, José. "NSA e CIA mantiveram em Brasília equipe para coleta de dados filtrados de satélite". *O Globo*, 08 jul. 2013. Disponível em: <http://oglobo.globo.com/mundo/nsa-cia-mantiveram-em-brasilia-equipe-para-coleta-de-dados-filtrados-de-satelite-8949723>. Acesso em 02 nov. 2013.

As revelações destacados no parágrafo anterior podem ser melhor entendidas a partir do contexto das denúncias feitas pelo ex-funcionário da NSA e da Agência Central de Inteligência (CIA, na sigla em inglês) Edward Snowden, segundo o qual o governo dos Estados Unidos tem coletado, através do programa *Prism* (entre outros), de maneira secreta e em busca de ameaças à segurança nacional, informações sobre estrangeiros no exterior através de grandes empresas como Google, Facebook, Microsoft, Apple etc.

O programa de vigilância da internet coleta dados de provedores *online*, incluindo e-mail, serviços de bate-papo, vídeos, fotos, dados armazenados, transferência de arquivos, vídeo-conferência e *log-ins*. O *Prism* é uma resposta da NSA para lidar com o crescimento explosivo das redes e mídias sociais[39]

Figura 02: Estrutura do sistema de vigilância de internet do governo americano



Fonte: Folha de São Paulo (2013)

[39] SAVAGE, Charlie; WYATT, Edward; BAKER, Peter. "**U.S. Confirms That It Gathers Online Data Overseas**". *The New York Times*, June 6, 2013. Disponível em: <http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html>. Acesso em 02 nov. 2013.

Eventos como estes fazem com que países do mundo inteiro, especificamente as grandes potencias mundiais, sintam-se reféns das tecnologias de vigilância, vez que, a eficiência destas tecnologias "[...] em comparação com o número de seres humanos, nos levarão aos poucos a nos transformar em uma sociedade de vigilância totalitarista global – e, com o termo 'totalitarista', quero dizer uma vigilância total"[40]

Evidentemente os fatos deixaram toda comunidade diplomática internacional com as atenções voltadas para a necessidade de estabelecer mecanismos de proteção contra estes atos, no entanto, acontecimentos como estes, estão longe de ser novidade no cenário mundial.

2.3 Registros de incidentes de espionagem mundial

Nos anos de 1980 espiões descobriram que era possível ter acesso a dados secretos através da internet sem que houvesse qualquer risco pessoal, iniciou-se assim, a guerra cibernética, que teve seu marco no decorrer desta década quando se iniciaram os primeiros atos de espionagem.[41]

Desde as primeiras ações de espionagem no decorrer da década de 1980 assistiu-se a uma evolução espantosa do espaço cibernético uma vez que aproximadamente 10 anos depois do início das espionagens começaram a surgir alguns casos famosos vinculados ao crime cibernético, dentre os quais é possível destacar "a invasão das intranets da GE e da rede de televisão NBC, que imobilizou vários postos de trabalho dessas gigantes e causaram milhões de dólares de prejuízos, em novembro de 1994".[42]

Cinco anos mais tarde, o satélite militar inglês Skynet foi colocado fora de circulação, a notícia de um suposto sequestro se fez saber no mundo inteiro uma vez

---

[40] ASSANGE, Julian *et. all*. **Cypherpunks: liberdade e o futuro da internet**. Tradução Cristina Yamagami. São Paulo: Boitempo, 2013, p. 81.

[41] ALMEIDA, José Eduardo Portella. **A tendência mundial para a defesa cibernética**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.88.

[42] ALMEIDA, José Eduardo Portella. **A tendência mundial para a defesa cibernética**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.88.

que na oportunidade o agência de notícia Reuters divulgou a informação sob os dizeres de que "*Hackers* supostamente tomaram o controle de um dos satélites militares da Grã-Bretanha e enviaram ameaças de chantagem".[43]

Era o ano de 1999 e outros casos de espionagem ainda estaria por vir à tona, de modo que, no ano de 2008 na intervenção armada da Rússia na Geórgia, vários computadores do governo da Geórgia foram invadidos e ficaram sob controle externo, pouco tempo antes de as tropas russas entrarem em território da Geórgia.[44]

O que ainda não se sabia neste período é que, a proteção no espaço cibernético está intrinsicamente ligada aos mecanismos de ataque existentes. Ataque e defesa (ou segurança) são, na prática, duas faces da mesma moeda.

Tornou-se quase que comum na mídia o noticiário com alertas sobre vulnerabilidade de modo que diversas reportagens podem serem ainda conferidas por meio de acesso à internet. Ante estes acontecimentos é comum ainda presenciar as autoridades, americanas em sua maioria, provocarem o maior alarde, nos EUA e, por consequência, no mundo a possibilidade de catástrofes geradas por ataques cibernéticos.[45]

Neste contexto, o primeiro grande caso foi o do vazamento de dados sigilosos da diplomacia mundial pelo *site* WikiLeaks. Quanto trabalho de coleta, análise e mesmo de diplomacia não foi perdido por falta de conhecimento sobre os perigos da internet. Um diplomata americano avaliou o escândalo como catastrófico para a diplomacia americana, o qual, no entanto, não foi mais grave graças ao teor das matérias.

De qualquer modo, a diplomacia americana ficou manchada e certamente o serviço diplomático e até a economia dos EUA vão sofrer revezes que poderiam ser evitados.

---

[43] ALMEIDA, José Eduardo Portella. **A tendência mundial para a defesa cibernética**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.88.

[44] ALMEIDA, José Eduardo Portella. **A tendência mundial para a defesa cibernética**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.88.

[45] ALMEIDA, José Eduardo Portella. **A tendência mundial para a defesa cibernética**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.88.

Outro acontecimento importante e de gravidade, ocorreu em junho de 2010 e chegou ao Brasil no fim de novembro do mesmo ano, numa breve reportagem do *Jornal Nacional*. Stuxnet foi o nome dado a um *worm* que pode ter danificado as instalações da usina nucelar iraniana de Natanz e atrasou o início das operações na usina nuclear iraniana de Bushehr. É o primeiro *worm* descoberto que espiona e reprograma sistemas industriais.

Há, portanto, um conjunto de medidas que podem ser adotadas para reagir à sensação de insegurança cibernética. Uma das mais produtivas é conscientizar a população, desde seus líderes políticos e militares até os trabalhadores das classes sociais mais baixas, sobre a possibilidade de estarem sendo alvo de levantamentos de dados, que podem comprometer indivíduos ou mesmo nações, ou de ataques, que podem ter efeitos gravíssimos.

As potências mundiais têm investido muito em informar seus povos para reconhecer a ameaça cibernética, além de preparar suas defesas para reagir a contento.

A preocupação que surge aqui é tanto pela necessidade de proteger a soberania das nações, quanto pela necessidade de garantir a todos os cidadãos do mundo a tutela de direitos universalmente protegidos.

Neste sentido, o marco da proteção da internet assume papel relevante, uma vez que através deste instrumento valioso se busca identificar os direitos individuais e coletivos relacionados ao uso da internet, em vista da necessidade de estabelecer um sistema de contenção, conforme será possível se verificar no capítulo que segue.

Portanto, o marco civil de internet servirá para apontar os caminhos necessários para estabelecer dispositivos capazes de abraçar o “ciber cidadão”, sobretudo no que compete ao tratamento de dados pessoais e proteção da privacidade no setor das comunicações eletrônicas, tendo em vista a carência de normas que trate do tema de forma abrangente.

CAPÍTULO III – MARCO DA PROTEÇÃO CIVIL DA INTERNET

3.1 Os Direitos individuais e coletivos

O Marco teórico da proteção civil da internet no Brasil encontra-se estruturado em eixos, de modo que o primeiro deles diz respeito discussão em torno da identificação dos direitos individuais e coletivos relacionados ao uso da internet uma vez que não se encontra no ordenamento jurídico nacional, qualquer dispositivo que tutele de forma explicita tais direitos.

Neste sentido, a compreensão da dignidade do homem e de seus direitos no decorrer dos tempos, tem sido, em grande parte, fruto de vários acontecimentos que resultaram em dor e sofrimento na história da humanidade. A cada grande surto de violência, os homens (não todos) se horrorizavam diante das atrocidades que viam diante de seus olhos. O remorso pelas torturas, pelas mutilações em massa, pelos massacres, pelas explorações humilhantes, fez surgir na consciência de cada um, a exigência de novas regras de uma vida mais digna para todos.[46]

Ante o exposto é que se observa a real necessidade de oferecer proteção constitucional ao cidadão brasileiro, de modo que, embora não sejam tratados de modo explicito pela Constituição, há de se observar que existem dispositivos capazes de abraçar o “ciber cidadão”, no entanto, existe uma carência por normas que trate do tema de forma abrangente.

> A intimidade e a vida privada são reconhecidas como direitos fundamentais pela nossa Constituição Federal, que assegura aos indivíduos indenização moral ou material na hipótese de sua violação. Há também previsões esparsas sobre o tema, em particular com relação à proteção de dados pessoais, no Código de Defesa do Consumidor e na Lei do *Habeas Data*. No entanto, o País não conta com um documento único que trate do tema de forma abrangente e ordenada.[47]

Neste sentido há de se destacar como exemplo deste modelo a ser implantado, a União Europeia “que editou diretivas tanto para a proteção das pessoas com relação ao

---

[46] COMPARATO, Fábio Konder. **Afirmação Histórica dos Direitos Humanos**. 7 ed. São Paulo: Saraiva, 2010.

[47] BRASIL. **Marco Regulatório Civil da internet no Brasil**. Ministério da Justiça/FGV. Disponível em: http://ccsl.ime.usp.br/files/ANEXO_9.pdf. Acesso em: 07 nov. 2013.

tratamento de seus dados pessoais (1995), quanto para o tratamento de dados pessoais e proteção da privacidade no setor das comunicações eletrônicas (2002)"[48].

Seguindo-se no rol de direitos que busca-se proteger dentro do novo contexto das interações sociais que cada vez mais se intensificam no meio cibernético, há de se chamar atenção para o direito fundamental ao sigilo da correspondência e comunicações.

> Outro direito fundamental reconhecido na Constituição Federal é o da inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e telefônicas. A própria Constituição faz ressalva a este direito, resguardando a possibilidade de não aplicação dessa proteção apenas por força de ordem judicial, para investigação criminal e instrução processual, e nos casos e na forma que a lei permitir. Destaca-se, assim, que cabe ao Poder Judiciário arbitrar a questão, a partir de balizas pré-definidas, quando houver conflito entre pretensões de garantia do direito à privacidade e ao sigilo, por um lado, e a investigação policial e a segurança pública, por outro.[49]

Surge, portanto, aqui a necessidade de se proteger tanto o direito à liberdade de expressão quanto à privacidade. No que diz respeito à privacidade, é importante destacar que:

> Uma regulamentação do ambiente digital deve levar em conta um regime sistematizado e transversal de proteção à privacidade, à vida privada, ao sigilo das comunicações e aos dados pessoais. Ainda que, para o mundo *offline*, esse contexto amplo ainda não esteja expresso em uma norma específica, a construção do marco civil da internet deve considerar a existência desses contornos gerais e, nesse panorama, assumir-se como um avanço na regulamentação da tutela dos dados pessoais, para a concretização legislativa de direitos fundamentais. Este é um dos objetivos do presente debate. [50]

O ponto fundamental nesta discussão é que conforma se pode observar este são um conjunto de direitos que se encontram devidamente tutelados na Constituição Federal, assim como na Declaração Universal dos Direitos Humanos.

Neste contexto cumpre esclarecer que após a Segunda Guerra Mundial, pelas atrocidades cometidas pelos regimes totalitários da época, houve uma maior

---

[48] BRASIL. **Marco Regulatório Civil da internet no Brasil**. Ministério da Justiça/FGV. Disponível em: http://ccsl.ime.usp.br/files/ANEXO_9.pdf. Acesso em: 07 nov. 2013.
[49] BRASIL. **Marco Regulatório Civil da internet no Brasil**. Ministério da Justiça/FGV. Disponível em: http://ccsl.ime.usp.br/files/ANEXO_9.pdf. Acesso em: 07 nov. 2013.
[50] BRASIL. **Marco Regulatório Civil da internet no Brasil**. Ministério da Justiça/FGV. Disponível em: http://ccsl.ime.usp.br/files/ANEXO_9.pdf. Acesso em: 07 nov. 2013.

conscientização em relação aos direitos inerentes ao ser humano. Verificou-se a valorização desses direitos na esfera internacional, especialmente com a Declaração Universal dos Direitos do Homem, em 1948.

Essa declaração afirmou o reconhecimento da dignidade humana e defendeu que ela é o fundamento da paz no mundo, destacou que atos bárbaros resultaram do desrespeito pelos direitos humanos e pressionou os Estados Soberanos a respeitá-los, consagrando os direitos de caráter individual, social, econômico, coletivo e difuso.[51]

O doutrinador Francisco Rezek identifica soberania como a ausência de subordinação de um Estado a qualquer autoridade que lhe seja superior, isto porque a soberania torna o Estado titular de competências, que apesar de limitadas, nenhuma outra entidade as possui igual. Essa limitação é proveniente, exatamente, da ordem jurídica internacional que coloca os países em uma postura de igualdade a fim de garantir a coordenação entre esses entes e o interesse internacional das mais diversas nações.[52]

Tal conceito começa florescer com o surgimento do Estado Moderno. O poder, que durante a Idade Média era majoritariamente da Igreja, passa a se concentrar nas mãos do rei e da burguesia, surgindo as monarquias absolutistas onde a Soberania passou a ser vista como independência do poder imperial ante qualquer outro poder e proibida qualquer interferência nas decisões internas.[53] (AGRA, 2008).

O ápice desse conceito é vislumbrado em Jean-Jacques Rousseau, em “O Contrato Social”. O principal defensor da idéia é responsável pela transferência da titularidade da soberania do monarca para o povo. Aqui a soberania confunde-se com a vontade geral dos indivíduos, onde o soberano não poderá contrariar os interesses do povo. Conforme depreendemos de suas lições:

> Digo, portanto, que, não sendo a soberania mais que o exercício da vontade geral, não pode nunca alienar-se, e o soberano, que é unicamente um ser coletivo, só por si mesmo se pode representar. É dado transmitir o poder, não a vontade.[54]

---

[51] PIOVESAN, Flávia. **Temas de Direitos Humanos**. 3 ed. São Paulo: Saraiva, 2009.
[52] REZEK, Francisco. **Curso de Direito Internacional Público.** 10 ed. São Paulo: Saraiva, 2007.
[53] AGRA, Walber de Moura. **Curso de Direito Constitucional**. 4 ed. Rio de Janeiro: Forense, 2008.
[54] ROUSSEAU, Jean-Jacques. **O Contrato Social**. Tradutor: Pietro Nassetti. São Paulo: Martin Claret, 2009, p.36.

Segundo Walber Agra são características da soberania: a unicidade (num mesmo Estado somente há uma soberania); indivisibilidade (não é fragmentável e se aplica em todo o território nacional); inalienabilidade (não pode ser mitigada ou delegada a outro Estado) e imprescritibilidade (perdura enquanto o Estado existir).[55]

Após a verificação desses conceitos e das características é mister entender como se deu a sua relativização em função da violação dos direitos humanos.

Durante a Segunda Guerra Mundial, o mundo assistiu a momentos de horror marcados pelas atrocidades cometidas pelo Nazismo (legitimado pelo Estado e pela legislação nacional) e pelo desrespeito à pessoa. Contudo, durante o Pós-Guerra, como resposta a essa crueldade, surgiu na ordem internacional uma perspectiva de reconstrução dos direitos humanos, conforme depreendemos da leitura de Flávia Piovesan:

> [...] no momento em que os seres humanos se tornam supérfluos e descartáveis, no momento em que vige a lógica da destruição, em que é cruelmente abolido o valor da pessoa humana, torna-se necessária a reconstrução dos direitos humanos, como paradigma ético capaz de restaurar a lógica do razoável... Se a Segunda Guerra significou a ruptura com os direitos humanos, o Pós-Guerra deveria significar a sua reconstrução.[56]

Começa a ser delineado o sistema normativo internacional de direitos humanos que protege os direitos fundamentais e limita o poder do Estado. Fortalece-se a idéia de que essa proteção não é apenas de competência do Estado interno, mas pela sua relevância, torna-se de interesse internacional.

Segundo Flávia Piovesan, duas consequências surgem dessa nova concepção de direitos humanos: A primeira é a *relativização* da noção de absoluta *soberania* estatal, vez que os Estados poderão ser responsabilizados em função da violação aos direitos humanos; e a segunda é a consolidação da ideia de que o indivíduo é sujeito de direito e como tal deve ter garantidos direitos na esfera internacional.[57] Em outras palavras, subentende-se que a forma como o Estado trata seus cidadãos não é apenas

---

[55] AGRA, Walber de Moura. **Curso de Direito Constitucional**. 4 ed. Rio de Janeiro: Forense, 2008.
[56] PIOVESAN, Flávia. **Direitos Humanos e Justiça Internacional**. 1 ed. São Paulo: Saraiva, 2007, p.9.
[57] PIOVESAN, Flávia. **Direitos Humanos e Justiça Internacional**. 1 ed. São Paulo: Saraiva, 2007, p.9.

um problema doméstico, mas merece uma tutela internacional. Corroeu-se, desta forma, a competência da soberania dos governantes em matéria de direitos humanos.

Outro ponto de relevo é o fato de que a liberdade de expressão tem um direito que lhe complementa, no destinatário da comunicação: a liberdade de receber e acessar informações. Também aqui, o direito à não discriminação é um fator importante para o pleno exercício de direitos individuais.

> Uma questão ainda não adequadamente discutida diz respeito ao acesso anônimo. Se o exercício da liberdade de expressão implica responsabilização pelo teor da comunicação emitida, o mesmo não é necessariamente verdadeiro com relação ao direito de acesso. Formas de identificação que impusessem, *a priori*, um monitoramento do conteúdo das comunicações recebidas ou emitidas feririam frontalmente os direitos à intimidade e privacidade.[58]

O direito de acesso à internet pode ser entendido como um desdobramento dos direitos fundamentais de expressão e de comunicação, em seus âmbitos de acesso à informação e de livre manifestação e formação do pensamento. É ainda condição para o pleno exercício da democracia, por meio do acesso a serviços de governo eletrônico e da possibilidade de interação que pode ser estabelecida com representantes políticos.[59]

Entendido como um direito fundamental, o acesso à internet não corresponde apenas à navegação, mas também à produção de conteúdo, seja pelo uso de ferramentas online, incluindo aí as chamadas redes sociais; seja pela intervenção nos processos comunicativos, por meio de comentários ou respostas a conteúdos prévios.[60]

Apresentado de forma sucinta esta rol de direitos constitucionais que podem ser aplicados no contexto da proteção aos direitos dos usuários do ciberespaço, é preciso destacar que um aprofundamento do tema não se faz pertinente neste momento, tendo em vista que o que se quer aqui é chamar atenção para esta necessidade premente de proteger juridicamente a sociedade virtual, tanto em nível nacional quanto internacional.

Assim no campo constitucional a proteção deste direitos se torna importante

---

[58] BRASIL. **Marco Regulatório Civil da internet no Brasil**. Ministério da Justiça/FGV. Disponível em: http://ccsl.ime.usp.br/files/ANEXO_9.pdf. Acesso em: 07 nov. 2013.
[59] BRASIL. **Marco Regulatório Civil da internet no Brasil**. Ministério da Justiça/FGV. Disponível em: http://ccsl.ime.usp.br/files/ANEXO_9.pdf. Acesso em: 07 nov. 2013.
[60] BRASIL. **Marco Regulatório Civil da internet no Brasil**. Ministério da Justiça/FGV. Disponível em: http://ccsl.ime.usp.br/files/ANEXO_9.pdf. Acesso em: 07 nov. 2013.

porque estaria de certa forma inseridos no rol daqueles classificados como de segunda geração, haja vista que, estes envolvem os direitos coletivos, culturais e econômicos, havendo uma restrição da atuação do Estado na intervenção da economia e na capacidade de organização dos entes não estatais.[61]

Este rol de direitos se apresentam importantes, sobretudo, porque, essa geração é constituída pelos direitos econômicos, sociais e culturais com a finalidade de obrigar o Estado a satisfazer as necessidades da coletividade, compreendendo o direito ao trabalho, à habitação, à saúde, educação e inclusive o lazer. Assim, podem referir os direitos de segunda geração como as liberdades sociais, pois o Estado tem a obrigação de proporcionar o bem estar da sociedade.[62]

3.2 A responsabilidade dos atores

O segundo eixo a ser discutido diz respeito as possibilidades de responsabilização dos indivíduos que são responsáveis pela viabilização do processo de comunicação na internet. Aqui estão incluídos os provedores de acesso, de conteúdo, de serviços, de aplicativos, de hospedagem, ou mesmo os usuários em sua condição de criadores de conteúdos criativos e participantes ativos de processos de comunicação em rede.[63]

Esta discussão é relevante, porque, em que pese a possibilidade de aplicação das normas de cunho constitucional, o que se observa, hoje é uma certa dificuldade no que compete á responsabilização dos intermediários de acesso à internet.[64]

Ainda não existe no Brasil uma legislação específica que trate da responsabilidade daqueles que prestam serviços de acesso à rede ou que prestam serviços a partir dela (provedores de acesso, conteúdo, aplicativos, hospedagem, etc.).

---

[61] MARRONI, Fernanda. **As Dimensões de Direitos Fundamentais**. 2011. Disponível em: <http://ww3.lfg.com.br/public_html/article.php?story=2011062115424915&mode=print>. Acesso em: 08 de outubro de 2012.

[62] MARRONI, Fernanda. **As Dimensões de Direitos Fundamentais**. 2011. Disponível em: <http://ww3.lfg.com.br/public_html/article.php?story=2011062115424915&mode=print>. Acesso em: 08 de outubro de 2012.

[63] BRASIL. **Marco Regulatório Civil da internet no Brasil**. Ministério da Justiça/FGV. Disponível em: http://ccsl.ime.usp.br/files/ANEXO_9.pdf. Acesso em: 07 nov. 2013.

[64] BRASIL. **Marco Regulatório Civil da internet no Brasil**. Ministério da Justiça/FGV. Disponível em: http://ccsl.ime.usp.br/files/ANEXO_9.pdf. Acesso em: 07 nov. 2013.

Com isso, prevalecem dúvidas sobre o regime de responsabilidade aplicável a estes provedores.

> Na ausência de legislação específica, a maior parte das decisões judiciais tem aplicado o regime de responsabilidade objetiva aos provedores de serviços na internet. Os fundamentos para isso estão tanto no Código do Consumidor quanto no Código Civil (art 927, p. único). A diferença entre responsabilidade objetiva e responsabilidade subjetiva consiste no fato de que, na responsabilidade objetiva, basta que se prove a existência de um dano e uma relação de causa e efeito. Na subjetiva, é necessário também a existência de uma conduta culposa do agente, que consiste em uma ação ou omissão voluntária, negligência ou imprudência.[65]

Partindo-se da premissa de que o ordenamento jurídico pátrio é responsável pela tutela dos direitos, sendo este o principal objetivo da ordem jurídica, tem-se verificado que a ordem jurídica tutela as condutas lícitas praticadas pelo homem e sanciona aquelas que são violadoras dos deveres jurídicos.

Neste sentido é a lição de Cavalieri Filho:

> O principal objetivo da ordem jurídica, afirmou o grande San Tiago Dantas, é proteger o lícito e reprimir o ilícito. Vale dizer: ao mesmo tempo em que ela se empenha em tutelar a atividade do homem que se comporta de acordo com o Direito, reprime a conduta daquele que o contraria[66]

Logo, com a finalidade de se garantir o objetivo almejado pelo ordenamento pátrio, a ordem jurídica prescreve deveres, por meio de enunciados gerais, para todos os cidadãos, estes enunciados são uma espécie de deveres que na verdade correspondem a verdadeiros direitos, os quais de acordo com a sua natureza, podem constituir direitos positivos (de dar ou fazer) ou negativos (de não fazer ou tolerar alguma coisa).[67]

Do mesmo modo, existem direitos considerados absolutos, ou seja, aqueles que atingem a todos indistintamente, e relativos destinados a determinada pessoa ou grupo de pessoas.[68]

---

[65] BRASIL. **Marco Regulatório Civil da internet no Brasil**. Ministério da Justiça/FGV. Disponível em: http://ccsl.ime.usp.br/files/ANEXO_9.pdf. Acesso em: 07 nov. 2013.
[66] CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 7ª ed. São Paulo: Atlas, 2007, p.1.
[67] CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 7ª ed. São Paulo: Atlas, 2007, p.1.
[68] CAVALIERI FILHO, Sergio. Programa de responsabilidade civil. 7ª ed. São Paulo: Atlas, 2007, p.1.

Ante o exposto, pode-se concluir pela existência de um dever jurídico, que vincula a todos, visando-se a uma melhor convivência social, correspondendo esses deveres, a verdadeiros comandos legais que impõe obrigações a toda a coletividade.

Neste sentido, é preciso esclarecer melhor o conceito de dever jurídico:

> Entende-se, assim por dever jurídico a conduta externa de uma pessoa imposta pelo direito positivo por exigência da convivência social. Não se trata de simples conselho, advertência ou recomendação, mas de uma ordem ou comando dirigido à inteligência e a vontade dos indivíduos, de sorte que impor deveres jurídicos importa criar obrigações[69].

Neste momento cumpre trazer a abordagem da noção de Responsabilidade Civil, condicionada à violação de um dever jurídico originário, que em ocorrendo, acarreta dano a outrem, gerando um novo dever jurídico, qual seja, o de reparar o dano causado, pela conduta do agente violador do direito de outrem.[70]

Esse novo dever violado é o chamado de “dever jurídico sucessivo, responsável pela noção que se tem nos dias atuais a cerca do que seja a Responsabilidade Civil”.[71]

Diante do exposto, urge que o governo busque saídas urgentes para que o Estado não se veja inerte diante dos inúmeros casos de violação de direitos que surgem no meio virtual (crimes cibernéticos), ofertando ao cidadão a sensação de segurança também na sociedade virtual, que é um ambiente internacionalmente constituído.

Ante o exposto, há de se observar que no que diz respeito à responsabilidade civil, surge uma problemática importante a ser analisada, tendo em vista que na aplicação da responsabilidade objetiva não leva em conta a dinâmica da internet como espaço de colaboração.

Neste sentido:

> Expor os provedores a um regime de responsabilidade civil tão amplo significa exigir de tais provedores um controle *a priori* das atividades dos usuários, para que não sejam responsabilizados. Isto aumenta os custos relacionados ao serviço e gera prejuízo à inovação. A insegurança com relação ao resultado de eventuais ações judiciais decorrentes de atos praticados por terceiros

[69] CAVALIERI FILHO, Sergio. Programa de responsabilidade civil. 7ª ed. São Paulo: Atlas, 2007, pp.1-2.
[70] CAVALIERI FILHO, Sergio. Programa de responsabilidade civil. 7ª ed. São Paulo: Atlas, 2007, p.2
[71] CAVALIERI FILHO, Sergio. Programa de responsabilidade civil. 7ª ed. São Paulo: Atlas, 2007, pp.1-2

> desincentiva o surgimento de novos serviços *online*, que não têm como avaliar com clareza a extensão do risco jurídico incorrido.[72]

3.3 Diretriz governamental

O terceiro eixo a ser discutido aponta para as diretrizes governamentais que possam servir de referência para a formulação de políticas públicas e para a posterior regulamentação em nível infralegal de aspectos relacionados à internet. No que compete a este eixo é importante destacar que existe diretriz quanto ao tema, necessitando apenas de atualização. Assim, tanto a Lei Geral das Telecomunicações quanto a Política Nacional de Informática, necessitam buscar novos valores resultantes deste contexto que mereçam ser alçados à condição de princípios para a atuação governamental.

Neste contexto, "é papel do Estado proteger suas infra-instrutoras críticas e, consequentemente, o espaço cibernético e a infraestrutura crítica de informação que a suportam, a fim de criar condições para o desenvolvimento sustentável do país"[73].

A principal dificuldade que se apresenta para que o estado possa garantir a efetividade deste eixo de discussão, O mundo da cultura digital é munido de várias portas de entrada e de vários caminhos para navegação. Esse feixe crescente mostra complexidade de um grau quase improvável, considerando os incontáveis atores que utilizam a rede para os mais variados propósitos, e com as mais diversas ferramentas.[74]

Assim, é que o marco civil da internet busca atender alguns princípios específicos:

Liberdade, privacidade e direitos humanos: O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática.

---

[72] BRASIL. **Marco Regulatório Civil da internet no Brasil**. Ministério da Justiça/FGV. Disponível em: http://ccsl.ime.usp.br/files/ANEXO_9.pdf. Acesso em: 07 nov. 2013.

[73] RIBEIRO, Sérgio Luis. **Estratégia de proteção da infra-estrutura crítica de informação e defesa cibernética nacional**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.145.

[74] BRASIL. **Marco Regulatório Civil da internet no Brasil**. Ministério da Justiça/FGV. Disponível em: http://ccsl.ime.usp.br/files/ANEXO_9.pdf. Acesso em: 07 nov. 2013.

Governança democrática e colaborativa: A governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva.

Universalidade: O acesso à Internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos.

Diversidade: A diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores.

Inovação: A governança da Internet deve promover a contínua evolução e ampla difusão de novas tecnologias e modelos de uso e acesso.

Neutralidade da rede: Filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento.

Inimputabilidade da rede: O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos.

Funcionalidade, segurança e estabilidade: A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.

Padronização e interoperabilidade: A Internet deve basear-se em padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento.

Ambiente legal e regulatório: O ambiente legal e regulatório deve preservar a dinâmica da Internet como espaço de colaboração.

Importa destacar que estes princípios tem a finalidade de conscientizar a sociedade em geral e de modo especial de que a disseminação das redes de informação, a integração entre diferentes infraestruturas e a interdependência cada vez maior resultam em algumas consequências que não podem ser negligenciadas.

Uma delas é que as vulnerabilidades em infraestruturas críticas tendem a crescer, o que tem tornado os problemas cada vez mais complexos. Outra consequência é que uma interrupção pode se propagar de uma rede para outra, ocasionando o efeito cascata de problemas, tornando indisponível um ou mais serviços.

> Assim, uma estratégia de proteção da infraestrutura crítica de informação e defesa cibernética deve permitir ao governo criar organismos e estratégias para agir de forma preventiva e também para minimizar o impacto provocado pelos eventos e sinistros, incluindo os consequentes transtornos na demora do restabelecimento dos serviços para uma população atingida. Além disso, o sistema deve prover informações e indicadores capazes de gerar subsídios para a formulação e constante evolução de estratégias, leis, normas e regulamentos.

Conscientes da importância de garantir a segurança no espaço cibernético, muitos países vêm investindo em planos estratégicos para mitigar, gerir e executar as ações necessárias para retomar a normalidade após uma situação de emergência provocada por catástrofe natural (como terremoto, furacão e inundação) ou ainda intencional (terrorismo e ataque cibernético, por exemplo).

CONSIDERAÇÕES FINAIS

A internet é uma ferramenta e, por si só, não garante o desenvolvimento social, a intensificação da democracia ou a promoção de justiça social. Nesse sentido, o dever estatal da educação deve abarcar o uso da internet como ferramenta de exercício de cidadania e promoção da cultura.

Essa capacitação deve primar não apenas pela transmissão de conteúdos, mas por uma construção do pensamento crítico e de saberes adaptáveis. A internet muda de forma veloz, e a aquisição de informações estáticas contribui pouco para um cenário de desenvolvimento da cultura digital. Os usuários devem ser estimulados e capacitados a descobrir novas formas de se relacionar com a rede, de acordo com sua própria evolução; bem como ser capacitados a desenvolver novos usos por conta própria.

Dessa forma, este trabalho buscou apresentar contribuições para o combate aos crimes virtuais fazendo um estudo dos crimes cibernéticos a partir dos acontecimentos que desencadearam a reflexão sobre a necessidade de proteção internacional contra a espionagem virtual e outros delitos: o caso de Julian Assange.

Portanto, a realização deste estudo possibilitou-nos entender que a fragilidade do espaço cibernético faz ainda surgir o temor de que a modernização tecnológica, especialmente das infraestruturas críticas, possa ser uma porta de entrada para ataques ou sabotagem de possíveis inimigos.

Do mesmo modo observou-se ainda que a acessibilidade digital trouxe-nos benefícios e encurtou distâncias de forma astronômica, entretanto o impacto que o avanço na área tecnológica trouxe implicações também para a área do direito. No ciberespaço, o campo do direito teve que adaptar-se para que as condutas dos utilizadores deste espaço não ferissem direitos de terceiros ou que as condutas dos mesmos não ferissem o interesse comum da população.

Outrossim, os crimes que os internautas acabam cometendo online tornam-se bastante complexos se analisarmos que: estes crimes não são propagados na realidade a qual estamos acostumados e estes delitos por vezes não são especificados no código penal, entretanto, as infrações sociais que estes cibercriminosos praticam dentro da rede causam danos reais àqueles que por ali ‘transitam’ porque muitas vezes

os danos vão além de problemas relacionados às máquinas, estes crimes que os indivíduos no ciberespaço cometem, que vão desde, calúnia, estelionato, difamação, clonagem de cartão de crédito e etc., causam danos graves fora da realidade virtual a qual os cidadãos se encontram.

Assim este é um fator importante no contexto da discussão que se buscou estabelecer neste trabalho. Portanto, conclui-se que o caso wikileaks, não obstante tenha sido um escândalo diplomático, quando observado por outro ângulo promoveu a discussão em nível internacional, da necessidade dos governos voltarem suas atenções também para as políticas de segurança e prevenção no meio virtual.

Desta forma, em que pese a lei de crimes cibernéticos já ser um realidade no cenário jurídico brasileiro, faz necessário que se busquem mecanismos capazes dar efetividade à mesma, tendo em vista que os ciberespaços deixam os usuário muito vulnerável a este tipo de delito.

Assim, a criação de delegacias especializadas seria uma alternativa importante, tendo em vista a complexidade que envolve estes crimes, conforme ficou demonstrado neste trabalho. Faz-se ainda necessário investimento em tecnologia, uma vez que o espaço cibernético é dinâmico, ou seja, encontra-se em constante aperfeiçoamento e modificação, ante as novas tecnologias que surgem constantemente.

REFERENCIAS BIBLIOGRÁFICAS

AGRA, Walber de Moura. **Curso de Direito Constitucional**. 4 ed. Rio de Janeiro: Forense, 2008.

ALMEIDA, José Eduardo Portella. **A tendência mundial para a defesa cibernética**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.88.

ASSANGE, Julian *et. all*. **Cypherpunks: liberdade e o futuro da internet**. Tradução Cristina Yamagami. São Paulo: Boitempo, 2013, p. 25.

BRASIL. **Desafios estratégicos para segurança e defesa cibernética**. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

BRASIL. Secretaria de Assuntos Estratégicos – SAE. Desafios estratégicos para a segurança e defesa cibernética. Brasília: SAE, 2011. Disponível em: <http://www.sae.gov.br/site/wp-content/ uploads/Seguranca_Cibernetica_web.pdf>.Acesso em 30 nov. 2013

BRASIL. Gabinete de Segurança Institucional da Presidência da República – GSI/PR. **Estatísticas de incidentes de rede na APF**: 4º trimestre/2012. Brasil: CTIR/DSIC/GSI/PR, 2013. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2012/Estatisticas_CTIR_> Acesso em: 30 nov. 2013.

BRASIL. **Marco Regulatório Civil da internet no Brasil**. Ministério da Justiça/FGV. Disponível em: http://ccsl.ime.usp.br/files/ANEXO_9.pdf. Acesso em: 07 nov. 2013.

CAVALIERI FILHO, Sergio. Programa de responsabilidade civil. 7ª ed. São Paulo: Atlas, 2007, p.1.

CLARKE, Richard; KNAKE, Robert. ***Cyber war***. New York, USA: CCCO, 2010.

COLARES, Rodrigo Guimarães. **Cibercrimes: os crimes na era da informática**. Conjur, jul. 2002. Disponível em: http://www.conjur.com.br/2002-jul-26/crimes_informatica. Acesso em: 02 nov. 20013.

COMPARATO, Fábio Konder. **Afirmação Histórica dos Direitos Humanos**. 7 ed. São Paulo: Saraiva, 2010.

CRUZ JUNIOR, Manoel Cesar da. **A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unido, Rússia e índia para os espaço virtua**l. Instituto de Pesquisa Econômica Aplicada.- Brasília : Rio de Janeiro: Ipea, 2013.

ESSE, Luis Gustavo; GONÇALVES, José Artur Teixeira. **Wikileaks e a primeira ciberguerra da história da humanidade – uma revolução ou apenas uma manifestação sufocada**?. *In*: Âmbito Jurídico, Rio Grande, XIV, n. 94, nov 2011. Disponível em: <http://ambitojuridico.com.br/site/?artigo_id=10718&n_link=revista_artigos_leitura>. Acesso em nov. 2013.

GREENWALD, Glenn; KAZ, Roberto; CASADO, José. "EUA **espionaram milhões de e-mails e ligações de brasileiros**". *O Globo*, 06 jul. 2013. Disponível em: <http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934>. Acesso em 02 nov. 2013.

KAZ, Roberto; CASADO, José. "NSA e CIA mantiveram em Brasília equipe para coleta de dados filtrados de satélite". *O Globo*, 08 jul. 2013. Disponível em: <http://oglobo.globo.com/mundo/nsa-cia-mantiveram-em-brasilia-equipe-para-coleta-de-dados-filtrados-de-satelite-8949723>. Acesso em 02 nov. 2013.

KHATCHADOURIAN, Raffi. **NO SECRETS Julian Assange's mission for total transparency**. The New Yorker, 7 de junho de 2010. Disponível em: <http://www.newyorker.com/reporting/2010/06/07/100607fa_fact_khatchadourian?currentPage=all>. Acesso em 25 out. 2013.

LEVY, Pierre. **Cibercultura**. Rio de Janeiro: Ed.34, 1999,p.29

MANDARINO JUNIOR, Raphael. **Reflexões sobre segurança e defesa cibernética**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.40.

MARRONI, Fernanda. **As Dimensões de Direitos Fundamentais**. 2011. Disponível em: <http://ww3.lfg.com.br/public_html/article.php?story=20110621154249 15&mode=print>. Acesso em: 08 de outubro de 2012

MAZZUOLI, Valério de Oliveira. **Curso de Direito Internacional Público**. 2 ed. São Paulo: Revista dos Tribunais, 2007.

MONTEIRO, Silvana Dumont. **O que é ciberespaço**. Departamento de Ciência da Informação da Universidade Estadual de Londrina [on line]. disponível em: http://departamentocienciadainformacao.blogspot.com.br/2010/05/o-que-e-o-ciberespaco.html. acesso em: 05 dez. 2013.

PACIEVITCH, Thais. **Paul Julian Assange**. In InfoEscola, 2013. Disponível em: http://www.infoescola.com/biografias/paul-julian-assange/. Acesso em 28 out. 2013.

PIOVESAN, Flávia. **Temas de Direitos Humanos**. 3 ed. São Paulo: Saraiva, 2009.

REZEK, Francisco. **Curso de Direito Internacional Público.** 10 ed. São Paulo: Saraiva, 2007.

ROUSSEAU, Jean-Jacques. **O Contrato Social**. Tradutor: Pietro Nassetti. São Paulo: Martin Claret, 2009.

SAVAGE, Charlie; WYATT, Edward; BAKER, Peter. "**U.S. Confirms That It Gathers Online Data Overseas**". *The New York Times*, June 6, 2013. Disponível em: <http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html>. Acesso em 02 nov. 2013.

ZUCCARO, Paulo Martino. **Tendência Global em segurança e Defesa Cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço**. In BRASIL. Desafios estratégicos para segurança e defesa cibernética. [org.] Otávio Santana Rêgo Barros, Ulisses de Mesquita Gomes, Whitney Lacerda de Freitas. – Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011,p.54.