CENTRO ESTADUAL DE EDUCAÇÃO TECNOLOGICA

PAULA SOUZA

ESCOLA TÉCNICA JORGE STREET

CLASSE DESCENTRALIZADA

ESCOLA ESTADUAL "MARIA TRUJILO TORLONI"

TÉCNICO EM SERVIÇOS JURÍDICOS

Denise Alencar de Paula

Eduarda Dantas Piotroski

Maria Carolina de Oliveira Prates

ESPIONAGEM GLOBAL

São Caetano do Sul / SP

2015

ESPIONAGEM GLOBAL

Trabalho de Conclusão de Curso apresentado ao curso técnico em Serviços Jurídicos da Etec Jorge Street, orientado pelo Prof. Waldir Gomes Magalhães como requisito parcial para obtenção do título de técnico em Serviços Jurídicos.

São Caetano do Sul

2015

"O governo dos Estados Unidos aperfeiçoou uma capacidade tecnológica que nos permite monitorar as mensagens transmitidas pelo ar (...). A qualquer momento, ela pode ser voltada contra a população, e a capacidade de vigiar tudo - conversas telefônicas, telegramas, qualquer coisa...".

Senador Frank Church, presidente do Comitê Especial do Senado para Estudar Operações do Governo.

Relacionadas a atividades de Inteligência, 1975.

RESUMO

“Em nome da segurança, o Estado se torna onipresente e passa a vigiar a todos. Nada acontece sem que se saiba, ninguém consegue escapar da vigilância

constante.” Em novembro de 2010, informações confidenciais dos Estados Unidos foram divulgadas por célebres jornais mundiais, assim o mundo todo ficou sabendo que o país tem acesso ás comunicações eletrônicas de diversos países inclusive do Brasil, tendo interceptado ligações da atual presidente Dilma Roussef atravéz do programa Echelon que é capaz de coletar mais de três milhões de mensagens por dia por meio de palavras chave que interesse o governo. Tais documentos foram recolidas por um ex-analista de sitema da Agência de Segurança Nacional (NSA) durante seu tempo de trabalho na instituição. Edward Snowden por todo o seu tempo de trabalho coletou dados para formar seu dossiê o qual quando completo compartilhou com o jornalista Glenn Greenwald que o publicou em diversas seções no jornal britânico The Guardian. O que não se sabia é que anteriormente em 2001 o Parlamento Europeu aprovou uma resolução denunciando a rede de espionagem porém logo foi abafada com ataque ás Torres Gêmeas no dia 11/09/2001 (onze do nove de dois mil e um), dando assim argumento para que os Estados Unidos continuar vigiando em prol da segurança de sua população, e ainda mais colocou em vigor a Lei Patriota a qual permite a vigilância a outros países ou pessoas suspeitas de terrorismo. Interferindo diretamente no Brasil tanto economicamente quanto politicamente, o direito a privacidade está disposto principalmente no 5°; inciso X da Constituição Federal – “são invioláveis a intimidade, a vida privada, a honra e as imagens das pessoas, assegurando o direito a indenização pelo dano material pelo dano material ou moral decorrente de sua violação.” Além disso feriu a declaração da ONU (Organização das Nações Unidas), “o acesso à internet como direito fundamental do ser humano, por promover a liberdade de expressão e o acesso de direitos civis como cultura e a educação.”

Palavras-chave: Espionagem , NSA, EUA, Brasil, Edward.

ABSTRACT

"In the name of security, the State becomes ubiquitous and watching everyone. Nothing happens without the record, no one can escape the constant

surveillance. "In November 2010, the United States classified information were disclosed by renowned world newspapers, so the world learned that the country has access to electronic communications from several countries including Brazil, having intercepted calls from current President Dilma Rousseff through Echelon program that is able to collect more than three million messages per day through key words that interest the Government. Such documents were collected by a system of ex-National Security Agency (NSA) during their work time at the institution. Edward Snowden throughout your working time collected data to form your dossier which when complete shared with journalist Glenn Greenwald who published it in several sections in the British newspaper The Guardian. What you don't know is that earlier in 2001 the European Parliament adopted a resolution denouncing the spy network but was soon drowned out with ACE attack twin towers the day 9/11/2001 (eleven of nine two thousand and one), thus giving argument for the United States keep watch for the safety of its population, and even more put into force the Patriot Act which allows the monitoring to other countries or persons suspected of terrorism. Interfering directly in Brazil both economically as politically, the right to privacy are you willing mainly in 5°; Item X of the Federal Constitution – "are inviolable intimacy, private life, honor and the images of people, ensuring the right to compensation for material damage or moral, arising out of your violation." Additionally hurt the UN Declaration (United Nations), "the internet access as a fundamental right of the human being, by promoting freedom of expression and civil rights such as access to culture and education."

Keywords: Spying, NSA, EUA, Brazil, Edward.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

O presente trabalho tem por principal objetivo apontar como a espionagem global pode interferir na privacidade e liberdade de cada cidadão, uma vez que as mesmas são frequentemente ameaçadas. Identificar os principais transtornos que foram e podem ser gerados por conta da espionagem, como a violação da privacidade de cada nação fere os princípios de não intervenção à soberania da mesma e identificar as leis internacionais que regem a confidencialidade entre países. Neste trabalho, visa-se alertar os cidadãos sobre seus direitos à privacidade, demonstrando os países que estão os violando, usando como justificativa a proteção contra atentados.

Pretende-se mostrar porque cada Estado deve ser mais transparente com seus cidadãos os conscientizando de seus direitos e mais opaco aos olhares de outros países.

Violar a privacidade de cada cidadão não é apenas um problema social, mas também político e econômico do qual o Brasil se destaca. A formação do indivíduo tem primordial importância, pois a privacidade é essencial para que isso ocorra. Um analista de sistema, Edward Snowden concluiu que o mundo tem direito de saber as atitudes do governo, abrindo mão de sua liberdade e divulgando documentos confidenciais da NSA, agência para a qual trabalhava. Conforme o tempo está passando, o caso está perdendo valor. Hoje quase inexistente, a noção de privacidade tem que ser resgatada, incluindo a diferença entre o que é privado e público para cada cidadão.

Com o objetivo específico de identificar por que informações confidenciais foram e ainda são adquiridas através da internet. Salientar o papel da NSA nas operações de vigilância dos Estados Unidos da América, identificando como ocorre a violação da privacidade ao adquirir dados privados. Evidenciar a jurisdição que rege tanto a confidencialidade de cada país, como a de cada cidadão. Relatar como a espionagem norte-americana ameaça a Soberania do Brasil e expor o posicionamento da ONU (Organização das Nações Unidas).

Utilizando de métodos de pesquisa jurisprudencial, doutrinária, artigos de periódicos e pesquisa de campo.

1. ORIGEM E EVOLUÇÃO HISTÓRICA

De acordo com Sun Tzu (filósofo, estrategista e general chinês) em seu livro Arte da Guerra, *"espionagem é um ato só permitido entre beligerantes, nações, grupos guerrilheiros em guerra e/ou guerrilha, consiste na prática de obter informações de caráter sigiloso relativas a governos ou organizações, sem a autorização desses, para obter certa vantagem militar, política, econômica, científica tecnológica e/ou social"* Para Tzu a espionagem não devia ser negligenciada para que haja o sucesso de um governante, pois é uma ferramenta fundamental.

Desde os tempos bíblicos as nações usavam em defesa de seu interesse o ato de espionar. Criado pelos antigos egípcios o primeiro sistema para aquisição de informação, que logo foi adotado pelos hebreus, estando relatado no velho testamento a queda de Jericó (Capítulo 5 e 6), onde após enviar dois espiões à cidade de Canaã, obtém informações por meio de uma prostituta (Raabe), e assim conseguem a derrota de Jericó.

Porém, durante o reinado de Luis XIV, também conhecido como Rei Sol, autor da frase *"O Estado sou eu"* o absolutista francês governou de 1661 até sua morte em 1715, tendo em seu reinado o primeiro serviço secreto oficial.

Até a Guerra Fria os sistemas de espionagem não eram muito utilizados, mas isso não significa que eram inexistentes. Há historiadores simpatizantes com a ideia de que se esses sistemas fossem utilizados, tanto a primeira quanto a segunda guerra mundial não teria eclodido, uma vez que não era esperado os conflitos nos Bálcãs, e na segunda poderia ter sido evitada a invasão da União Soviética.

Durante o processo revolucionário, foi criado pelos soviéticos o Tcheka (Comitê Contra Atos de Sabotagem e Contra Revolução), criada por um decreto emitido no dia 20 de dezembro de 1917, sendo um serviço secreto que atuava contra atividades internas à revolução comunista. O Comitê sofreu diversas reorganizações após 1922, sendo a sucessora da antiga Okhrana tsarista que sua tarefa era "reprimir e liquidar", que possuía diversos poderes quase sem limites legais para qualquer ato contrarrevolucionário.

Até 1940, não existia vontade dos Estados Unidos em desenvolver um sistema de espionagem. Tendo como sua principal agência de segurança a Agência

Federal de Investigação (*Federal Bureau of Investigation – FBI*), que tinha como foco a vigilância de grupos fascista, socialistas e anarquistas. Assim que estourou a Segunda Guerra Mundial o país criou a *Office of Stratégic Services* (Agência de Serviços Estratégicos – *OSS*) que é considerada a antecessora da Central Americana de Inteligência (*CIA*).

Mas o mais importante sistema de espionagem é o Echelon, criado em 1948, durante a Guerra Fria para deter o Império Soviético, porém, a rede vem sido utilizada até os dias atuais. A primeira revelação feita de caso de espionagem com o Echelon foi feita por Margaret Newsham que contou aos membros do congresso norte-americano que as ligações de um membro do Partido Republicano estavam sendo coletadas pela NSA. Outra revelação foi feita apenas em 2013, através do Jornalista Glenn Greenwald que publicou no The Guardian revelações de vigilância eletrônica global americana feita também pela NSA.

1.1. GUERRA FRIA

Ao fim da Segunda Guerra Mundial, os maiores países do mundo na época, Estados Unidos Da América e União Soviética. Tanto um quanto o outro tinham ideias contrárias em relação a estabelecer um novo “regime” ao mundo, um com a escolha do capitalismo, o outro a favor do socialismo. Assim então, os dois permitiam-se criticar o próximo, para tentarem ver qual poderia ser a melhor escolha, o nome dado a essa rivalidade? Guerra Fria.

A Europa Ocidental, Canadá e Japão se aliaram aos EUA enquanto que a Tchecoslováquia, Polônia, Hungria, Iugoslávia, Romênia, Bulgária, Albânia, parte da Alemanha e a China se uniram com a URSS.

Na década de 50 e 60, ocorreu a tal chamada corrida armamentista, afinal, qual dos dois países poderia possuir a maior tecnologia em relação a armas? Porém, nenhum dos dois países usaria as armas como forma de ataque ao outro, mas apoiava a guerra entre países menores, cada um incentivando seus aliados. Uma prova seria a guerra da Coréia, entre 1950 e 1953.

Como forma de tentativas para verem qual deles poderia ser melhor, decidiram então lançar homens ao espaço, qual prova de poder poderia ser melhor

na época do que isso? Portanto, URSS mandou Yuri Gagárin ao espaço, enquanto os EUA enviaram Neil Armstrong à Lua.

Depois da simples prova como essa, a Alemanha, destruída pela Segunda Guerra, acabou sendo dividida em duas, Alemanha Oriental e Ocidental.

Vendo que poderia investir seu regime como prova de que funcionaria, os Estados Unidos adota então o capitalismo na Alemanha Ocidental, investindo milhões de dólares no local. Enquanto isso, a Alemanha Oriental, vivendo através do Socialismo não se desenvolvia nem muito menos crescia moradores então da mesma, vendo o desastre decidem migrar para Alemanha Ocidental. Claro que o Governo da RDA (República Democrática Alemã) se irritou e em 1961 ordenou a construção de um muro isolando Berlim Ocidental do restante da Alemanha. Era o *Muro de Berlim*, que é considerado um dos maiores símbolos da Guerra Fria.

O investimento em armamentos e a curiosidade em saber o que a outra potência estava projetando era tanta que ai então, deu-se início a investigação do país rival, ou tão conhecida como a Espionagem Global.

A liberdade de cada cidadão corre riscos corriqueiramente de ser privada, uma Estada coleta segredo de Estado do seu adversário para conseguir usá-la de determinadas formas, desde muito tempo atrás, tudo isso se iniciou na Guerra Fria quando para coletar informações dos dois lados da Alemanha foi utilizado o sistema de vigilância dos Estados Unidos com seus vigilantes.

Nessa época que foram criadas a CIA e a NSA, e já existia o FBI que era para acabar com o conflito interno, ou seja, os sistemas de espionagem global foram lançados nos Estados Unidos, é a fonte de onde tudo começou e foi se estendendo, agora os maiores países “o monopólio” cada um desenvolveu seu programa, sua técnica de vigilância.

A *CIA*, *Central Intelligence Agency*, foi criada em 1947 e seu objetivo era coletar informações de grupos e de países estrangeiros e depois avaliá-las.

1.1.1 ECHELON

Para o melhor domínio de informações mundiais, foi criado em 1948 durante o período da Guerra Fria uma rede global de computadores que busca dados

automaticamente por meio de milhões de mensagens interceptadas por palavras-chave. É automaticamente pesquisado para cada termo de mensagem digitado nas frequências e canais selecionados em uma estação.

Este instrumento foi denominado Echelon, de acordo com a cultura popular. Desenvolvido pela Agência Nacional de Segurança dos EUA, com direta participação do Reino Unido, Canadá, Austrália e da Nova Zelândia.

Segundo Nicley Hager:

> *"A chave da interpretação reside em poderosos computadores que perscrutam e analisam a massa de mensagens para delas extraírem aquelas que apresentam algum interesse. As estações de interceptação recebem milhões de mensagens destinadas de estações terrestres credenciadas e utilizam computadores para decifrar as informações que contêm endereços ou textos baseados em palavras-chave pré-programadas."*

Suas atividades iniciaram-se nos anos 40, que tem como embrião o pacto secreto entre os EUA e a Grã Bretanha, na atualidade denominada de Reino Unido, (Pacto UKUSA) do qual resultou na instalação de estações de rastreamento de mensagens enviadas na Terra desde então por satélites das redes *Intelsat*, *International Communications Satellite,* e a *Inmarsat.* Além do Echelon foram enviados para o espaço diversos satélites de espionagem para a escuta de rádio de celulares, e para registro de mensagens de correio eletrônico. O segredo tecnológico do Echelon consiste na intercomunicação de todos os sistemas de escuta.Como descreve a imagem:

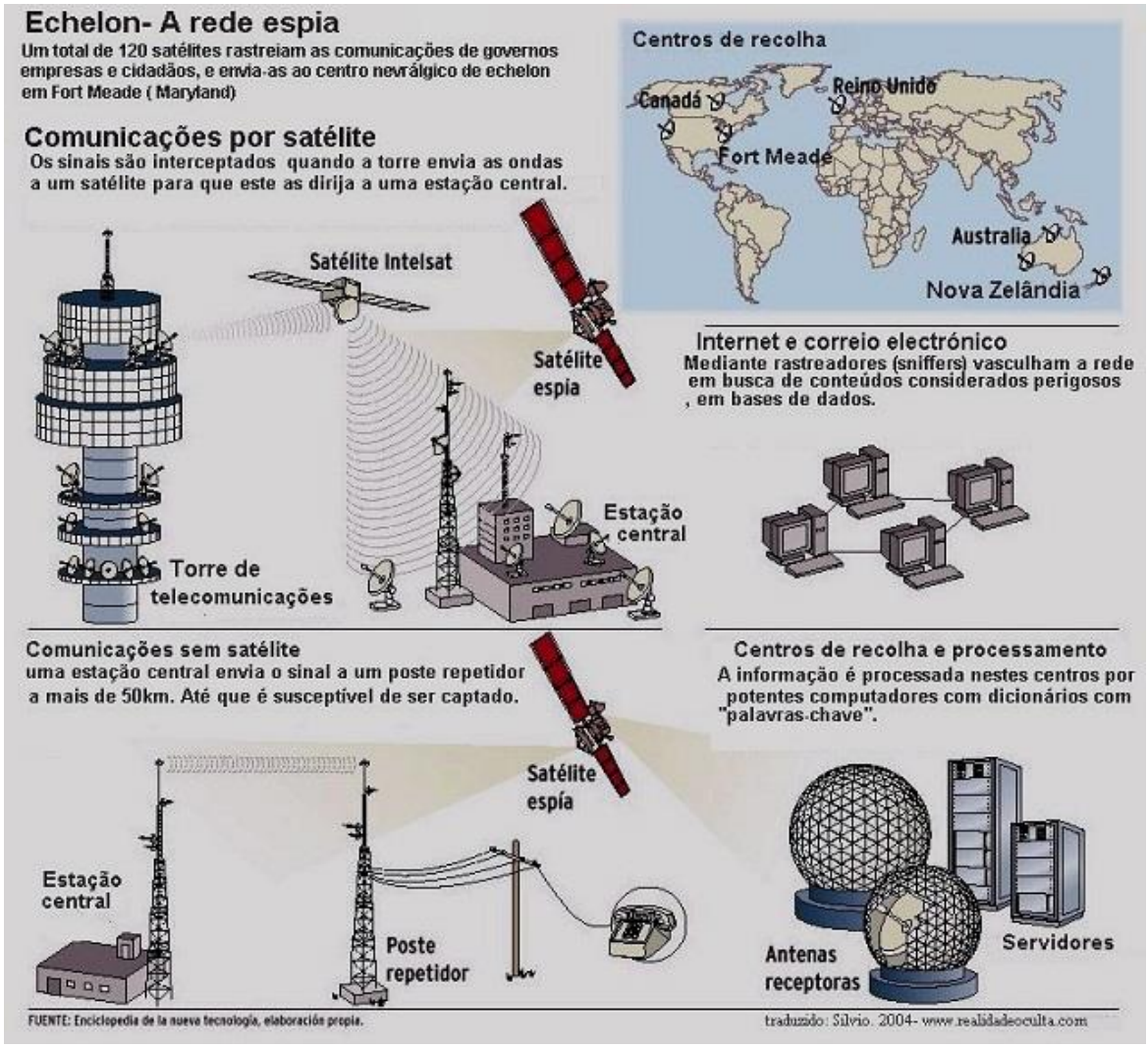


Figura 1 Echelon - A rede espia. Encicloplédia de la nueva tecnología. Traduzido: 2004 - www.realidadeoculta.com.

A rede funciona durante às vinte e quatro horas do dia sendo assim até o final de 1990 o Echelon já era capaz de arrecadar mais de 90% dos dados da internet. Podendo também interceptar por dia mais de três bilhões de comunicações. Para tamanha eficiência possui algumas estações:

- Menwith Hill (Reino Unido);
- Base Aérea de Misawa (Japão);
- Morwenstow (Reino Unido);
- Pine Gap (Austrália);
- Sabana Seca (Estados Unidos);
- Shoal Bay (Austrália);
- Yakima (Estados Unidos);

- Waihopai (Nova Zelândia).

O que não era de conhecimento desses membros é que mesmo após o término da Guerra Fria os EUA continuou utilizando a rede, e não apenas contra seus inimigos mas também contra seus aliados.

Em 5 de setembro de 2001 foi aprovada uma resolução do Parlamento europeu denunciando o Echelon, também foi pedido a seus cidadãos que codificassem suas contas. Porém, seis dias depois, ocorreu o ataque às Torres Gêmeas no dia 11/09/2001 (onze de setembro de dois mil e um) sendo usado o atentado como justificativa para continuar usando a rede para segurança nacional.

Existe também o Echelon Financeiro, que rastreia possíveis financiamentos terroristas por meio do *SWIFT* (Sociedade Internacional para as Telecomunicações Financeiras e Interbancárias), que dá o acesso a todas as transferências multimilionárias diariamente. Tendo o completo acesso de todas as contas importantes. Agora é utilizado para conter todos os cidadãos não apenas estadunidenses, mas de todo o mundo violando um direito fundamental seja em qualquer país, o direito de liberdade.

2. PENTÁGONO

Sede do Departamento de Defesa Americana, foi inaugurado em 15 de Janeiro de 1943, e é o órgão onde concentra-se a maior inteligência americana, e situa-se no Condado de Arlington aos redores de Washington D.C., na Vigínia. É um edifício em forma de um pentágono quando visto de forma panorâmica e foi e ainda é abrigo de militares, centro de treinamento e base estratégica de defesa. Onde em seu edifício comporta a Marinha, a Força Aérea, a Guarda Costeira, o Exército, a Agência Nacional de Segurança, a Agência Inteligência de Defesa e entre outros parceiros.

A NSA é um braço do pentágono e sua vigilância é feita pela aliança dos Cinco Olhos.

2.1. ALIANÇA DOS CINCOS OLHOS

Os “Cinco Olhos” é uma organização de vigilância formada por: Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia, países anglófonos coletando muitas informações.

Esse pacto entre os países visava o controle das ligações da União Soviética e seus aliados durante o período da Guerra Fria. Todavia esse sitema ainda está ativo e monitora 90% das comunicações globais através da internet. Um dos principais objetivos da organização é o domínio e supremacia econômica sobre os outros países do mundo.

Nessa organização investem e exercem em diversas atividades de inteligência, propagando-as e criando contrainteligência para defesa sob outros países, construindo uma fortaleza e coletando dados para nunca ser ultrapassado adquirindo novos objetos de pesquisa a cada dia que se passa.

A maior parte dos arquivos do acervo da NSA são assinados pelo “FVEY”, ou seja, *Five Eyes* (Os Cinco Olhos).

O órgão mais próximo à NSA dos Cinco Olhos é a GCHQ- Central de Comunicações do Governo britânica que recebe uma grande quantia de dinheiro por ano para apoiar os Estados Unidos, assim permanecendo aliados.

Todo ano há uma conferência onde todos os países membros compartilham entre si o que foi desenvolvido da vigilância de cada um, pelo menos a maior parte, colaborando uns com os outros para que haja um desenvolvimento através da cooperação.

Em 2010 o general Keith B. Alexander, apaixonado pela vigilância e inteligência, apresentou um documento em uma Conferência dos Cinco Olhos, sobre um programa que foi criado por ele cujo nome é TARMAC, que significa asfalto porque o objetivo é fazer busca de dados mais complicados de serem obtidos, na intenção de coletar tudo.

3. NATIONAL SECURITY AGENCY – NSA (AGÊNCIA DE SEGURANÇA NACIONAL).

Fundada em 1952, pouco depois da Segunda Guerra Mundial, com o objetivo de rastrear informações e prever ataques-surpresa ao país — como aconteceu em

Pearl Harbor, durante a Segunda Guerra Mundial, é um órgão importante do Departamento de Defesa dos Estados Unidos da América responsável pela utilização do sistema SIGINT (Signals Intelligence), uma inteligência conseguida através de sinais, o que inclui criptoanálise e interceptação, é também responsável pela proteção dos dados obtidos pelo SIGINT, tornando-se o maior órgão de dados de criptologia do mundo. A grande responsabilidade do núcleo é a interceptação e análise de ligações com o objetivo de manter a seguridade nacional e a dos países aliados. A agência localiza-se no Estado de Maryland, região nordeste norte americana.

Como parte do protocolo de segurança da NSA, os dados e informações obtidos por meio de interceptações raramente são divulgados. Isso permite também que muita dúvida tenha surgido em relação à agência devido à violação deliberada da privacidade de milhões de pessoas por todo o mundo.

Outros sistemas utilizados pela NSA para espionar o conteúdo gerado pela internet são o PRISM e o MUSCULAR. O primeiro possui colaboração das grandes empresas de tecnologia, como *Google*, *Microsoft*, *Apple*, *Facebook* e outras, que enviam dados para análise das informações. O segundo está ligado diretamente aos e-mails do *Yahoo!* e ao *Gmail*. Esse sistema intercepta os cabos dos *data centers* que levam as mensagens de e-mail para seus destinatários.

A agência dispõe de quatro satélites posicionados ao redor do globo monitorando frequências que vão de *walkie-talkies* e celulares na Líbia até sistemas de radares na Coreia do Norte. Os equipamentos são capazes de conseguem filtrar o conteúdo de acordo com regiões-chave escolhidas.

Para vigiar os outros países, a NSA dispõe de escritórios espalhados nos Estados Unidos. Cada um é responsável por uma região, como os escritórios presentes em Fort Gordon, na Georgia, em que os 4 mil funcionários são designados para interceptar dados provenientes da Europa, Oriente Médio e a parte norte da África.

A rede de dados da NSA também conta com “filiais” em diversos cantos dos Estados Unidos, onde agentes coletam informações de diversos pontos, incluindo

operadoras de telecomunicação. Isso gerou protestos no país, pois a agência passou a interceptar dados e investigar a vida dos próprios americanos.

Todas as informações coletadas devem ser direcionadas ao novo *data center* da NSA, que está sendo construído em Utah. Depois disso, esses dados podem ir para o centro de pesquisas que fica em Oak Ridge, no Tennessee. Lá, analistas e engenheiros de alto escalão deverão utilizar os supercomputadores mais rápidos do mundo para decifrar as informações secretas.

Parte dos arquivos do novo data center também devem seguir diretamente para o quartel general da NSA que fica em Fort Meade, em Maryland. De lá, relatórios serão disparados para a Casa Branca, a *CIA* e o Pentágono.

O ex-operador da NSA disse que chegou a sugerir que a agência interceptasse apenas informações de suspeitos e pessoas ligadas a eles, mas acabou sendo ignorado.

O Prisma está em vigor desde 2007, é um programa de vigilância que monitora e buscam dados como fotos, documentos, mensagens, toda mídia eletrônica em tempo real destacando o objetivo de prevenir o mundo de ataques terroristas, permitindo a NSA ter ligações com empresas para obter informação sobre os utilizadores, portanto se você é um usuário de algum programa licenciado com o Prisma ele consegue monitorar todos os seus movimentos dentro do determinado aplicativo, e tudo somente foi possível por causa das leis implementadas após o atentado de 2001 para poder manter a população segura.

3.1 UTAH DATA CENTER (CENTRO DE PROCESSAMENTO DE DADOS UTAH)

O complexo terá como objetivos interceptar, decifrar, analisar e armazenar um grande volume de informações de comunicações provenientes de diversos pontos do país e do mundo.

O data center de 2 bilhões de dólares deve entrar em funcionamento completo até setembro deste ano, carregando informações provenientes de praticamente todos os meios de comunicação existentes. Isso inclui conversas de e-

mail, ligações de telefonia celular, pesquisas em sites de busca e mais um grande número de dados adquiridos por meio digital.

Além de analisar todas essas informações, o complexo será responsável por descriptografar um grande volume de dados, desde negociações a segredos diplomáticos. O maior problema está em saber como a agência vai interpretar as informações obtidas e definir quem pode ou não ser um inimigo em potencial.

4. DA ESPIONAGEM GLOBAL

O papel central da espionagem nas relações internacionais antecede a própria formação do sistema internacional moderno e a consolidação dos Estados como são conhecidos hoje. À época do Renascimento, a diplomacia das cidades-estado italianas já era afeita a intrigas, conspirações e sigilo. Também o rei Luís XIV da França tinha a seu serviço uma extensa rede de espionagem e mantinha em vários arquivos os segredos adquiridos, fossem eles comprados ou roubados, que lhe permitiam antecipar acontecimentos e se aproveitar das situações já esperadas.

No século XVII, quando as relações diplomáticas permanentes já eram comuns na Europa, a maioria das embaixadas utilizava os serviços de agentes secretos. E não demorou muito para que os próprios embaixadores passassem a ser considerados “espiões com licença”: suas principais funções eram abrir cartas alheias, subornar e corromper desde ministros até serviçais.

Mais tarde, organizações especializadas na interceptação e decodificação de mensagens se tornaram comuns na Europa – as chamadas “Câmaras Negras”. Após a invenção do telégrafo, na década de 1840, a possibilidade da comunicação quase instantânea fez com que o fluxo de informações aumentasse muito e com isso cresceu também a preocupação com interceptações e espionagem.

Toda essa preocupação decorre da necessidade dos Estados de assegurarem por seus próprios meios a sua sobrevivência em um sistema internacional no qual não existe autoridade superior capaz de regular as interações conflitivas entre entidades soberanas. A ONU não está acima dos países, e os EUA nos lembram disso com frequência.

Os países desconfiam uns dos outros, e têm razões para tanto. Por isso possuem forças armadas. Também por isso mantém segredos, ainda que nem todos

legítimos. Por isso devem investir em sistemas de inteligência capazes de assegurar seus interesses e a segurança nacional.

A interceptação de informação pelos Estados Unidos não é uma novidade no cenário internacional. Muitos países foram alvos, gerando certa apreensão e tensões diplomáticas em relação à segurança da internet em todo o mundo. A justificativa norte-americana para tais atividades é que elas visam detectar e combater atividades terroristas, e assim são necessárias e vantajosas para todos. Esse foi inclusive um dos argumentos utilizados pelo presidente Barack Obama, em seu discurso nas Nações Unidas. Ele afirmou que, como resultado desse trabalho e da cooperação com os aliados, o mundo agora é mais estável do que há cinco anos.

O governo brasileiro tem razão em condenar veementemente a espionagem norte-americana. Mas o que se condena na realidade é o escândalo, já que a espionagem não é novidade. E o escândalo decorreu mais uma vez da incapacidade dos EUA de manterem em sigilo seus documentos ultrassecretos.

Casos de vazamentos de informações sigilosas têm sido recorrentes naquele país, apesar da perspectiva de prisão perpétua e dos muitos bilhões de dólares investidos no sistema de proteção aos segredos de estado.

Muito já foi dito acerca da chamada “superextensão” do sistema americano de classificação de informações. O excesso de segredos e o número alto de funcionários com acesso a informações sigilosas de fato comprometem tanto a obrigação democrática de transparência, quanto a capacidade dos governos de proteger informações estratégicas. Mas é a natureza dos segredos guardados o ponto negligenciado.

Apesar de o sigilo em questões de defesa e política externa ser justificado pelos governos com apelo ao argumento da segurança nacional, a questão é que legítimos segredos de segurança nacional representam apenas uma parcela pequena de todo o conjunto de informações classificadas. Também é protegida toda uma gama de segredos políticos e burocráticos, muito questionáveis e até mesmo prescindíveis.

Os Estados Unidos se consideram um país excepcional, com a missão fundamental de levar democracia, direitos humanos e liberdade ao resto do mundo. Acreditam que esses direitos são absolutos, soberanos e intrínsecos a todo ser humano, e rejeitam a noção de que tais princípios possam ter acepções diferentes para diferentes culturas. Eles declaram abertamente que estão preparados para usar todos os meios, inclusive militares, para assegurar seus interesses vitais, que vão desde o combate ao terrorismo até a garantia do suprimento de petróleo.

No mesmo discurso, na abertura da 68ª sessão da Assembleia Geral das Nações Unidas, o presidente Obama afirmou: *"The danger for the world is not an America that is too eager to immerse itself in the affairs of other countries or to take on every problem in the [middle east] region as its own. The danger for the world is that the United States, after a decade of war […] may disengage, creating a vacuum of leadership that no other nation is ready to fill."* Ou seja, os Estados Unidos não apenas afirmam ter o dever de intervir em outros países, no melhor interesse de todas as nações, mas também se consideram como os únicos com poder suficiente para tal. Nenhum Estado se configura como uma ameaça para eles, especialmente considerando que seu investimento militar é maior do que os da Europa e Ásia somados.

Esse sentimento de superioridade se aplica também à inteligência norte-americana. Os episódios recentes de espionagem demonstraram uma superioridade tecnológica dos Estados Unidos e a vulnerabilidade relativa dos demais países, uma vez que ele possui o domínio de uma tecnologia de monitoramento que os outros ainda não conseguiram desenvolver, e nem sequer têm meios de detectar e combater. Frente às acusações de espionagem, o governo dos EUA admitiu que existe sim um monitoramento de informações, mas alegou que seu objetivo é apenas o combate ao terrorismo, e que suas atividades foram distorcidas pela imprensa. Nenhum outro pronunciamento foi feito por parte do governo, evidenciando o descaso perante o assunto.

O vazamento de informações confidenciais dos Estados Unidos teve início no final de novembro de 2010 quando o *site* *WikiLeaks* cinco grandes jornais publicaram documentos oficiais do departamento de Estado do país. O ex-técnico da *CIA* Edward Snowden foi acusado por vazar essas informações e revelar com

detalhes alguns dos programas de vigilância que o país usa para espionar a população americana e vários países da Europa e da América Latina, inclusive conversas da presidente Dilma Rousseff com seus assessores.

Outro sinal de que essa questão foi tratada como tendo menor importância é que o discurso da presidente Dilma Rousseff na abertura da sessão da ONU tratou longamente da espionagem, e demandou desculpas, explicações e garantias de que tal ato não se repetiria. O discurso do presidente Obama, por sua vez, tratou brevemente do assunto, afirmando apenas que seu país começou a rever o modo como adquirem inteligência, para que pudesse equilibrar propriamente as preocupações legítimas de segurança de sua população e de seus aliados com as preocupações relativas à privacidade compartilhadas por todas as pessoas.

A primeira repercussão concreta da espionagem ao Brasil foi o adiamento por tempo indefinido da visita de Estado que a presidente faria aos Estados Unidos. Essa decisão, junto com todo o conjunto de eventos que levou a ela, indica certa fragilização das relações Brasil-EUA, que são importantes para ambos os países, envolvendo múltiplas áreas e movimentando cerca de 100 bilhões de dólares por ano em comércio e serviços. Essa atitude, assim como o discurso incisivo na ONU, foi considerada por muitos uma demonstração de força e a tentativa de estabelecimento de um diálogo “de igual para igual” com os EUA.

A mesma crença em ideais democráticos e valores morais capaz de mobilizar o povo americano a grandes feitos é também capaz de levar homens como Snowden a assumir o risco de desafiar o Estado em nome da verdade, da transparência e da democracia.

Um ponto crucial é que foi alvo da espionagem a Petrobrás, uma das maiores empresas brasileiras, e os dados coletados teriam valor econômico, além de estratégico. A espionagem por razões de segurança e combate ao terrorismo já teria sido ultrajante, mas este fato indica que também houve interesses econômicos motivando, ou ao menos se beneficiando, dessa atividade.

O presidente Obama se comprometeu a trabalhar conjuntamente com Brasília para amenizar as tensões geradas, e com isso e um pedido de desculpas oficial, a

questão da espionagem deve passar gradualmente a segundo plano. Porém ficou claro que o propósito principal não é combate ao terrorismo, não é segurança nacional, não é combate a outros crimes como a pedofilia. É para aumentar o poder dos EUA e dar vantagem econômica.

Ao mesmo tempo em que a comunidade internacional procura desenvolver mecanismos institucionais para dar conta, de maneira democrática, participativa e multissetorial, do cenário complexo de organização e funcionamento da Internet, os Estados Unidos têm uma posição privilegiada no *status quo*. Apesar de o país demonstrar disponibilidade em colaborar no processo multissetorial de governança da Internet, e de se apresentar como um grande promotor da causa da Internet "aberta, estável, segura e interoperável", cada vez mais – especialmente com a revelação de detalhes que orientam as políticas públicas domésticas e internacionais do país - fica claro que os Estados Unidos vêm usando essa posição privilegiada em prol de seus próprios interesses no plano internacional em detrimento dos interesses do resto do mundo. De forma declarada, o presidente Obama diz: *"temos de desenvolver o uso do ciberespaço (da Internet), como uma parte integral da promoção de nossos interesses em tempos de paz, de crise, e até mesmo de guerra. Para isso estamos dispostos a empregar nossa experiência e nossas capacidades concentradas nesse campo.".*

No contexto competitivo e anárquico das relações internacionais, tal conjuntura pode levar ao reforço de ações isoladas pelos diferentes países com a finalidade de obterem maior controle sobre a Internet, de maneira a diminuir a assimetria de poder (político e econômico) que decorre do protagonismo norte-americano.

A importância dessa revelação está em conscientizar as pessoas das consequências do uso de tecnologias digitais. O que é colocado nas redes sociais, por exemplo, fica armazenado por tempo indeterminado nos servidores das empresas que as mantêm. Se há um componente de cautela do ponto de vista dos usuários que precisa ser fomentado, é também preciso que sejam criadas e revisadas as regras a respeito do que se pode fazer com os dados que trafegam pela Rede e que são armazenados nos computadores de empresas e órgãos governamentais. O Brasil – através da ideia de ter sua própria Carta de Direitos

Fundamentais para a Internet, formulada com ampla participação popular – tem avançado no processo de adaptação do ordenamento jurídico ao cenário sociotécnico complexo do mundo contemporâneo. A paralisia da iniciativa, nos termos atuais, é um retrocesso com custo altíssimo para a população, ainda que isso tenha bem menos espaço do que deveria na agenda política do país.

4.1 CONCEITO

A espionagem é usualmente compreendida como a atividade de agentes de um governo ou outra entidade, de caráter secreto ou confidencial em busca de dados sigilosos e estratégicos de outro governo ou organização com o objetivo de obter vantagem militar, política, tecnológica, econômica ou social.

A definição vem sendo restringida a um Estado que espia inimigos potenciais ou reais, sobretudo para finalidades militares, porém, ela também abrange a espionagem envolvendo empresas (conhecida como espionagem industrial) e pessoas físicas, através de contratação de detetives particulares.

Os tipos de espionagem mais comuns são a industrial, a militar, a tecnológica, a econômica, a financeira, a política e a eleitoral.

A espionagem não tem um tratamento intrínseco na legislação brasileira, sendo tratada de maneira esparsa na legislação penal, geralmente referenciada à espionagem militar, isto é, ao acesso e apropriação de informações e dados sigilosos atinentes à defesa. Todavia, os efeitos jurídicos da espionagem não se restringem à esfera do direito penal, podendo também repercutir em outras instâncias do direito, como a civil e a administrativa.

Além dos casos específicos e nominais de espionagem, a lei pune o acesso a dados ou os meios de obtenção, conforme o caso. A debilitada ausência de menção ao termo espionagem não significa que ela não gere repercussões perante nosso ordenamento jurídico. Há casos, em que o termo espionagem é salientado. Isso acontece no Código Penal Militar e na Lei de Segurança Nacional.

Numa análise criminal, deve-se levar em conta que há condutas que são revestidas caracterizadas como espionagem, sem que se precise recorrer ao contexto ou motivação do caso concreto.

É possível estabelecer uma categoria de crimes eventualmente relacionados à espionagem, pois há um grande número de crimes que em nenhuma hipótese poderiam constituir meio de prática de espionagem, como o estupro (art. 213, CP), abandono intelectual (art. 246, CP), aborto (art. 124, CP), esbulho possessório (art. 161, II) e outros.

Há as hipóteses em que a mera obtenção do dado secreto não é em si criminosa, mas sim a forma de sua obtenção.

Além das provisões penais, a espionagem também é tratada, implicitamente, na legislação de crimes de responsabilidade, que, conforme o entendimento predominante, não constituem infrações penais. A Lei de Crimes de Responsabilidade é aplicável ao presidente da República, aos ministros de Estado, aos ministros do Supremo Tribunal Federal e ao procurador-geral da República e prevê como pena a perda do cargo e a inabilitação, por até cinco anos, para o exercício de função pública. Entre os crimes de responsabilidade contra a existência da União, praticáveis exclusivamente pelo presidente da República, encontramos o do art. 5º, n. 4, c/c art. 4º, I. A revelação de negócios políticos e militares sigilosos constituirá necessariamente uma forma de espionagem.

A espionagem representa poder e pode determinar o domínio político ou econômico de um país sobre o outro, podendo chegar a gerar uma guerra digital.

4.1.1 CRIPTOGRAFIA

A Agência de Segurança Nacional desenvolveu secretamente a habilidade de quebrar ou contornar a criptografia na internet usada para proteger desde e-mails até transações financeiras.

Contudo, ainda existe uma última barreira de segurança que impede que os agentes do governo tenham acesso irrestrito a esse grande **volume** de informações: a criptografia. Qualquer um, desde terroristas, vendedores de armas, instituições financeiras e qualquer pessoa que envie mensagens por email, pode utilizar a criptografia para proteger os seus documentos.

Os documentos mostram que a NSA teve “grandes” problemas com o Truecrypt, serviço gratuito (agora extinto) para criptografar arquivos no computador; e com o Off-the-Record, que criptografa mensagens instantâneas.

Há também uma série de serviços aparentemente seguros que, segundo o documento, na verdade são fáceis para a NSA monitorar. Isso inclui conexões HTTPS, que muitos de nós usamos diariamente ao fazer login em sites bancários e outros websites “seguros”: a NSA teria interceptado 10 milhões de conexões https *por dia* em 2012.

O protocolo mais utilizado é o *Advanced Encryption Standard* (AES), que existe em três formatos diferentes: 128, 192 e 256 bits. Esse sistema está incorporado na maioria dos serviços de email comerciais e navegadores da web.

O AES é tão difícil de ser quebrado que a própria NSA aprovou a sua utilização nas mensagens ultrassecretas do governo americano. Somente para ter uma ideia: para quebrar uma criptografia assim utilizando o método de força bruta (aquele em que todas as combinações possíveis são testadas uma atrás da outra), levaria mais tempo que a idade do próprio universo, já que um arquivo criptografado com o método AES 128 bits teria cerca de 340 undecilhões de combinações possíveis.

É aí que entra o novo complexo da NSA. Para a decodificação são necessários supercomputadores e mensagens cifradas. Quanto maior o número de mensagens, maior é a probabilidade de os analistas e supercomputadores encontrarem padrões reveladores.

Documentos revelam que a NSA e o GCHQ trabalham juntos em um programa que tem custado US$ 250 milhões (R$ 581 milhões) por ano e que tem como objetivo decodificar dados protegidos com criptografia, procedimento que impede a leitura de informações interceptadas.

O programa teria sido criado após o fracasso da NSA em garantir que todas as tecnologias de criptografia tivessem uma "porta dos fundos" para o uso da agência.

O programa é composto por iniciativas de quebra dos algoritmos de segurança com o uso de supercomputadores. É uma área conhecida como "criptoanálise".

4.1.2 ANALOGIA AO LIVRO 1984

O livro "1984", de George Orwell, publicado no final da década de 1940, era uma distopia em que todos os cidadãos eram perseguidos e observados por teletelas onde quer que estivessem. A ideia de sua composição já estava na mente de Orwell desde a Guerra Civil Espanhola (1936-1939), mas o estopim para colocar a mão na massa foi após a Segunda Guerra Mundial, no fim de 1946. Se Oscar Wilde dizia que *"a vida imita a arte muito mais do que a arte imita a vida",* a previsão de Orwell tornou-se uma realidade quando foram publicados dados que comprovam que os Estados Unidos, através da Agência de Segurança Nacional, espionaram milhares de e-mails e ligações pessoais no mundo inteiro. As semelhanças entre o mundo fictício de Orwell e o Estado de vigilância da NSA são inegáveis.

A história é protagonizada pelo personagem Winston Smith que vive aprisionado na engrenagem totalitária de uma sociedade totalmente dominada pelo Estado. Um governo repressivo e autoritário, cujo poder está baseado no controle e na vigilância sobre os cidadãos, esse controle é denominado "Grande Irmão" do qual ninguém escapa de ser vigiado no mundo criado por Orwell.

As teletelas que apresentam o Grande Irmão (ou "Big Brother") na obra de Orwell jamais poderiam ser desligadas completamente. "Não havia como saber se você estava sendo observado em um momento específico – era possível controlar todo mundo o tempo todo", sintetiza uma passagem do livro. Esse dispositivo de poder leva o indivíduo à constante sensação de visibilidade, fazendo com que ele se sinta submetido a um poder visível, mas jamais inverificável, — deu-se o nome de Panóptico. Trata-se de uma técnica de vigilância desenvolvida pelo jurista Jeremy Bentham, em 1785, quando ele idealizou uma construção em forma de anel, com celas que convergiam para uma torre central. Esse sistema pode ser utilizado em presídios, hospitais, fábricas ou na casa das pessoas, como no caso de 1984. Era até possível pensar que todos estavam sendo vigiados o tempo inteiro, mas de qualquer forma, ela podia conectar seu fio a você sempre que fizesse. Você precisava viver – e vivia, por um hábito que se tornava instinto – na suposição de que todos os sons que produzia eram ouvidos e, a não ser no escuro, todos os seus movimentos, monitorados.

Quando observamos o caso de vigilância realizada pelo governo dos Estados Unidos é impossível não fazer um paralelo com o "Grande Irmão" da distopia

prevista por Orwell. A internet e outros meios de comunicação, com propósito de libertar a humanidade, foram transformados nos mais perigosos facilitadores do totalitarismo.

Entretanto esse paralelo entre o livro e a vida real é veemente negado pelos defensores da vigilância, pois, segundo eles, a sociedade não está sando vigiada o tempo todo.

É tentadora a comparação entre o slogan orwelliano e essa política externa “o que os olhos não veem o coração não sente” praticada por Washington. Para os EUA, eliminar o desgaste de uma ocupação militar de longa duração seria o equivalente a pôr fim à guerra. Com essa mudança, essas técnicas de guerra “menos convencionais” podem continuar indiscriminadamente em tempos de paz.

Snowden jogou luz sobre o pretensamente sutil efeito Panóptico ao qual os cidadãos estão submetidos. Nas últimas décadas, a crescente instalação de câmeras de segurança, seja em residências e condomínios, seja em estabelecimentos comerciais e instituições privadas, já era um panoptismo consentido. Inspirado no líder supremo da ficção de Orwell, o próprio programa de televisão mundial *Big Brother* é um exemplo claro do momento em que uma sociedade panóptica se transformou em uma sociedade do espetáculo, em que a exacerbação da própria imagem já se traduz pelo fetiche pela visibilidade. No entanto, a conversão dos computadores, tablets e celulares em teletelas portáteis foi um choque em nível global, comprovando que 1984 de fato não é tão fictício assim.

4.2 EDWARD SNOWDEN

Edward Joseph Snowden nascido em 21/06/1983 (vinte e um de junho de mil novecentos e oitenta e três) em Elizadeth City (Carolina do Norte- Estados Unidos), não concluindo o ensino médio, estudou programação na Universidade Comunitária Annne Arundel de 1999 a 2005. Após dois anos de sua formação foi contratado pela NSA, onde começou a colher dados secretos para formar seu dossiê. Aos 31 anos já teve que pedir asilo político a vinte e um países dentre eles encontra-se o Brasil, porém apenas três se dispuseram a lhe abrigar sendo a Venezuela, Bolívia e Nicarágua.

Trabalhou em várias empresas relacionadas a NSA de maneira terceirizada, começou a recolher informações pela *Dell Corporation.* Em busca de encontrar mais informações foi trabalhar mais próximo da agência e passou muito tempo coletando arquivos confidenciais do governo americano, sem sequer notarem, era seu modo de fazer o mundo enxergar as coisas que omitem e "maquiam" como se não fossem coisas importantes. Como o mesmo descreveu:

"Não quero viver em um mundo onde a vigilância foi banalizada."

"Quero que o foco de atenção sejam os documentos e o debate que espero que gerem entre os cidadãos de todo o mundo sobre o tipo de mundo em que querem viver. Minha única motivação é informar o público do que fizeram em seu nome e o que se faz contra ele".

No momento que estava trabalhando na *CIA* descreveu ser o pior momento que vivenciou, enxergando que o país não estava fazendo apenas o que permanecia dentro da lei, e sim trabalhando com o setor privado, invadindo muito mais do que o que ele imaginava.

Em 13 de junho foi iniciada uma investigação penal contra Snowden. Logo após, o governo americano apresentou as acusações criminais por espionagem, roubo e conversão de propriedade do governo.

Edward Snowden reside desde então na Rússia onde obteve asilo temporário. Em janeiro de 2014, a Rússia anunciou que vai estender o período de asilo e não vai manda-lo de volta aos EUA.

Por meio de deputados do Partido Verde Europeu Snowden foi indicado ao Prêmio Sakharov, o qual homenageia defensores dos direitos humanas dentre eles encontra-se nomes como Nelson Mandela (líder do Apartheid, e mais importante governante da África do Sul) e também Guilhermo Farinãs (dissidente cubano). Para os europeus prestou um "enorme serviço" por ter ajudado a revelar tamanha dimensão das espionagens norte-americanas. *"Edward Snowden arriscou sua liberdade para nos ajudar a nos protegermos e ele merece ser homenageado por ter lançado luz sobre sistemáticas infrações a liberdades civis feitas pelos serviços secretos dos EUA e da Europa"* Sete personalidades são indacadas ao prêmio, dentre elas estão Malala Yousafzai (jovem paquinesa que foi baleada por terrorista do Talibã) e também Mikhail Khodorkovsky (ex-magnata do petróleo russo e crítico

do governo Putin). Juntamente com Khodorkoysky e Papa Francisco, foi indicado para o Prêmio da Paz de 2015 *“por mostrar como os cidadãos são monitorados com poucos controles democráticos.”*. Foi indicado e venceu o prêmio da Noruega (Prêmio Bjornson), por liberdade de expressão graças a “seu trabalho de proteção da vida privada e por ter mostrado, de forma crítica, a vigilância que os Estados fazem dos cidadãos”. No entanto o país é aliado dos Estados Unidos, e para que houvesse chance do vencendor ir buscar seu prêmio a Academia Bjornstjerne Bjornson pediu ao governo que garantisse que Snowden não seria extraditado.

Snowden teve seu primeiro encontro secreto com uma chefe de Estado em abril de 2015. Foi divulgado que a Argentina sofreu grande espionagem por parte do Reino Unido, logo após essa descoberta Cristina Kirchiner teve-se essa reunião na Rússia com duração de cinco dias contando no último com a presença de Vladimir Putin, presidente da Rússia.

Desde sua revelação ao Jornal *The Guardian* vem sendo objeto de ameaça de morte por agentes de várias organizações americanas incluindo o Pentágono e a NSA.

4.2.1 DECLARAÇÃO

O autor da coleta de dados espionados pelos Estados Unidos ficou durante vinte e três dias na zona de trânsito do aeroporto de Moscou a espera de que um dos países que pediu refúgio o respondesse, tem sido aceito em apenas em quatro países (Rússia, Venezuela, Bolívia e Nicarágua). Hoje vive em um asilo político concedido por Vladimir Putin (presidente da Rússia). Snowden tinha uma boa vida, um bom salário, mas acredita no princípio de Nuremberg, de 1945 onde os indivíduos acima de sua pátria tem obrigações mundiais, e baseado nisto que divulgou os dados coletados pela NSA, pois tinha consciência de que o país não estava apenas violando leis nacionais mas também internacionais, assim passando por cima da soberania de cada país.

Mesmo sabendo que sua vida e também a de sua família não seria mais a mesma, sua maior preocupação era que a divulgação não causasse impacto o suficiente, pois sabia que estaria exposto a sua sentença de morte assim como diversos norte-americanos desejam.

Declaração dada por Edward Snowden:

"Olá. Meu nome é Ed Snowden. Até a pouco mais de um mês, eu tinha uma família, um pedaço do paraíso para chamar de lar e vivia com muito conforto. Também tinha os meios para, sem precisar de qualquer mandado judicial, capturar e ler as suas comunicações. As comunicações de qualquer um a qualquer momento. Isso é o poder de mudar o destino das pessoas.

É igualmente uma grave violação da lei. As 4ª e 5ª Emendas à Constituição do meu país, o Artigo 12 da Declaração Universal dos Direitos Humanos e várias leis nacionais e tratados internacionais proíbem tais sistemas invasivos de vigilância em massa. Por mais que a Constituição dos Estados Unidos considere esses programas ilegais, meu governo argumenta que decisões judiciais secretas, as quais o mundo não está autorizado a ver, de algum modo legitimam uma ilegalidade. Essas decisões simplesmente corrompem a noção mais básica de justiça – a de que algo deve ser visto para que possa ser feito. O imoral não se torna moral pelo recurso a uma lei secreta.

Acredito no princípio declarado em Nuremberg, em 1945: "Indivíduos têm deveres internacionais que transcendem as obrigações nacionais de obediência. Portanto, cidadãos têm o dever de violar leis domésticas para prevenir crimes contra a paz e a humanidade".

Portanto, fiz o que acreditava ser o certo e comecei uma campanha para corrigir esses equívocos. Não tentei me enriquecer. Não tentei vender os segredos dos Estados Unidos. Não me associei a nenhum governo estrangeiro para garantir minha segurança. Em vez disso, tornei público o que eu sabia, para que aquilo que afeta a todos nós possa ser discutido por todos nós à luz do dia, e clamei a todo o mundo por justiça.

Essa decisão ética de tornar pública a espionagem que nos afeta a todos tem exigido seu preço, mas era a coisa certa a ser feita e não me arrependo."

4.2.2 AMEAÇAS

A partir da declaração anterior, Edward Snowden vem sofrendo diversas ameaças, dos cidadãos estadunidenses, mas principalmente por agentes de organizações como o Pentágono e a NSA. No dia 7/03/14 (sete de março de dois mil e quatorze) Snowden deu uma declaração ao Parlamento europeu afirmando que os Estados Unidos pediu sua execução. Enquanto isso a mídia do país mostra nenhum posicionamento diante do caso.

Em todas as ameaças querem sua morte, algumas sendo mais grosseiras do que outras.

Em depoimento ao parlamento Europeu em 7 de março de 2014 Edward relatou que os Estados Unidos teria pedido a sua execução. A mídia preferiu permanecer em silêncio sobre o assunto.

O artigo referiu-se sobre a citação de um agente do Pentágono:

"Eu gostaria de colocar uma bala na cabeça dele."

Um analista anônimo da NSA apontou:

"Em um mundo onde eu não estaria impedido de matar um americano, eu iria matá-lo pessoalmente."

Um oficial de alto nível do exército americano disse:

"Eu acho que se tivéssemos a oportunidade, acabaríamos com isso rapidamente. Apenas de maneira bem casual, quando ele (Snowden) vai andando nas ruas de Moscou, voltando de comprar seus mantimentos. No caminho de volta para seu apartamento, ele recebe um esbarrão aparentemente acidental por um transeunte. Ele nem pensa muito sobre isso no momento em que acontece, mas pouco depois se sente um pouco tonto e pensa que é um parasita da água local. Dai, ele vai para casa muito inocentemente e a próxima coisa que você fica sabendo é que ele morreu no chuveiro."

Citou Washington:

"Senhor Snowden, você é culpado por ter dito a verdade. E nós não queremos que essa verdade seja dita".

O advogado de Snowden, Anatoly Kucherena falou que o governo deveria se explicar sobre as ameaças feitas ainda sem limitações, e os nomes das pessoas citadas deveriam ser punidos.

4.3 DADOS COLETADOS

Os arquivos da NSA são diversos, há vários setores, e várias agências, e muitas vezes eram escritos em uma linguagem de difícil compreensão, repleto de termos internos específicos da agência.

Um dos primeiros programas que foi avistado pela lista marcada como principal pelo Snowden, na hora que Greenwald estava visualizando o conteúdo foi o BOUNDLESS INFORMANT, do qual faz a coleta de ligações e e-mails e o calculo das quantidades recebidas diariamente.

E há mais programas similares como o SHELLTRUMPET, BLARNEY, OAKSTAR, STORMBREW e FAIRVIEW.

O programa SHELLTRUMPET iniciou em 2007 e era apenas um analisador de coleta clássica que muitos programas aderiram sua tática mais posteriormente.

O programa BLARNEY foi criado e 1978 para obter com autorização da FISA, *Foreign Intelligence Surveillance,* lei de Vigilância de Inteligência Estrangeira para ter acesso as comunicações estrangeiras e terroristas. Em 2010 (dois mil e dez), os países que lhe possuíam propósitos eram incluídos: Brasil, França, Alemanha, Grécia, Israel, Itália, Japão,México, Coréia do Sul e Venezuela, além da União Européia e da ONU.

Com o acesso a “parceiros” corporativos da NSA ao alcaance de sistemas de telecomunicação estrangeiras o OAKSTAR mantém-se funcionando.

Parceiro do FBI o programa STORMBREW é receptor de todas ligações que entram de países a fora para os Estados Unidos, com sete acessos internacionais.

Um dos cinco maiores programas da NSA é o FAIRVIEW, funcionando desde 1985, foi criado para ser um dos maiores colhetador de dados.

Diferente do Prisma como de início citado, que coleta os dados diretamente dos servidores, os demais programas dependem da interceptação por cabos de fibra óptica e outros tipos de infraestrutura.

A coleta de dados por fibra óptica é denominada *upstream* e também podem inserir *malwares* em computadores, que ocasiona a Exploração da Rede Computacional (CNE), nessa prática eles se tornam “donos” de seu coomputador.

5. DIVULGAÇÃO DOS ARQUIVOS SOBRE ESPIONAGEM

Arquitetando um esquema, Snowden já sabia como lidar com a situação, o primeiro arquivo liberado e não muito apreciado com importância foi sua iniciativa de postar no sítio WikiLeaks apenas uma primeira denúncia, o começo de muitas coisas que vinham pela frente.

Certo do que queria e das consequências que sofreria cuidou para que ninguém próximo dele se envolvesse, então foi estruturando e conversando com jornalistas dos quais eram interessados e já escreviam sobre o tema desde o atentado de 2001, dentre eles Laura Poitras e Glenn Greenwald, a quem confiou e entregou todos os dados para que fossem bem delatados e a nível mundial, gravou um documentário com direção dos mesmos repórteres que usaram para revelar essas informações de suma importância no jornal The Guardian e depois no The Intercept.

Postando cada revelação por dia, separaram uma ordem de postagens de acordo com o tamanho impacto que elas iriam causar, aumentando a relevância dos arquivos gradualmente.

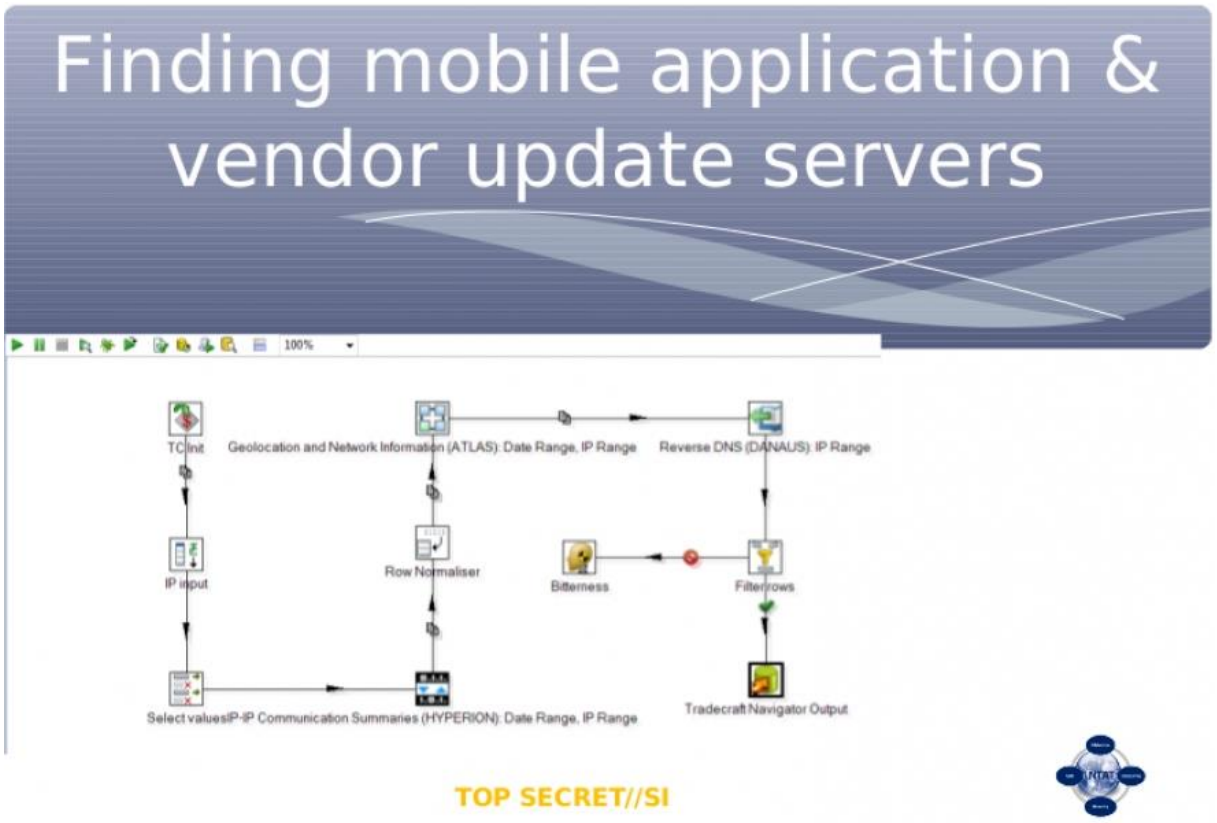


Figura 2 Legenda: Documentos descobertos por Edward Snowden mostram "projeto" da NSA para roubar dados dos usuários.

5.1 GLENN GREENWALD

O Ex-advogado especialista em Direito Constitucional e Civil, também jornalista Glenn Greenwlad, nasceu em Nova York (6 de março de 1967) , EUA, e nos últimos tempos mora no Rio de Janeiro, Brasil. Era colunista no jornal The Guardian e hoje tem vários livros escritos e trabalha no The Intercept, novo veículo de mídia criado junto com seus colegas Laura Poitras e Jeremy Scahill.

Foi colaborador para as denúncias de Edward Snowden, pois sempre trabalhou visando a política para questionar a posição do governo americano sobre o acontecimento terrorista ocorrido em 2001, dos quais não foram comprovados os culpados até hoje.

Escreveu por dois anos sobre a coleta de dados da NSA, feitas sem mandado na época em que Bush ainda presidia no país, conectando o mundo em seus escritos com questionamentos sobre a nossa liberdade e as escolhas que fazemos, dentro da mídia compartilhando nossa vida inteira nela e deixando para que todos possam ler ou utilizá-las de determinadas formas explicando sobre os mecanismos

históricos e atuais utilizado pelos governos mais avançados para montar estratégias de controle para montar estratégias de controle dos seus aliados e inimigos.

O primeiro contato antes de vir a surpreender-lhe sobre as informações que viam a seguir, nem foi dado como importante, ignorou o estranho e-mail por um tempo não se interessando muito, mas chegou uma hora que resolveu agir de tanta insistência da fonte anônima, se dispondo a baixar programas de criptografia e aprender a lidar com este novo mecanismo, para conseguir ler determinados documentos.

Teve que viajar à Hong Kong para encontrar-se com Snowden, desviando de toda a imprensa, quando encontrou-o, ficou muito surpreendido com o que encontrou, passaram horas a fio trabalhando juntos, gravando o documentário, e debatendo. A saída foi difícil mas acabou dando tudo certo, então Snowden se escondeu enquanto Greenwald e Laura publicavam no jornal as matérias, muitas vezes com alguns problemas, mas nada que não podia ser resolvido.

Um deputado americano, cujo nome é Peter King, abriu portas para que Glenn fosse muito questionado, e para uma grande iminência de que fosse processado, alegando que o mesmo estava infringindo o título 18 do Código Legal dos Estados Unidos, § 798, que torna ilegal a publicação de informações confidenciais que revelem criptografia ou inteligência de comunicação do governo.

5.2 LIVRO – SEM LUGAR PARA SE ESCONDER – EDWARD SNOWDEN, A NSA E A ESPIONAGEM DO GOVERNO AMERICANO

O livro descreve toda a jornada de Glenn Greenwald e Edward Snowden, através de e-mails, arquivos ultrassecretos e conversas criptografadas, e até pessoalmente, todos os momentos, até de desabafos, e quando não havia uma sequer saída.

Revela dados de suma importância ao mundo, estatísticas, descreve cada programa principal dentro da NSA, destacando a opinião de seu autor e os pensamentos de Edward Snowden sobre o mundo e as consequências da espionagem global. Trás uma linguagem jurídica e formal sobre o assunto.

Destaca a posição tanto do Greenwald quanto a do Snowden perante a espionagem, esclarecendo sua visão sobre o assunto e fundamentando-o na lei.

A intenção de Snowden sobre a espionagem era como ele mesmo disse: *“Quero iniciar um debate mundial sobre privacidade, liberdade na internet e os perigos da vigilância estatal.”* E sua primeira comunicação expunha totalmente seu objetivo ao tratar de se comunicar com Greenwald: *“A segurança das comunicações das pessoas é muito importante para mim.”*

6. ESPIONAGEM NO BRASIL

Sabe que a NSA utilizou de seus aparatos de espionagem para obter informações sobre a Petrobras. Caso que contradiz plenamente tanto o argumento utilizado pelo governo americano de que a NSA se dedica exclusivamente a combater o terrorismo, como uma declaração dada ao jornal americano *“The Washington Post”* a qual alega *“ não se engajar em espionagem econômica em qualquer área”.*

A partir desses documentos evidencia-se o interesse estadunidense em torno do petróleo brasileiro, afinal, informações obtidas por meio de espionagem poderiam favorecer algumas empresas nos leilões do Pré-Sal. O nome da Petrobras – maior empresa do país - com um faturamento anual de R$ 280 bilhões – é citado pelo menos quatro vezes. A NSA alegou, por meio de sua assessoria, que "não usa nossa capacidade de espionagem internacional para roubar segredos comerciais de companhias estrangeiras para dar vantagens competitivas a empresas americanas”.

“Estamos, senhor presidente, diante de um caso grave de violação dos direitos humanos e das liberdades civis, da invasão e captura de informações sigilosas relativas às atividades empresariais, e sobretudo de desrespeito à soberania nacional do meu país”, disse a presidente Rousseff em seu discurso de abertura da 68ª sessão da Assembleia Geral das Nações Unidas. A chefe de Estado expressou indignação quanto às recentes denúncias de espionagem norte-americana ao Brasil, incluindo a interceptação de e-mail e linhas telefônicas tanto de civis, como da própria presidente, e o acesso às informações da Petrobras.

A NSA confirma que o alvo principal não são os brasileiros (apesar dos 2,3 bilhões de dados espionados somente no primeiro mês de 2013), e o general Michael Hayden, ex-diretor da CIA e da NSA informa que o interesse dos EUA no Brasil nesse sentido, gira em torno dos cabos transatlânticos que transmitem voz e internet pelo mundo e que saem pela costa brasileira.

O Brasil é uma central importante na transmissão desses dados, com uma série de cabos passando por seu litoral.

Em um dos slides revelados por Snowden, é possível ver esse mapa como plano de fundo, com os cabos destacados na imagem. Isso quer dizer que espionam o Brasil não somente para espionar o país, mas para obter informações que passam por aqui por meio dos tubos transatlânticos.

A ideia de os EUA considerarem o Brasil um ponto estratégico, além é claro de recursos naturais que vão desde a Amazônia ao petróleo Pré-Sal, por si só já "justifica" a espionagem em empresas e ministérios estratégicos para o desenvolvimento e para a soberania nacional.

O histórico dos Estados Unidos em relação à América Latina mostra que espionagem e outras ações envolvendo a inteligência fazem parte do modus operandi da política externa do país — a chamada Operação Condor, que deflagrou diversos golpes militares contra governantes eleitos na América do Sul, é um exemplo disso.

A denúncia causou um sério mal-estar entre os governos do Brasil e dos Estados Unidos, pois a violação fere os princípios de não intervenção a respeito à soberania nacional brasileira.

Um caso que ocorreu é a licitação para execução do Sistema de Vigilância da Amazônia (SIVAM) onde a empresa vencedora da licitação é uma das mais importantes para as captações e rastreamento do Echelon. De modo que agora tudo descoberto na Amazônia será de pleno conhecimento da NSA.

Para proteger suas informações estratégicas, além de investir no aprimoramento do sistema nacional de inteligência, o Brasil precisa suprimir segredos ilegítimos ("sujos") e prescindíveis em favor daqueles realmente necessários e legítimos – os verdadeiros segredos de segurança nacional. No contexto da Era da Informação, o excesso de segredos e muitos funcionários com acesso a informações sigilosas comprometem tanto a obrigação democrática de transparência, quanto a capacidade dos governos de proteger informações estratégicas.

Um sistema de inteligência forte, capaz de neutralizar a espionagem estrangeira não basta quando qualquer funcionário com acesso a informações

sigilosas se torna um delator em potencial, capaz de vazar segredos em massa com facilidade e rapidez. Por essa razão é necessário que o Estado mereça a confiança do seu cidadão, o que exige transparência. Ser mais transparente para seus cidadãos e mais opaco para os olhares indiscretos dos espiões, e não o contrário: eis um dos importantes desafios para o Brasil.

A CPI, Comissão Parlamentar de Inquérito da Espionagem, que já foi encerrada após 180(cento e oitenta) dias, criada pela Senadora Vanessa Grazziotin em conjunto com outros Senadores, constituída por onze membros titulares e sete suplentes para substituí-los quando fosse necessário, foi abrangido nos termos do Requerimento nº 811 de 2013, para fins de descobrir a existência de uma estrutura de espionagem dos Estados Unidos que violasse os direitos instituídos na Constituição Federal brasileira, como grampos telefônicos e dados digitais dos cidadãos e do próprio governo.

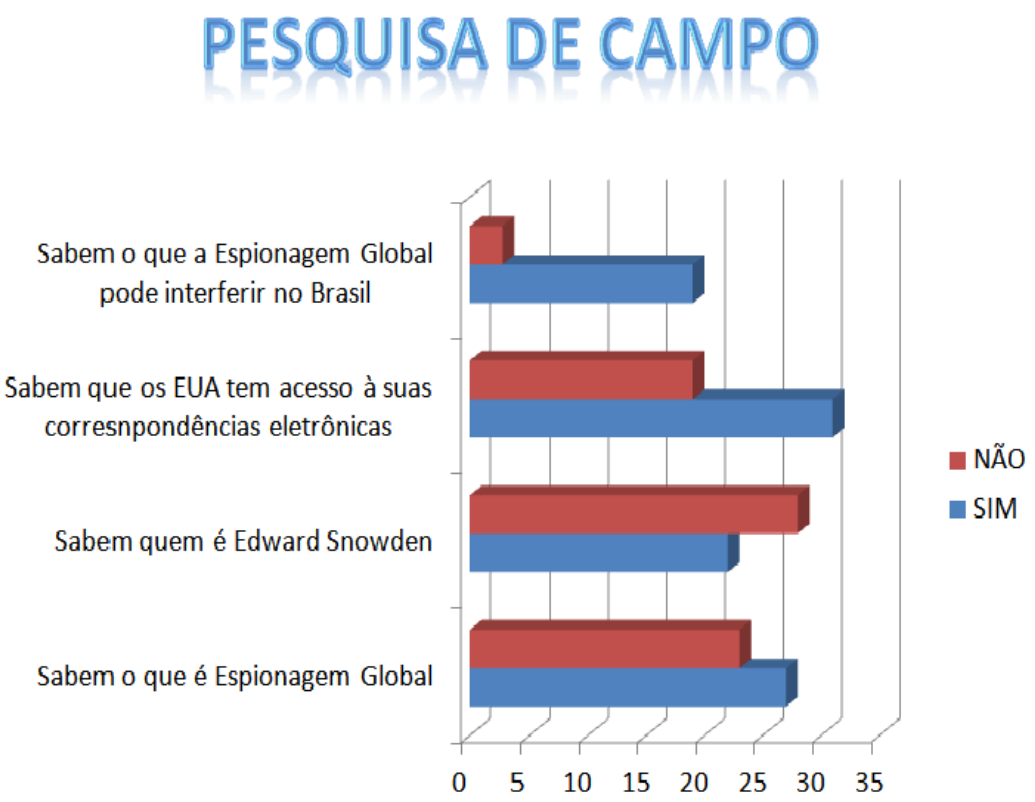
Em seu relatório final destacou que era necessária a criação da Agência Brasileira de Inteligência de Sinais colocando em observância que deve ser proposta do Executivo essa ação para a proteção e obtenção de dados de interesse do país.

No final de 2013 a Abin, Agência Brasileira de Inteligência apurou no momento em que estava realizando uma operação contra-espionagem salas que foram alugadas pela Embaixada americana em Brasília, após denúncias de determinados agentes estarem passando dos limites instalando equipamentos do centro de operações e análise de inteligência. Documentos encaminhados à Rousseff , revelaram 6 (seis) logradouros da embaixada americana que trabalham com sinais de rádio da Anatel (Agência Nacional de Telecomunicações) permitidos em outorga e válidos até 2019 em Brasília, no primeiro governo de Fernando Henrique Cardoso, é importante destacar que este faz uso limitado-privado com as informações recolhidas.

O Brasil obtém apenas um satélite próprio, que foi repassado à Embratel em 1997, e mais oito alugados dos EUA.

6.1 PESQUISA DE CAMPO – RELEVÂNCIA SOBRE O ASSUNTO ATUALMENTE E OPINIÕES

A pesquisa de campo busca analisar o conhecimento das pessoas sobre o assunto Espionagem Global, e como é demonstrado no gráfico a seguir, há um equilíbrio, na maior parte das questões as pessoas tem conhecimento porém distanciado sobre o assunto



7. FUNDAMENTAÇÃO LEGAL

7.1 LEGISLAÇÕES INTERNACIONAIS

A NSA obtém autorização judicial para realizar coleta de dados de empresas que atuam em solo norte-americano. Mas realizar espionagem em países estrangeiros é a própria missão da NSA. Segundo documentos vazados por Edward Snowden, o ex-colaborador terceirizado da agência que vazou as informações sobre a espionagem, a NSA rotineiramente comprometeu equipamentos de rede em outros países para instalar grampos.

A legislação dos Estados Unidos também não altera os compromissos que empresas norte-americanas têm com seu governo e com os governos de outros países em que atuam. Da mesma maneira que o Brasil impõe que essas empresas devem respeitar as leis brasileiras e que devem ceder dados solicitados pela Justiça daqui, independentemente do local em que esses dados estejam armazenados, os

Estados Unidos fazem o mesmo. Eles também podem pedir dados armazenados por empresas norte-americanas em qualquer lugar do mundo, e têm um tribunal secreto para isso (justamente para a população não ficar sabendo).

No campo do direito internacional público, o aspecto mais diretamente vinculado com os fatos da Espionagem relaciona-se com a dimensão de proteção aos direitos humanos. E, nesse domínio, com a necessidade de se respeitar a vida privada das pessoas.

O direito à privacidade sobressai como mecanismo de proteção contra a arbitrariedade praticada por agências de governo estadunidenses no vasculhar indiscriminada e indistintamente a vida de súditos de diferentes países, bem como seus respectivos governos. Os episódios ocorridos em relação à espionagem global, a juízo de muitos, é uma verdadeira ofensa a esse direito, consagrado em vários instrumentos internacionais.

Dessa forma, a interceptação irrestrita de comunicações, bem como a gravação injustificada de dados pelos serviços de inteligência dos EUA denota implacável violação à privacidade do ser humano. Essa forma de agir significa — sobretudo em democracias consolidadas como as envolvidas no episódio — ofensa gravíssima a esse direito.

Nessa ordem de ideias, convém recordar o que estabelecem alguns instrumentos internacionais em relação ao assunto. De início, a Declaração Universal dos Direitos Humanos [DUDH (1948)], que assim dispõe:

> Artigo XII. Ninguém será sujeito a interferência arbitrária na sua privacidade, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques.

É, por igual, oportuno consignar o estipulado em relação ao tema no Pacto Internacional sobre Direitos Civis e Políticos [PIDCP (1966)]:

> Artigo 17. 1. Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação. 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.

No ponto, a Convenção Americana de Direitos Humanos [CADH, Pacto de San José da Costa Rica (1969)] estipula:

> Artigo 11. Proteção da Honra e da Dignidade 1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade. 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação. 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.

A Convenção Europeia dos Direitos Humanos [CEDH (1950)] prescreve, por igual, que:

> Artigo 8°. Direito ao respeito pela vida privada e familiar. 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção de infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

A Carta dos Direitos Fundamentais da União Europeia (2010) contempla, sobre a matéria, o seguinte dispositivo:

> Artigo 7°. Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.

Dos textos transcritos, é apropriado destacar que: a) inexiste, para fins do direito que se almeja proteger, distinção de substância entre “privacidade” (DUDH) e “vida privada” (CEDH); cuida-se, em derradeira análise, tão só da tentativa de assegurar a concordância entre os textos inglês e francês; b) o Artigo 17 do PIDCP, cópia do Artigo XII da DUDH, é, no entanto, mais enfático na proibição. Com efeito, ele visa a proibir “interferência arbitrária ou ilegal”, ou seja, nenhuma interferência pode ocorrer, exceto nos casos previstos em lei; c) a CEDH, por seu turno, prevê (Art. 8°, II) limitações que podem ser fixadas ao direito proclamado (Art. 8°, I). Com exceção do “bem estar econômico do país”, as demais limitações previstas na CEDH

são compreensíveis. Contudo, mesmo em relação a esses limites é necessário juízo de ponderação, de razoabilidade e de clara percepção no sentido de que, na dúvida sobre se determinada forma de ação do Estado afronta essa proteção, deve-se garantir o direito à privacidade da potencial vítima.

Tão exato quanto o que foi acima mencionado é a circunstância de que as normas de direito internacional que, de tal ou qual forma, cuidam da matéria não definem o que se entende por “privacidade” ou “vida privada”. O conceito, de resto, é ambíguo também no plano jurídico interno dos Estados. Cuida-se provavelmente do direito mais difícil de definir no amplo catálogo internacional de direitos humanos. As definições variam enormemente à vista do contexto e do ambiente que se tem em consideração. A depender do interessado/intérprete, ele pode adquirir distintas acepções. Assim, por exemplo, contemplar proteção:

1. Da inviolabilidade física e mental do indivíduo e da liberdade intelectual e moral da pessoa; 2. Contra ataques à honra ou reputação do indivíduo e ofensas similares; 3. Do nome, identidade ou imagem do indivíduo contra uso não autorizado; 4. Contra a divulgação de informação abrangida pelo dever de segredo profissional; e 5. Contra ser espionado, vigiado ou molestado.

Os tratados transcritos representam avanço no plano internacional da proteção do direito à privacidade, mas vinculam, tão só, os Estados que formalmente se comprometeram por meio da ratificação/adesão. Essa circunstância não vale para a DUDH, é certo; não menos certo, entretanto, é que esse instrumento não é autoaplicável. A Declaração, em síntese, não dispõe de mecanismos asseguradores do cumprimento de suas disposições.

Já o PIDCP possui meios de implementação e monitoramento, que envolve a sistemática de relatórios encaminhados pelos Estados-partes, bem como o mecanismo opcional de comunicações interestatais. A esse sistema, o Protocolo Facultativo ao Pacto adiciona a possibilidade de petições individuais a serem apreciadas pelo Comitê de Direitos Humanos. O direito de petição individual mencionado colabora com a institucionalização da capacidade processual internacional dos indivíduos e constitui forma de proteção. Há, assim, algum modo de *International Accountability* (normas internacionais de contabilidade para o setor público).

Ocorre, entretanto, que os Estados Unidos da América não estão vinculados a esses meios de proteção. Eis aí uma contradição: o Estado que pretende ser o guardião dos direitos e garantias fundamentais não endossa os documentos internacionais relacionados com a matéria. Em relação aos seus nacionais, o governo americano adota um procedimento; já no tocante ao estrangeiro, a conduta é outra. “Faça o que eu digo, mas não faça o que eu faço”. Tratando-se de país com sólida tradição democrática, esse exemplo é, a vários títulos, lamentável.

No âmbito da ONU, convém recordar, desde logo, que o tratado constitutivo da Organização estabelece entre seus propósitos “promover e estimular o respeito aos direitos humanos e às liberdades fundamentais para todos” (Art. 1°, III, da Carta da ONU). Com o tempo, essa finalidade foi alargada — tanto no que tange aos instrumentos quanto no tocante às instituições — e adquiriu maior consistência. Nos dias de hoje, o Alto Comissário das Nações Unidas para os Direitos Humanos trabalha para oferecer conhecimento e apoio aos diferentes mecanismos de monitoramento dos direitos humanos no sistema onusiano. Ele é, de algum modo, o coração do sistema.

Dentro da essência de ampliar o debate em torno das graves violações perpetradas pelo governo dos Estados Unidos e de modo a levá-lo para o campo do multilateralismo, o governo brasileiro estimou adequado acionar os canais disponíveis nas Nações Unidas. Nesse sentido, o Brasil, em conjunto com a Alemanha, ofereceu proposta de resolução à Terceira Comissão da Assembleia-Geral (AG) da Organização. Ambos os países apresentaram, no dia 1° de novembro de 2013, projeto de resolução sobre o direito à privacidade na era digital. O assunto foi endereçado, como referido, à Terceira Comissão da AG, responsável por temas relacionados com aspectos sociais, humanitários e culturais.

A proposta bilateral em comento tem sua gênese vinculada às revelações feitas por Edward Snowden. Em conformidade com o que foi divulgado, os serviços de espionagem dos EUA desrespeitaram a privacidade de pessoas físicas e jurídicas de diversos países, com destaque para as comunicações telefônicas e eletrônicas de distintos chefes de Estado.

Entretanto, diferentes países, destacadamente europeus, hesitam em assumir atuação mais bem definida no plano diplomático. O cenário começa a se alterar com

revelações de que os Estados Unidos também espionaram alemães, franceses, espanhóis e, até mesmo, o Papa. Em face disso, o Brasil conseguiu apoio da Alemanha na tentativa de avançar na ONU proposta de resolução, a ser encaminhada à consideração da Assembleia-Geral (AG), com o objetivo de ampliar o direito à privacidade previsto no *Pacto Internacional de Direitos Civis e Políticos*. A proposta foi aprovada no dia 26 de novembro de 2013 na referida Comissão, tendo sido encaminhada à apreciação da AG no final do ano. Nessa ordem de ideias, o projeto em comento é o primeiro passo no sentido de conter, ainda que minimamente, a intrusão de determinados órgãos de governo de diferentes países nas comunicações, sobretudo online, de estrangeiros.

A desenvoltura da Assembleia-Geral das Nações Unidas não têm, em princípio, a capacidade de produzir norma vinculante de direito internacional. Elas, de resto, obedecem à dinâmica própria no campo internacional. Sua gênese se dá no contexto de uma organização internacional e o ato final de aprovação não prevê, em regra, audiência preliminar dos respectivos parlamentos dos Estados membros da organização.

As resoluções aprovadas com maioria qualificada, as que interpretam dispositivos do tratado constitutivo da ONU e as vocacionadas a codificar normas consuetudinárias na esfera internacional têm adquirido, para alguns, estatura de norma vinculante. Há, por igual, percepção de que, em determinados casos, as resoluções da Assembleia constituem evidência de direito consuetudinário internacional.

Essa constatação, no entanto, não cria, por si só, nova regra de direito consuetudinário. Representa, contudo, importante ponto de partida para o estabelecimento de norma costumeira.

Nessa ordem de ideias, ambos os países estimaram por bem apresentar o projeto de resolução em análise. O texto produzido foi o primeiro esboço, que recebeu sugestões e resultou aprovado no âmbito da Terceira Comissão. Com efeito, no dia 26 de novembro de 2013 essa Comissão aprovou, como mencionado, o texto. No entanto, a redação final sofreu alguma alteração. De forma a angariar o apoio dos EUA, da Grã- Bretanha, da Austrália, do Canadá e da Nova Zelândia, o

projeto foi amenizado em seu tom inicial. A principal modificação foi no sentido de afastar eventual relação direta entre espionagem e direitos humanos.

A proposta dá o tom do que se deseja: ampliar e reafirmar na era digital o direito à privacidade, contemplado em distintos instrumentos internacionais.

O projeto prescreve que os mesmos direitos que as pessoas possuem fora da rede *(offline*) devem ser protegidos em rede (*online*). O texto termina conclamando os Estados a respeitar os direitos humanos, de modo especial, o direito à privacidade; a adotarem medidas com vistas a cessar eventuais violações; a revisarem suas práticas, procedimentos e legislação no que tange ao tema; e a estabelecerem mecanismos nacionais independentes de supervisão de modo a assegurar transparência e responsabilização por possíveis transgressões. O projeto solicita, por fim, à Alta Comissária das Nações Unidas para os Direitos Humanos, Senhora Navanathen (Navi) Pillay, que apresente à AG relatório preliminar sobre a proteção do direito à privacidade no contexto da vigilância nacional e extraterritorial das comunicações, sua interceptação e coleta de dados pessoais em massa.

O teor do documento aprovado na Terceira Comissão e na AG não oferece elementos caracterizadores da *opinio juris*. Sendo assim, ele não tem, mesmo que em estado latente, o jeito de costume. Ou seja, o projeto como redigido não tem efeito jurídico gerador de obrigações internacionais. Em resumo, trata-se, ao menos no primeiro momento, de instrumento mais político do que jurídico. E mesmo sob essa ótica, ambos os governos não pretendem apontar os EUA como grandes vilões. Eles buscam, de um lado, dar recado político de suas insatisfações; de outro, caminhar no sentido de se ampliar a proteção para as comunicações online do direito à privacidade. Essa extensão, ao sentir de muitos, é necessária, visto que o Pacto Internacional de Direitos Civis e Políticos foi adotado pela XXI Sessão da Assembleia-Geral das Nações Unidas, em 16 de dezembro de 1966. Naquela altura, os meios de comunicação e de troca de informações eram muito mais rudimentares.

Historicamente, as resoluções da Assembleia-Geral representam mais a necessidade de manter o tema objeto do instrumento na agenda internacional e na direção de algo vinculante no futuro do que fonte cogente do direito internacional. Os exemplos podem ser contados à exaustão. Ocorre, no entanto, que, passados quase 69 anos do nascimento das Nações Unidas, tanto a doutrina quanto a jurisprudência

internacionais começam a indicar que determinados documentos têm, pelo menos, o requisito da *opinio juris* que todo costume encerra.

Todavia, o projeto trata-se de iniciativa que poderá, de modo eventual, tornar-se o embrião de algo mais consistente no sentido de se proteger o direito à privacidade na era digital. Essa perspectiva, havendo vontade política no campo internacional, já dispõe de instrumentos para sua implementação. Outro aspecto a considerar é o fato de que possível resolução no sentido do que se deseja carrega forte conteúdo moral.

No âmbito do direito comunitário, bem assim as iniciativas da UE no tocante tanto à proteção dos direitos humanos, sobretudo de seus cidadãos, quanto ao combate da espionagem indiscriminada mediante novas tecnologias. Essa análise revela-se importante no sentido de verificar outras práticas, bem como de constatar que a indignação do parlamento brasileiro com a espionagem realizada pela NSA não é ato isolado.

O direito das pessoas atualmente trata de variados temas. Isso se dá considerando, entre outras coisas, a globalização, a proliferação de normas, o aumento no número de atores com poder negocial, o fim do mundo bipolar e a emergência da democracia em seus domínios, ainda que relativamente mitigada. Ele, em síntese, penetra áreas que se relacionam ao econômico, social, cultural, técnico. Esse aumento nas faixas de atuação é consequência da crescente necessidade de os atores internacionais enfrentarem novas questões no seu relacionamento mútuo sem as amarras de muitos dos acontecimentos referidos.

Os atuais desafios perpassam diferentes domínios, que faz com que o direito internacional continue em constante evolução. A linha mediana deve prevalecer na compreensão das fases de desenvolvimento do direito internacional, mas, sobretudo, na projeção de seus desdobramentos futuros.

Nesse sentido, é imprescindível o estimulo à toda iniciativa no sentido de levar o assunto para foros multilaterais. Para tanto, as organizações internacionais [p. ex. ONU, Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), União Internacional de Telecomunicações (UIT)] representam espaço mais adequado para a ampliação dos debates em torno da espionagem global. É certo também que as organizações têm suas vicissitudes; não menos certo é que, apesar

dos seus enormes desafios, os debates realizados em seus domínios têm o condão de deixar o assunto em evidência.

Outra possibilidade é dispor de tratados tangenciais ao assunto, em relação aos quais a comunidade internacional possui mais consistência e consenso em seus desígnios. A via convencional pode consolidar, por exemplo, a iniciativa brasílico-germânica apresentada à consideração da ONU. Ela pode, ainda, partir para a elaboração de arcabouço jurídico internacional de forma a dar os contornos mínimos dos assuntos aqui analisados. Partir para uma governança global e mais democrática da Internet, por exemplo. Esse caminho é mais longo, mas é também aquele em que se podem vislumbrar maiores possibilidades de êxito futuro no sentido de se combater episódios como os denunciados pelo Sr. Edward Snowden.

O Ato Patriota (*Patriot Act*) é uma lei dos Estados Unidos sancionada pelo presidente republicano George W. Bush com partes renovadas pelo presidente democrata Barack Obama. Foi aprovada após os ataques terroristas de 11 de setembro de 2001. Seu objetivo geral é fortalecer o país reforçando a segurança interna e fornecendo as ferramentas necessárias para interceptar atos terroristas. É dividido em 10 partes e abrange muitos assuntos.

A aprovação e a renovação do Ato Patriota foram extremamente controversas. Os defensores afirmam que ele foi útil em uma série de investigações e prisões de terroristas, ao mesmo tempo em que críticos defendem o fato de que o ato concede muito poder ao governo, ameaça os direitos civis e prejudica a própria democracia que pretende proteger.

O Tribunal de Vigilância da Inteligência Estrangeira dos Estados Unidos (Fisc, na sigla em inglês), que supervisiona atividades de vigilância, justificou como legal a prática da Agência de Segurança Nacional (NSA) americana de espionar registros telefônicos nos Estados Unidos, pois não viola os direitos básicos dos norte-americanos à privacidade por estar amparado por uma lei conhecida como Ato Patriota, na qual entre suas dez partes, a Medida II autoriza a intercepção das comunicações caso estiverem ligadas com atividades terroristas e permite que as agências de cumprimento da lei compartilhem informações relacionadas às atividades terroristas com autoridades federais. Autoriza tambem a vigilância móvel, permitindo oficiais de usar quaisquer meios disponíveis para interceptar a comunicação. Além disso, permite que o governo peça os arquivos para os

fornecedores de serviços de comunicação com os detalhes sobre o uso específico do serviço pelo cliente.

Porém, a Corte Federal de Apelação dos Estados Unidos do 2º Circuito julgou que o programa de coleta de registros telefônicos da Agência Nacional de Segurança dos Estados Unidos (NSA) é ilegal.

Segundo o tribunal, a lei antiterrorista - Ato Patriota não autorizava a NSA a manter essas informações de cidadãos norte-americanos.

Ao tomar essa decisão, o juiz Gerard Lynch, concedeu uma vitória à American Civil Liberties Union (ACLU), uma ONG norte-americana de defesa dos direitos e liberdades civis. Já o congresso americano fica pressionado a decidir rapidamente se o governo deverá ou não dar um fim ao polêmico programa de espionagem antiterrorismo.

Na prática isso significa dizer que o tribunal, no entanto, não emitirá uma ordem judicial para interromper o programa com o argumento de que a lei irá expirar de qualquer modo no próximo dia 1º de junho. Lynch disse que seria *"prudente ceder ao Congresso a possibilidade de decidir qual tipo de vigilância é permitida, dado que os interesses da segurança nacional estão em jogo".*

O governo ainda pode recorrer da decisão, mas isso só deve ser feito se o se o Ato Patriota for renovado. Caso o governo recorra, o processo pode inclusive chegar à Suprema Corte dos Estados Unidos, que terá de decidir se a espionagem fere ou não a Constituição do país.

No dia 31 de maio de 2015, o Senado dos Estados Unidos da América se reuniu para definir se partes do Ato Patriota seriam renovadas.

Caso a legislação não seja aprovada, algumas disposições fundamentais do chamado "*Patriot Act*" vão expirar, e a Agência de Segurança Nacional que desligar um enorme sistema de vigilância.

A espionagem global foi retratada por Edward Snowden, como uma violação as Terceira e Quarta Emendas da Constituição dos Estados Unidos da América.

A Quarta Emenda à Constituição dos Estados Unidos é uma das emendas feitas na Carta dos Direitos. Refere-se à proteção contra buscas e

apreensões arbitrárias e foi instituída como resposta aos abusos do controverso *writ of assistance*, um tipo de mandado geral de busca emitido pelo governo colonial britânico e que foi uma importante fonte de tensão na América pré-revolucionária. A emenda proíbe a busca e apreensão sem que haja motivo razoável e mandado judicial baseado em causa provável.

De acordo com a Quarta Emenda, busca e apreensão (incluindo prisão) devem ser de alcance limitado, baseando-se em informações específicas transmitidas ao tribunal emissor, geralmente por um agente da justiça.

A jurisprudência acerca da Quarta Emenda refere-se a três questões centrais: que atividades governamentais constituem "busca" e "apreensão", o que constitui a *causa provável* para essas ações, e como as violações da Quarta Emenda devem ser encaminhadas.

Evidências descobertas como resultado de uma busca ilegal também podem ser consideradas como "frutos da árvore venenosa", ou seja, se a fonte da prova (a "árvore") se corrompe, então qualquer coisa que venha dela (o "fruto") também estará corrompido.

A Quinta Emenda à Constituição dos Estados Unidos institui garantias contra o abuso da autoridade estatal, tais como o julgamento pelo grande júri, o direito de permanecer calado e evitar assim a auto-incriminação, o direito de ser julgado apenas uma vez sobre mesmos fatos (vedação ao *bis in idem*), o direito a justa compensação por bens desapropriados. Além disso, a emenda traz a cláusula de devido processo legal, segundo a qual "*ninguém pode ser privado de sua vida, liberdade ou propriedade sem o devido processo legal*".

7.2 LEGISLAÇÃO BRASILEIRA

Apesar de a atividade de inteligência ser ainda precária no Brasil, pode-se dizer que o ordenamento jurídico brasileiro é bastante restritivo a ações que violem as liberdades fundamentais dos cidadãos; os órgãos de Estado, nesse caso, operam, principalmente segundo os limites da lei e no escopo da autorização judicial (que no país é condição é *sine qua non* para qualquer quebra de sigilo de correspondência, telefônico, e de comunicações eletrônicas). O Brasil, é um dos

principais países que ordena, judicialmente, a entrega de informações judiciais. Isso leva a crer que há, nesse caso, estrita observação dos procedimentos legais para o acesso a bases de dados públicos e privados. Atos de espionagem usualmente atingem o direito fundamental de intimidade do cidadão, mas podem também gerar repercussões na esfera cível.

Amparada pelo Código Civil de 2002, a privacidade realizou-se no bojo do capítulo referente aos direitos da personalidade e com atenção ao tratamento jurisprudencial que o tema vinha recebendo - não destoando, portanto, da técnica de atualização utilizada pelo legislador em diversas outras ocasiões.

A privacidade é componente fundamental à formação da pessoa. A sutil definição do que é exposto ou não sobre alguém, ou a quem se deseja revelar algo, mais do que uma preferência ou capricho, define propriamente o que é um indivíduo - quais suas fronteiras com os demais, qual seu grau de interação e comunicação com seus conhecidos, seus familiares e todos os demais.

Há, uma série demasiadamente complexa de nuanças que definem o que deve ser considerado privado em certa ocasião, tanto que a salvaguarda que o legislador fornece ao cidadão ao início do artigo 21 do Código Civil de 2002 - “A vida privada da pessoa natural é inviolável…” - acaba por ser muito menos um imperativo do que um elemento a ser sopesado dentre outros para que se verifique sua real extensão. Uma breve análise do significado da privacidade em nosso ordenamento a partir de suas bases normativas será o objetivo deste ensaio.

A emanação de um valor na redação do artigo 21 do CC2002 se evidencia, quanto menos, pelo vigor demonstrando pela determinação em se considerar inviolável a vida privada. A inviolabilidade é, tradicionalmente, atributo dos direitos da personalidade, ao lado de outros como a irrenunciabilidade e imprescritibilidade que acabam por compor um perfil muito específico para este instituto, justamente por estar tão próximo à finalidade última do ordenamento jurídico - a proteção da pessoa humana.

O repúdio à violação da vida privada, apesar da sua ressonância como mandamento e regra geral, não é algo que se pode qualificar concretamente com facilidade, o acaba amenizando o caráter absoluto - e, portanto, algo retórico - que

aparentemente possui a norma. Na menção feita pelo CC2002 à “vida privada”, sente-se de imediato o eco da disposição constitucional de proteção à vida privada, presente no artigo 5º, X da Constituição Federal - que, literalmente, protege não somente esta como também a intimidade, a hora e a imagem.

A profusão de termos dos quais a doutrina brasileira se utiliza para representar a privacidade, é considerável; além de "privacidade" propriamente dita, podem ser lembradas a vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros termos menos utilizados, como “privatividade” e “privança”, por exemplo.

A verdade é que a ausência de uma definição amparada, que reflita uma consolidação do seu tratamento semântico, não é um problema localizado da doutrina brasileira.

A Constituição Federal de 1988 impõe em seu artigo 5º,X - “são invioláveis a intimidad e, a vida privada, a honra e as imagens das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação” estão sendo violados.

O Código Civil reforça a disposição em seu artigo 21, trazendo a previsão de tutela judicial inibitória para os casos de violação da intimidade. Temos ainda a proteção à intimidade na Convenção Americana de Direitos Humanos e da Declaração Universal de Direitos Humanos.

Portanto, além da eventual responsabilidade criminal do agente que pratica espionagem ou colabora com ela, pode haver sua responsabilização civil, seja por danos materiais e/ou morais. Isso porque a ação de espionagem atentará sempre contra o patrimônio ou a intimidade do indivíduo, quando não, contra ambos.

Logo, conforme os manuais militares, espionar envolve diretamente um serviço de inteligência. Ou seja, de obtenção de informação. E se proteger contra espionagem envolve um serviço de contra inteligência, ou seja, de segurança da informação. E um não existe sem o outro. Isso mostra que praticamente estamos o tempo todo na Sociedade do Conhecimento ou espionando ou sendo espionados.

Atualmente, a espionagem vem muitas vezes abraçada com o conceito de vazamento de informação, que significa revelar para terceiro não autorizado uma informação sigilosa obtida de forma legítima ou clandestina sem a ciência do proprietário da mesma.

O Marco Civil da Internet – que é de suma importância para determinar os direitos e deveres da comunidade envolvida com a Internet no Brasil – trata, em parte, disto: do que é tolerável e do que não é em termos de guarda de registros de acesso e de comunicação por empresas de TI, e do maior ou menor acesso, pela via judicial, a esses dados. Postergar o Marco Civil – como vem sendo feito no Congresso em virtude do forte lobby exercido, em grande medida, pelas operadoras de telecomunicação que atuam no Brasil – gera insegurança jurídica que pode levar a abusos parecidos com o PRISM.

Mesmo que tenha crescido o investimento na capacitação do funcionalismo público nos últimos anos, especialmente no que diz respeito à operação no ciberespaço (a excelência do Brasil no combate a ilícitos cibernéticos e na arrecadação de tributos são casos de destaque internacional), é preciso que se reconheçamas limitações estruturais que o país enfrenta quando é comparado com os Estados Unidos. Afinal, de todo o *backbone* das redes de telecomunicação de alcance mundial, apenas uma ínfima parte toca o território brasileiro. E, do agregado de empresas que controlam as bases de dados correspondentes, uma parcela ainda menor se localiza no país. Isso dificulta não apenas a execução de medidas coercivas, mas também o próprio alcance do consentimento necessário para aabertura de tais bases de dados.

8. ATUALIDADES

No dia 31 de maio do ano de 2015, o Senado americano não cumpriu o prazo de renovação da Lei Patriota, ou *Act Patriot* que acabou expirando. Após muitas discussões, foi aprovada e sancionada a Lei da Liberdade, ou *Freedom Act* pelo presidente dos Estados Unidos, Barack Obama, da qual impõe a proibição da coleta de dados indiscriminada pelo país sob chamadas telefônicas, só ocorrendo a mesma através de um mandado judicial expedido pela FISC, e toda ligação tem dever de ser armazenada nas companhias telefônicas apenas.

No dia 04 de junho de 2015, Snowden revelou mais um documento demonstrando o aumento da espionagem nas redes sociais que ocorre desde 2012, com o objetivo principal de monitorar o fluxo de comunicação entre seus cidadãos e de outros países. O governo federal americano alertou que hackers da China teriam invadido o sistema e coletado informações de funcionários públicos federais.

9. CONCLUSÃO

Pôde-se observar que nas mais variadas épocas a espionagem possuiu objetivos específicos e sofreu uma evolução, hoje em dia controla o mundo, em parte, e dispõe da melhor tecnologia existente.

Para adquirir essa magnitude os governos criaram diversos programas consequentemente ocasionando a violação da privacidade das pessoas.

A espionagem já foi modo de defesa em estratégias de guerra mas nos últimos anos ultrapassou os limites impostos pela lei.

Deixou marcos na história, como o Echelon que foi o primeiro e mais importante sistema de espionagem já criado do qual é apegado a justificativa de funcionar para combater atentados terroristas, assim impedindo-os.

O país que mais desenvolveu e ampliou as técnicas de vigilância é os Estados Unidos da América, que atualmente é muito visado neste contexto pelas mídias eletrônicas. Isso apenas ocorreu por decorrência das denúncias de Edward Snowden que buscou levar à público a violação da Declaração dos Direitos Humanos, que defende a privacidade assim como pactos e conciliações que destacam ser incorreta a intervenção da vida privada dos cidadãos, para obter como reotrno a consciência do que é corriqueiro nos dias de hoje com a tecnologia em massa, condenando sua vida fazendo o que acredita ser correto, pois esses fatores infringem nossa liberdade fundamental impostas na ONU.

As violações estão ocasionando os mais variados estranhamentos entre Nações, com possibilidade de corte de relações entre Estados, entretanto tampouco há distinção do público para o privado.

A questão base é: Você arriscaria a violação de sua privacidade em prol da segurança de seu país? Ainda há variadas discussões e opiniões se é correto ou não serem violados diversos direitos dos quais tem objetivo de não haver o controle total do Estado sob nossas vidas, rumo em que a Espionagem Global está nos encaminhando.

10. GLOSSÁRIO

Data center É um local projetado para guardar servidores e outros componentes.

Intelsat *International Telecommunications Satellite Organization*. Consórcio intergovernamental que financiava uma rede de salétites de comunicação.

Inmarsat Existe há mais de 30 anos e é a maior provedora do mundo de comunicação satelital móvel.

República democrática alemã Era formada pelo Leste Europeu, o lado socialista de Berlim na Guerra Fria, construída em 1949 ocupava as zonas que atualmente constituem os estados alemães de Berlim, Brandemburgo, Mecklemburgo-Pomerânia, Saxônia, Saxônia-Anhalt e Turíngia.

Muro de berlim Construção erguida em 1961 pelo regime socialista de hoje extinta Alemanha Oriental que destinava separar Berlim que estava dividida entre capitalismo e socialismo, também foi grande simbolo da Guerra Fria.

Cabos transatlânticos Cabos submarinos que passam pelo oceano atlântico, eles transmitem eletricidade, dados, voz ou outro sinal.

Status quo Se apresenta, como uma expressão utilizada para restabelecer o desequilíbrio promovido na vida de alguém.

Modus operandi Modo de operação. Utilizado para designar uma maneira de agir, operar ou executar uma atividade seguindo sempre os mesmos procedimentos.

Sistema onusiano Contribuição Político-Jurídica da Organização das Nações Unidas.

Opinio juris Em direito Consuetudinário é o segundo elemento necessário para estabelecer um costume juridicamente vinculatino. Denota uma obrigação sujetiva.

Países Anglófonos Países falantes da língua inglesa.

Backbone Em português espinha dorsal. O backbone é o trecho de maior capacidade de rede e tem por objetivo conectar várias redes locais.

FISC ou Foreing Intelligence Surveillance Court ou tribunal FISA, supervisiona os pedidos de vigilância mandados contra estrangeiros espiões dentro dos Estados Unidos.

Criptoanálise Estuda formas de tornar legível uma mensagem codificada ou cifrada sem conhecer o seu algorítmo de conversão.

11 . REFERÊNCIAS BIBLIOGRÁFICAS

Nas Cercanias do Palácio. Disponível em:<http://www.Cartacapital.com.br/revista/761/nas-cercanias-do-palacio-3844.htmL >. Acesso em: 18/03/2015.

Hoje na História: 1943- Prédio do Pentágono é Inaugurado. Disponível em: < http: //operamundi.uol.com.br/conteudo/ historia/26574/hoje+na +historia+1943+-+predio+do+pentagono+e+inaugurado+nos+eua.shtml >. Acesso em: 21/02/2015.

GREENWALD, Glenn. Dez dias em Hong Kong.In: –.Sem Lugar Para Se Esconder. Edward Snowden, a NSA e a espionagem do governo americano. Tradução: Fernanda Abreu. Rio de Janeiro: Sextante,2014.288pg.

Novos Documentos da NSA Revelam Planos de Distribuir Spyware Pelo Google Play. Disponível em: <http://info.abril.com.br/noticias/seguranca/2015/05/novos-documentos-da-nsa-revelam-planos-de-distribuirspyware-pelo-googleplay.shtml. Acesso em: 24/04/2015.

UMA NOVA GUERRA FRIA.In: Jusnavegndi, 2014.Disponível em: <http://jus.com.br/artigos/30252/uma-nova-guerra-fria>. Acesso em 19 out. 2014

A ESPIONAGEM NO DIREITO BRSILEIRO. In: Jusnavegandi, 2012.Disponível em: <http://jus.com.br/artigos/22668/a-espionagem-no-direito-brasileiro>. Acesso em 03 set. 2014

A ESPIONAGEM NORTE-AMERICANA NO BRASIL E A HEGEMONIA DOS ESTADOS UNIDOS, POR JOANA SOARES. In: Boletimmundorama, 2013. Disponível em: <http://mundorama.net/2013/10/12/a-espionagem-norte-americana-no-brasil-e-a-hegemonia-dos-estados-unidos-por-joana-soares/>.Acesso em 07 jan. 2015

O QUE É A NSA? In: Canaltech, 2014. Disponível em: <http://canaltech.com.br/o-que-e/espionagem/O-que-e-a-NSA/>.Acesso em 12 mar. 2015

ESPIONAGEM GLOBAL. In: Defesanet, 2013.Disponível em:<http://www.defesa net.com.br/cyberwar/noticia/11491/Espiona gem-Global/>. Acesso em: 12 mar. 2015.

Denúncias de Snowden revelam mais un tipo de espionagem dos EUA. Disponível em: < http://g1.globo.com/jornal-nacional/noticia/2015/06/denuncias-de-

snowden-revelam-mais-um-tipo-de-espionagem-nos-eua.html >. Acesso em: 05/06/2015.