CARLOS ROBERTO DE ALMEIDA CERQUEIRA FILHO

OS ARQUIVOS SNOWDEN:

o episódio e os reflexos no Brasil

Trabalho de Conclusão de Curso - Monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia.

Orientador: Cel Av R/1 Josué Batista de Jesus Neto

Rio de Janeiro
2014

C2014 ESG

Este trabalho, nos termos de legislação que resguarda os direitos autorais, é considerado propriedade da ESCOLA SUPERIOR DE GUERRA (ESG). É permitido a transcrição parcial de textos do trabalho, ou mencioná-los, para comentários e citações, desde que sem propósitos comerciais e que seja feita a referência bibliográfica completa.
Os conceitos expressos neste trabalho são de responsabilidade do autor e não expressam qualquer orientação institucional da ESG

_____
Assinatura do autor

Biblioteca General Cordeiro de Farias

Cerqueira Fº, Carlos Roberto de Almeida
Os arquivos Snowden : o episódio e os reflexos no Brasil / Auditor-Fiscal da Receita Federal do Brasil, Carlos Roberto de Almeida Cerqueira Filho - Rio de Janeiro : ESG, 2014.

53 f.: il.

Orientador: Cel Av (R1) Josué Batista de Jesus Neto
Trabalho de Conclusão de Curso – Monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra como requisito à obtenção do diploma do Curso de Altos Estudos de Política e Estratégia (CAEPE), 2014.

1. Segurança cibernética. 2. Segurança da informação. 3. Edward Snowden. I. Titulo.

A todos da minha família que contribuíram com a minha educação oficial e a formação de meu caráter.

A minha gratidão, em especial, à minha esposa Luciana e às minhas filhas Marina, Larissa e Letícia pela compreensão, como resposta aos momentos de minhas ausências e omissões, em dedicação às atividades da ESG.

AGRADECIMENTOS

Aos estagiários da Turma “ESG 65 anos pensando o Brasil”, a melhor turma do CAEPE, pelo excelente ano de bom convívio e pelas novas e valorosas amizades.

Ao Corpo Permanente da ESG pelos ensinamentos e orientações que me fizeram refletir, cada vez mais, sobre a importância de se estudar o Brasil com o compromisso que deve ter um cidadão brasileiro.

É preferível ser irresponsável e estar com a verdade a ser responsável e no erro.

Winston Churchill

RESUMO

Esta monografia aborda o episódio intitulado “Arquivos Snowden” como um dos mais relevantes acontecimentos no contexto das atividades de inteligência internacional. O objetivo deste estudo é, a partir de uma breve descrição do citado episódio e das formas de ação do programa de inteligência norte-americano PRISM, analisar a reação brasileira, e desta forma, identificar possíveis vulnerabilidades técnicas e políticas no Brasil, fornecendo subsídios que sirvam de base para a implementação de um projeto capaz de atender às necessidades do país no contexto da contrainteligência, da segurança cibernética e da segurança das informações. A metodologia adotada comportou uma pesquisa bibliográfica e documental, visando buscar referenciais teóricos, além da experiência do autor como profissional da segurança da informação. O campo de estudo delimitou-se ao episódio “Arquivos Snowden” e à reação brasileira, embora no decorrer do trabalho haja citações de outros incidentes de segurança da informação e de outras nações que tenham reagido ou não ao episódio. Os principais tópicos são: o episódio “Arquivos Snowden” propriamente dito, o programa PRISM, a reação brasileira e o marco civil da internet. Há também uma análise que indica ações positivas a serem desenvolvidas e cuja implementação poderia contribuir para a formulação de uma proposta de projeto de segurança de informação capaz de atender às necessidades do Estado brasileiro, apontando ainda, para a necessidade de integração entre os diversos órgãos da administração pública que possuem competência normativa e experiência nas áreas de estudo envolvidas.

Palavras-chave: Segurança da informação. Segurança cibernética. Edward Snowden.

ABSTRACT

This monograph discusses the episode "Snowden Files" as one of the most relevant events in the context of foreign intelligence activities. The aim of this study is, from a brief description of that episode and the action mechanisms of the U.S. intelligence PRISM program, analyze the Brazilian reaction, and thus identify potential technical and policy vulnerabilities in Brazil, providing subsidies that serve as the basis for the implementation of a project that can meet the needs of our country in the context of counterintelligence, cyber security and information security. The adopted methodology involved bibliograph and documental research, aiming to seek theoretical frameworks beyond the author's experience as a information security professional. The field of study is delimited to the episode "Snowden Files" and the Brazilian reaction, although in this work there are quotes from other information security incidents and from other nations that have reacted or not to the episode. The main topics are: the episode "Snowden Files" itself, the PRISM program, the Brazilian reaction and the civil internet law. There is also an analysis that indicates positive actions to be developed and the implementation that could contribute to the formulation of a information security project proposal able to meet the needs of the Brazilian State, also pointing to the need for integration between the various government departments that have legislative competence and experience in the involved areas of study.

Keywords: Information security. Cybersecurity. Edward Snowden.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

NSA	National Security Agency

SUMÁRIO

1 INTRODUÇÃO

Edward Snowden, analista de sistemas norte-americano e ex-contratado da Agência de Segurança Nacional norte-americana (NSA), publicou detalhes secretos do sistema de Vigilância Global da NSA, no ano de 2013, revelando ao mundo a existência de um projeto de monitoramento global, o PRISM, que vigiou conversas telefônicas e transmissões de dados na Internet de cidadãos americanos e estrangeiros, inclusive brasileiros. Neste contexto, as autoridades brasileiras protestaram contra o comportamento estadunidense e desde então vêm anunciando mudanças nas normas e na estrutura das comunicações de Estado e da sociedade, com o propósito de diminuir a fragilidade na proteção dos dados, seja na transmissão ou no armazenamento destes. Dentre as mudanças nas normas, destaca-se a Lei nº 12.965 de 23 de abril de 2014, a qual estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, e ficou conhecida como o “Marco Civil da Internet” no Brasil.

No entanto, pode-se questionar: O Brasil protege adequadamente as suas informações sensíveis ao Estado? A partir deste questionamento principal, cabem também as seguintes indagações: o Brasil tem o direito de questionar a atividade de inteligência desenvolvida por outros países? E pode o país tratar assuntos de segurança do Estado no âmbito de uma lei que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil?

O objetivo geral deste trabalho, portanto, é analisar estas questões, procurando apresentar argumentos e recomendações, a partir do exame da literatura disponível e recente.

Partindo do incidente de segurança intitulado “Arquivos Snowden”, onde busca-se mostrar os seus antecedentes e como ocorreu, um destaque foi dado ao PRISM, o já citado projeto de monitoramento. Além disto, este trabalho também faz constar os reflexos no Brasil e seus desdobramentos normativos, mas notadamente o “Marco Civil da Internet”, quando em breve análise, buscou-se identificar os artigos que sofreram influência direta do episódio supracitado. Além disto, há um estudo de um modelo de infraestrutura de segurança cibernética, de comunicações e informações que procura mitigar problemas de vulnerabilidades de segurança existentes.

A questão proposta é fundamental em função de alguns argumentos. O primeiro diz respeito à formação do autor, superior em Informática, e à sua trajetória como profissional da área de segurança da informação e comunicação. O segundo argumento, de natureza social, revela que a sociedade brasileira está preocupada com a sua liberdade de comunicação e sua soberania, e deseja proteger suas informações e comunicações por meio de dispositivos e canais mais seguros, desde que não mitigue suas liberdades individuais. O terceiro refere-se ao interesse acadêmico, principalmente nas questões de inteligência, contrainteligência, segurança e defesa cibernética e segurança das informações e comunicações. Secundariamente, há os reflexos nas relações internacionais, notadamente entre Brasil e Estados Unidos da América. Nestes aspectos, novos estudos permitirão aprofundamento e detalhamento.

Trata-se de uma pesquisa bibliográfica e documental, baseada em reportagens e matérias técnicas, e de cunho qualitativo sobre as questões delimitadas já apresentadas, à luz de conceitos sólidos das áreas afetadas, além do código de prática para a gestão da segurança da informação e da posição de profissionais das diversas áreas de estudo envolvidas no trabalho.

De forma preliminar, os conceitos que perpassam a discussão são: comunicações informatizadas e globalizadas; segurança da informação e comunicação; inteligência e contrainteligência; segurança e defesa cibernética; e relações internacionais.

Esta monografia encontra-se estruturada em cinco seções. A introdução descreve o problema, as principais finalidades da pesquisa, sua justificativa e as opções teórico-metodológicas empregadas. A segunda seção apresenta a fundamentação teórica, isto é, o suporte teórico para os estudos, análises e reflexões sobre os dados e/ou informações coletadas. A terceira seção resume o episódio intitulado “Arquivos Snowden” (“The Snowden Files”, originalmente) e explica com algum detalhe o que seria o projeto PRISM, já citado como o principal programa de espionagem da agência norte-americana de espionagem. A quarta seção apresenta os reflexos no Brasil do vazamento dos dados de inteligência, uma breve análise sobre os artigos do “Marco civil da Internet” que sofreram influência do episódio “Arquivos Snowden” e termina com uma discussão da situação descrita no trabalho, em que o autor propõe um modelo integrado de estrutura governamental para lidar com as questões da segurança da informação e da segurança cibernética.

A quinta seção é a conclusão que responde aos principais questionamentos propostos no trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

O presente trabalho foi desenvolvido com base em outras pesquisas, jornalísticas e técnicas, e encontrou sustentação teórica nos mais diversos campos da atividade pura e aplicada da segurança da informação, tais como: o conjunto de conceitos e práticas de gestão da segurança da informação, tomando como base a ABNT/NBR ISO/IEC 27002:2005[1]; as atividades de inteligência e de contrainteligência; a segurança a defesa cibernética; e outras atividades que, de uma forma ou de outra, tratam diretamente ou indiretamente da segurança da informação. E para adentrar no arcabouço técnico pesquisado, preliminarmente precisou-se conceituar dados, informação e ativos de informação.

Dados são elementos de partida que servem de base para o tratamento e sobre os quais um computador efetua as operações necessárias à tarefa em questão. Os dados são uma representação dos fatos, conceitos ou instruções de uma maneira normalizada que se adapte à comunicação, interpretação e processamento pelo ser humano ou através de máquinas automáticas.

Rezende e Abreu definem informação como todo o dado trabalhado, útil, tratado, com valor significativo atribuído a ele. O dado é o elemento da informação, que isoladamente não transmite nenhum conhecimento (REZENDE, 2000).

J. Paulo Serra define informação como o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, animal ou máquina) que a recebe (SERRA, 2007).

Ativos de informação é qualquer coisa que tenha valor para a organização. Raphael Mandarino Jr. conceitua ativos de informação como os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso (computadores, equipamentos de comunicação e de interconexão), os sistemas utilizados para tal, os sistemas de informação de modo geral, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso (MANDARINO, 2009).

1 Esta norma estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos definidos nesta Norma provêem diretrizes gerais sobre as metas geralmente aceitas para a gestão de segurança da informação.

A segurança da informação, portanto, é caracterizada pela preservação da tríade básica: confidencialidade, integridade e disponibilidade da informação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005). Entende-se por confidencialidade a garantia de que a informação só será acessível a pessoas autorizadas. A integridade está relacionada à “exatidão” e “completeza” da informação. A disponibilidade é a garantia de que os usuários autorizados terão acesso à informação e aos ativos correspondentes sempre que necessário.

Gurpreet Dhillon defende que a tríade básica da segurança da informação apresentada é restrita (DHILON, 2001). E princípios como responsabilidade, integridade, confiança e ética são imprescindíveis em um contexto de mudanças organizacionais. Tais princípios estão relacionados aos profissionais que vão manusear a informação, principais responsáveis pelo seu sigilo. E sem entrar propriamente na discussão de possíveis benefícios e/ou malefícios decorrentes da divulgação dos dados de inteligência realizada por Snowden, estes princípios adicionais no trato das informações são fundamentais para evitar que um usuário autorizado a manipular informações, o faça com propósito diverso do preconizado pelo órgão detentor da titularidade das informações.

A atividade de Inteligência compreende, resumidamente, a produção de conhecimentos e de dados e a salvaguarda destes, que ao Estado interessa preservar. Para o correto exercício da inteligência, é impositivo o uso de metodologia e de técnicas voltadas para a produção do conhecimento, que permitam afastar a prática de ações meramente intuitivas e a adoção de procedimentos sem uma orientação racional.

A atividade de contrainteligência tem como objetivo neutralizar a inteligência adversa, proteger o conhecimento sensível e manter o sigilo das operações de inteligência para evitar que agentes de outros países ou de instituições concorrentes penetrem no governo, forças armadas, agências de inteligência, ou em setores estratégicos de empresas.

A segurança cibernética refere-se à proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (redes de comunicações e de computadores e seus sistemas informatizados) que controlam as infraestruturas críticas nacionais. Também abrange a interação com órgãos públicos e privados envolvidos no funcionamento das

infraestruturas críticas nacionais, especialmente os órgãos da Administração Pública Federal (CARVALHO, 2011).

A defesa cibernética é o conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os nossos sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente. No contexto do preparo e emprego operacional, tais ações caracterizam a Guerra Cibernética (CARVALHO, 2011).

Além das teorias já apresentadas, cabe ainda registrar que esta pesquisa também considerou as mais diversas opiniões e trabalhos realizados por especialistas da área de segurança da informação, inteligência e contrainteligência e segurança e defesa cibernética sobre os assuntos abordados.

E para relatar o episódio “Arquivos Snowden”, foi necessário recorrer também a matérias e pesquisas jornalísticas, uma vez que se trata de um episódio recente, e portanto ainda carente de análises técnicas aprofundadas na literatura científica. No entanto pode-se dizer que o objetivo do trabalho foi atingido, pois a fundamentação teórica não restou prejudicada.

3 OS 'ARQUIVOS SNOWDEN'

3.1 O INCIDENTE

O mundo mal havia digerido o episódio WikiLeaks, em que diversos documentos secretos da diplomacia norte-americana foram divulgados em ampla mídia universal, quando surgiu um novo escândalo de vazamento de documentos internos do governo dos Estados Unidos, desta vez capitaneado por Edward Snowden, um profissional de computação norte-americano, em um episódio ainda mais ousado do que o WikiLeaks sob o ponto de vista da atividade de inteligência, pois documentos de governo ainda mais protegidos foram colocados à apreciação pública. Tal episódio foi intitulado “Arquivos Snowden” ou “Snowden Files”, como ele é conhecido pela mídia internacional.

Edward Snowden foi administrador de sistemas na Agência Central de Inteligência norte-americana (CIA); instrutor de contraespionagem da Agência de Inteligência de Defesa (DIA); contratado pela agência de inteligência privada Dell, dentro da Agência de Segurança Nacional (NSA) no posto avançado do Japão; e contratado pela consultoria Booz Allen Hamilton, dentro do centro da NSA no Havaí. E foi justamente trabalhando nestas duas últimas empresas que ele teria feito a captura dos milhares de documentos confidenciais que ele veio divulgar em junho de 2013. Mas apenas citar as funções profissionais que desempenhou e as empresas em que trabalhou não permite delinear sua personalidade e identificar sua motivação para realizar ato tão polêmico e radical. Em vista disto, tornou-se necessário descrever um breve resumo histórico dos principais acontecimentos de sua vida pessoal e profissional, o que o autor deste trabalho passa a tratar nos próximos parágrafos.

Filho de Lonnie Snowden, um oficial da guarda costeira dos Estados Unidos da América, de perfil conservador, libertário e com visões fortemente patriotas; e de Elizabeth Barret Snowden, com a qual foi viver após uma tumultuada separação entre seus pais, Edward Snowden teria sofrido um grave problema de saúde quando ainda cursava o ensino médio, motivo pelo qual sua formação escolar teria desandado, conforme relembra seu pai (HARDING, 2014). Desta forma, mesmo tendo cursado posteriormente uma espécie de supletivo (GED – General Educacional Development) e ainda ter frequentado cursos de computação, seus

conhecimentos de informática, ao que parece, teriam sido adquiridos por autodidatismo. Esta falta de uma qualificação lastreada em uma educação formal pode ter sido a causa de uma possível insegurança e consequente necessidade de afirmação, o que pode explicar, em parte, a sua vontade de divulgar os documentos secretos e não se manter anônimo após a divulgação dos mesmos, exibindo-se ao mundo para obter reconhecimento pelos seus feitos, considerados de alta dificuldade técnica.

Em que pese ter crescido próximo às instalações físicas da Agência de Segurança Nacional norte-americana (NSA), Snowden não via muitas perspectivas de ingressar na atividade governamental, mas sua intimidade com computadores era notória, o que muito o ajudou em sua vida profissional. Certa vez postou na internet: “Eu sou um MCSE (Microsoft Certified Solutions Expert) sem diploma ou autoridade, que mora em Maryland. Leia-se desempregado” (HARDING, 2014).

A invasão liderada pelos Estados Unidos ao Iraque, em 2003, fez com que ele pensasse em uma carreira militar, a exemplo de seu pai: “Eu queria lutar na Guerra do Iraque porque, como ser humano, sentia uma obrigação de ajudar a libertar as pessoas da opressão” (HARDING, 2014).

Em maio de 2004, Snowden alistou-se nas Forças Especiais americanas, onde mesmo os recrutas sem prévia experiência poderiam tornar-se soldados de elite. Esta oportunidade veio bem a calhar com sua condição: sem educação formal, sem experiência e alinhado ideologicamente com o propósito da operação militar, pelo menos em teoria. No entanto, mesmo possuindo bom condicionamento físico, sua visão era limitada, acima de seis graus de miopia. E sua condição anatômica, de pés estreitos e de difícil adaptação aos calçados, rendeu-lhe diversos problemas. O maior deles, no entanto, não veio de incompatibilidade física, mas de propósitos, pois poucos de seus colegas compartilhavam da mesma causa nobre ou desejo de ajudar cidadãos. Seus superiores queriam simplesmente matar pessoas, preferencialmente muçulmanos: “A maioria do pessoal que nos dava treinamento parecia incentivado a matar árabes, não a ajudar alguém”, relata (HARDING, 2014).

Concluído o treinamento de Forças Especiais, foi iniciado o treinamento de infantaria, em que Snowden quebrou as duas pernas e acabou sendo dispensado do Exército.

Ao retornar a Maryland, ele começou a trabalhar como especialista em segurança no Centro de Estudos Linguísticos Avançados, na Universidade de

Maryland. Aparentemente começou como guarda de segurança e depois migrou para tecnologia da informação. Um detalhe muito importante é que o tipo de trabalho formal que começou a desempenhar tinha relação direta com a atividade de espionagem norte-americana. É possível que sua passagem pela vida militar tenha criado as condições necessárias para seu ingresso no mundo dos serviços de inteligência. Fato é que Snowden já estava dentro da NSA, no campus da Universidade de Maryland, e seu ego já estava começando a inflar: “para começar, esse negócio de diploma é besteira, pelo menos no mercado doméstico. Se você 'realmente' tem 10 anos de experiência sólida em T.I.... você PODE, SIM, conseguir um emprego muito bem pago em T.I.”, escreveu em julho de 2006. E ainda complementou em outra ocasião: “É, trabalhar no T.I. do Departamento de Estado lhe garante acesso a tudo de máximo sigilo” (HARDING, 2014).

Em 2007, a CIA o enviou para Genebra, na Suíça, em sua primeira turnê internacional, com o encargo de manter a segurança da rede de computadores daquela agência estadunidense.

Defensor fervoroso do capitalismo e do livre mercado, Snowden apoiou a candidatura de Ron Paul à presidência dos Estados Unidos, em 2008. Paul era o mais famoso expoente do libertarismo americano e a figura que mais incorporava as visões dissidentes de direita de Snowden. Além disso, o citado político fez longa carreira no Congresso norte-americano, marcada por posições contrárias ao socialismo, à economia keynesiana, ao Federal Reserve, à intervenção norte-americana no exterior e, principalmente, à vigilância do governo. Esta posição libertária e notadamente contra qualquer tipo de vigilância do governo tem forte relação com o comportamento futuro de Snowden no episódio do vazamento dos documentos oficiais. Mas até este momento ele ainda não havia percebido “onde teria se metido”, pois seus trabalhos não lhe agrediam, pelo contrário, só o faziam sentir-se ainda mais confiante.

Mas um evento em particular o influenciou negativamente no sentimento que ele possuía sobre seu trabalho. Trata-se de um episódio em que operadores da CIA tentaram recrutar um banqueiro suíço de modo a obter informações financeiras secretas. Snowden teria informações de que fizeram esta operação embebedando o banqueiro e depois o incentivando a ir pra casa dirigindo, o que resultaria em sua prisão pela polícia suíça. Um agente disfarçado então teria se oferecido para ajudar e aproveitou o incidente para formar uma amizade bem-sucedida com o banqueiro,

para depois recrutá-lo: “Muito do que vi em Genebra realmente me desiludiu quanto à forma como meu governo funciona e qual seu impacto no mundo. Percebi que eu fazia parte de algo que estava causando muito mais danos do que benefícios”, concluiu Snowden (HARDING, 2014).

Sua insatisfação com o seu governo foi aumentando na mesma proporção em que Snowden se afirmava em suas convicções e se aprofundava em suas missões.

Certa vez, preenchendo o formulário anual de autoavaliação da CIA, detectou falhas na ficha de pessoal da rede e as apontou para seu chefe. Mesmo não tendo concordado inicialmente, seu chefe acabou permitindo que Snowden fizesse um teste de suscetibilidade do sistema, contra invasão, o que teria ocorrido por meio da inserção de códigos e textos não maliciosos, provando seus argumentos de vulnerabilidade. Apesar de seu chefe imediato ter ratificado o teste, um gerente acima, com quem Snowden anteriormente tivera um conflito, descobriu o que ele havia feito e ficou furioso, o que o levou a produzir um relatório depreciativo na ficha de Snowden. Este episódio foi importante para formar opinião de que fazer queixas através de canais internos não seria produtivo, ou pior, levaria à punição, o que ficou muito bem registrado na mente de Snowden.

Em fevereiro de 2009, Snowden pediu demissão da CIA e foi trabalhar como terceirizado em uma unidade da NSA, em uma base militar norte-americana no Japão, o que durou até 2012. Foi nesta época que Snowden descobriu os principais programas de vigilância em que a agência trabalhava e suas supostas irregularidades: “A intenção deles é tomar conhecimento de todas as conversas e tipos de comportamento no mundo” (HARDING, 2014). Este comportamento da NSA, se não começou com o episódio de 11 de setembro de 2001, foi acentuado consideravelmente após tal data. Snowden já poderia ser considerado um delator em potencial.

Um certo dia, realizando uma tarefa do tipo “busca por palavra suja”, isto é, uma limpeza minuciosa no sistema para remover material indevido, Snowden se deparou com um relatório confidencial, de 2009, redigido pelo inspetor-geral da NSA: um documento de 51 páginas que detalhava como a administração Bush havia realizado seu programa de escutas ilegais após o 11 de setembro de 2001. O programa, de codinome STELLAR WIND (Vento Estelar), envolveu a coleta de conteúdo e metadados de milhões de norte-americanos, sem mandado judicial. Para Snowden era o fim. Tratava-se de uma prova incontestável de que altos funcionários

do governo norte-americano estavam quebrando a lei: “Você não pode ler algo assim sem se dar conta do que aquilo significa para todos os sistemas que temos”, disse ele ao periódico New York Times (HARDING, 2014).

Mas Snowden já tinha visto de perto o calvário de uma outra pessoa que também havia se desiludido com a NSA: Thomas Drake. Trata-se de um veterano condecorado da Força Aérea norte-americana, e também da Marinha dos Estados Unidos, que veio a ser executivo da NSA. Drake tornou-se descontente com os programas secretos de combate ao terrorismo da agência, em especial com uma ferramenta de coleta de inteligência, o Projeto TRAILBLAZER. Drake sentiu que violava a quarta emenda à constituição norte-americana ao realizar buscas e apreensões arbitrárias. A partir daí, Drake decidiu levantar seus questionamentos através de todos os canais corretos: desde seus chefes na NSA até o inspetor-geral da agência, o mesmo que redigiu o relatório do Programa STELLAR WIND. Procurou ainda o Pentágono e o Congresso norte-americano. Frustrado, foi ao periódico Baltimore Sun. Considerada ingênua, sua abordagem só teria enfurecido as autoridades norte-americanas. Até que finalmente, em 2007, o FBI invadiu sua casa e Drake foi condenado a 35 anos de prisão. Somente quatro anos depois, em 2011, o governo retirou as queixas a partir de um acordo com o próprio Drake, em que ele teria se declarado culpado de uma contravenção menor, momento em que ele foi posto em liberdade condicional.

Para Snowden, Drake foi uma inspiração. A maneira punitiva como as autoridades perseguiram Drake, o convenceu de que não fazia o menor sentido trilhar o mesmo caminho: “O sistema não funciona. Você tem que denunciar o delito aos seus principais responsáveis”, admite (HARDING, 2014). Snowden sabia que além de Drake, haveria outros dissidentes na NSA que teriam sofrido em circunstâncias similares. E como terceirizado externo da aludida agência, trabalhando naquela época para a Dell, ele nem teria direito à mesma proteção de denunciante que Drake.

Em dezembro de 2012, Snowden já estava convencido de que precisava contatar jornalistas. E foi numa verdadeira via-crúcis de dimensões hollywoodianas que Snowden decidiu para quais jornalistas contaria sua estória, como iria contactá-los, como iria convencê-los a fazer uso de ferramentas criptográficas para transmissão das informações, como iria encontrá-los pessoalmente, enfim, todo

processo de libertação daquilo que poderia ser facilmente intitulada a sua “reclusão ideológica”.

Talvez não tenha havido uma “gota d'água” ou um momento específico em que ele tenha decidido contar a sua estória. E explica:

> Imagino que a experiência de cada um seja diferente, mas para mim não houve um único momento. Estava vendo toda uma ladainha interminável de mentiras dos altos funcionários para o Congresso – e, portanto, para o povo americano – e fui compelido a agir ao perceber que o Congresso, especificamente a Gangue dos Oito, apoiava inteiramente as mentiras. Ver alguém na posição de James Clapper – diretor de inteligência nacional – descaradamente mentindo para o público sem a devida repercussão, é evidência de uma democracia subvertida. O consentimento dos governados não existe se eles não foram informados (HARDING, 2014).

Snowden referiu-se à declaração feita por James Clapper, diretor da NSA, em março de 2013, ao comitê de inteligência do Senado de que o governo dos Estados Unidos coletava dados sobre milhões de norte-americanos “não intencionalmente”. A afirmação era falsa, conforme o próprio Clapper admitiu posteriormente.

Em 20 de maio de 2013, Snowden voou do Havaí para Hong Kong, onde, no início de junho, reuniu-se com os jornalistas Glenn Greenwald e Laura Poitras, quando lhes entregou numerosos documentos da NSA e assim revelou ao mundo o maior conjunto de programas de vigilância já realizados na história. Em 9 de junho, quatro dias depois do primeiro programa da NSA ter sido exposto pela imprensa, Snowden revelou sua identidade em um vídeo filmado por Poitras e publicado pelo periódico britânico The Guardian (GREENWALD, 2013a).

Em 14 de junho, o Departamento de Justiça dos Estados Unidos acusou Snowden de violar a Lei de Espionagem e de roubo de propriedade do governo (FINN, 2013), punível com até 30 anos de prisão (HERSZENHORN, 2013). Snowden teve seu passaporte revogado pelo Departamento de Estado de seu país em 22 de junho daquele ano. Segundo o presidente russo, Vladimir Putin, Snowden se reuniu com diplomatas russos enquanto estava em Hong Kong (NOVOSTI, 2013) e em seguida viajou para Moscou (MAYER, 2014), cujo aeroporto foi local em que ficou aguardando uma definição sobre sua entrada na Rússia por 39 dias, durante os quais ele pediu asilo em 21 países. Em 1º de agosto, as autoridades russas concederam-lhe um ano de asilo temporário renovável.

Os documentos vazados por Snowden revelaram a existência de inúmeros programas de vigilância global, muitos deles executados pela NSA e pelos Cinco

Olhos (Estados Unidos da América, Reino Unido, Canadá, Austrália e Nova Zelândia), com a colaboração de empresas de telecomunicações e de governos europeus. Dentre os documentos, foram revelados a existência dos programas: BOUNDLESS INFORMANT; PRISM, o programa eletrônico de mineração de dados; a ferramenta analítica XKEYSCORE; o projeto de interceptação TEMPORA, executado pelo GCHQ (Government Communications Headquarters) do Reino Unido; o ponto de acesso MUSCULAR; e o banco de dados FASCIA, que contém trilhões de registros de dispositivo de localização. Em 2014, foram revelados o britânico Threat Joint Research Intelligence Group; o banco de dados DISHFIRE; o monitoramento de redes de mídia social em tempo real SQUEAKY DOLPHIN; e o programa NERVO ÓPTICO, uma coleta de imagens de webcam privadas.

Logo em seguida, a publicação online *Interception*, criada por Poitras, justamente para divulgar os documentos revelados por Snowden, informou que a NSA estava trabalhando em parceria com a DEA (Drug Enforcement Administration) dos EUA, e nesta parceria, gravaria o conteúdo de todas as chamadas de telefonia celular, realizadas nas Bahamas (SNOWDEN, 2014a). Slides vazados por Snowden e revelados no livro de Greenwald, *"No Place to Hide"*, lançado em maio de 2014, mostrou que objetivos declarados da NSA eram de "coletar tudo", processar tudo", explorar tudo", "participar de tudo", "vasculhar tudo" e "saber de tudo".

O tamanho exato da divulgação de Snowden é desconhecida, mas há estimativas colocadas por vários funcionários governamentais de que 15.000 ou mais arquivos de inteligência australianos, mais de 58 mil arquivos de inteligência britânicos e cerca de 1,7 milhão de arquivos de inteligência dos Estados Unidos teriam sido afetados.

E a disposição exata dos arquivos extraídos da NSA por Snowden é incerta. Em outubro de 2013, Snowden disse ao periódico *The New York Times* que todos os documentos classificados que havia obtido foram dados a jornalistas que ele conheceu em Hong Kong, antes de voar para Moscou, e não manteria nenhuma cópia para si mesmo (RISEN, 2013). Em janeiro de 2014, Snowden disse a um entrevistador da TV alemã: "Eu dei todas as minhas informações para o público americano e para jornalistas americanos que estão relatando sobre questões americanas" (SEIPEL, 2014).

Em março de 2014, o general do exército norte-americano Martin Dempsey, presidente do Joint Chiefs of Staff, declarou que a maior parte dos documentos que

Snowden extraiu dos mais altos níveis de segurança não tinha nada a ver com a fiscalização governamental sobre as atividades domésticas e estariam relacionados às capacidades militares, às operações táticas, às técnicas e aos procedimentos norte-americanos (CAPRA, 2014).

No entanto, segundo Snowden, ele não teria entregue os documentos de forma indiscriminada a jornalistas: “Eu cuidadosamente avaliei todos os documentos divulgados para garantir que cada um deles representava legitimamente o interesse público”, afirmou (GREENWALD, 2013a).

Além disto, uma outra informação, desta vez divulgada pela própria NSA, é a de que Snowden não teria agido sozinho. Ele teria obtido ajuda de funcionários da própria NSA para acessar e copiar diversos dos documentos que foram expostos.

A NSA editou um memorando interno que mostra que eles teriam conseguido identificar três funcionários que teriam dado acesso a Edward Snowden em diversos documentos classificados como “Top Secret” (BAUMAN, 2014). Além disto, Snowden teria recebido um certificado digital que era utilizado para acessar a NSANet, a intranet da NSA. Com ele foi possível garimpar aquilo que era de mais secreto dentro da própria NSA.

3.2 O PROGRAMA PRISM

De todos os programas de vigilância divulgados por Snowden, destaca-se o PRISM, um programa que permite que os funcionários da NSA coletem vários tipos de dados de usuários em poder de serviços de Internet, incluindo histórico de pesquisas, conteúdo de e-mails, transferências de arquivos, vídeos, fotos, chamadas de voz e vídeo, detalhes de redes sociais, log-ins e quaisquer outros dados em poder das empresas de internet.

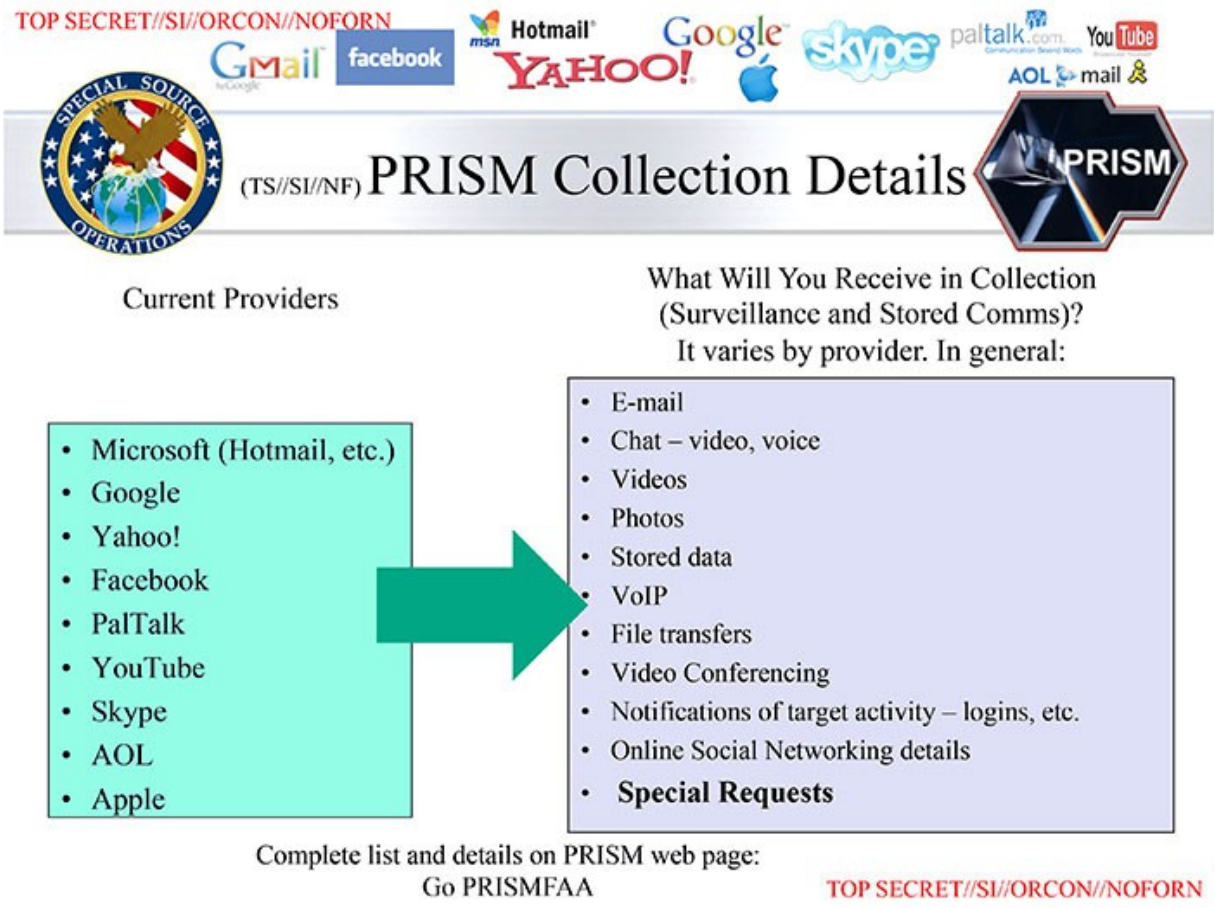
Não é o propósito deste trabalho esgotar os detalhes do programa PRISM, mas tão somente mostrá-lo, por ter sido o mais importante dos programas, inclusive por ter sido possível identificar a presença do Brasil em, pelo menos, uma das apresentações relacionadas a ele. Para isto, cabe caracterizá-lo como um complexo projeto de monitoramento, interagindo com empresas, ferramentas de internet, pontos de acesso de comunicações e governos estrangeiros aliados na tarefa de monitoramento. Por isso, cabe fazer constar algumas informações, a seguir.

Uma apresentação de 41 slides, preparada para orientar agentes de inteligência, e contida entre os documentos vazados, afirma que o programa PRISM é executado com a participação das seguintes empresas: Microsoft, Google, Facebook, Yahoo!, Apple, YouTube, AOL, Paltalk e Skype (figura 1). A NSA afirmou ainda ter acesso direto aos servidores de algumas delas, como: Google, Facebook, Apple e outras gigantes da internet nos Estados Unidos (EUA..., 2012; GELLMAN, 2013a). As empresas listadas na citada apresentação da NSA negaram seu envolvimento com a agência de inteligência americana (MATSUURA, 2013).

O PRISM coleta os dados que são posteriormente armazenados e analisados por meio de outros programas de vigilância que fazem parte do sistema de vigilância e espionagem implantado pela NSA. Alguns exemplos de programas que utilizam os dados coletados através do PRISM são: MYSTIC, um programa que é parte integrante e crítica do PRISM, feito para interceptação de áudio (voz) e gravação de "100 por cento" das chamadas telefônicas de um país estrangeiro, o que permite a NSA ou outras agências americanas a retroceder e ouvir na íntegra conversas telefônicas, mesmo um mês depois de terem ocorrido (MICK, 2014); o NUCLEON, que os slides de apresentação da NSA indicam ser o programa usado para analisar dados de voz reunidos através do programa PRISM (GELLMAN, 2013b); e o DISHFIRE, que processa e armazena mensagens SMS coletadas em nível mundial.

Foi utilizando o DISHFIRE que a NSA reuniu quase 200 milhões de mensagens de texto por dia de todo o mundo, incluindo a localização, as redes de contato e detalhes do cartão de crédito do emissor da mensagem, de acordo com documentos ultrassecretos revelados pelo periódico britânico *The Guardian*. (NSA..., 2014). Uma análise mais detalhada dos dados teria sido realizada posteriormente pelo PREFER (BALL, 2014), um sistema usado pela NSA que recebe os dados coletados via PRISM, os identifica e os classifica em pelo menos 11 categorias diferentes, incluindo log-ins, fotos, vídeos e metadados (NSA..., 2014).

Figura 1: Slide de apresentação do PRISM: os colaboradores.



Fonte: http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

Além do PREFER, foi revelado ainda o PINWALE, um banco de dados usado para armazenar e analisar vídeo e outros conteúdos selecionados pelo PRISM e por outros programas, sendo capaz de armazenar uma grande quantidade de dados por até cinco anos (GREENWALD, 2013b).

Além das parcerias com as empresas de serviços de internet, a NSA também desenvolveu diversas parcerias corporativas com fabricantes de equipamentos utilizados em redes de dados, para receber dados e informações de clientes de empresas de Tecnologia da Informação e de Comunicações. Uma das formas de facilitar o recebimento dos dados se daria por meio da fabricação de equipamentos com backdoors, que são falhas intencionais na segurança dos equipamentos. Estas falhas facilitariam a inserção de dados maliciosos pela NSA, e tais códigos fariam a tarefa de enviá-los à citada agência.

No livro “Sem lugar para se esconder”, de Glenn Greenwald, foram revelados os nomes das empresas fabricantes de equipamentos parceiras na NSA. (DIRECT..., 2014). Seriam elas: Cisco, Oracle, Intel, Qwest, EDS, Verizon, Microsoft e IBM. Além destas, estaria também a Qualcomm, uma das principais empresas no fornecimento de chipsets e outras tecnologias, incluindo processadores para dispositivos móveis, bem como de hardware e software distribuídos ao redor do mundo e em parceria direta com a NSA, fabricando e vendendo no mercado mundial equipamentos com backdoors para os malwares que facilitam a espionagem da aludida agência norte-americana.

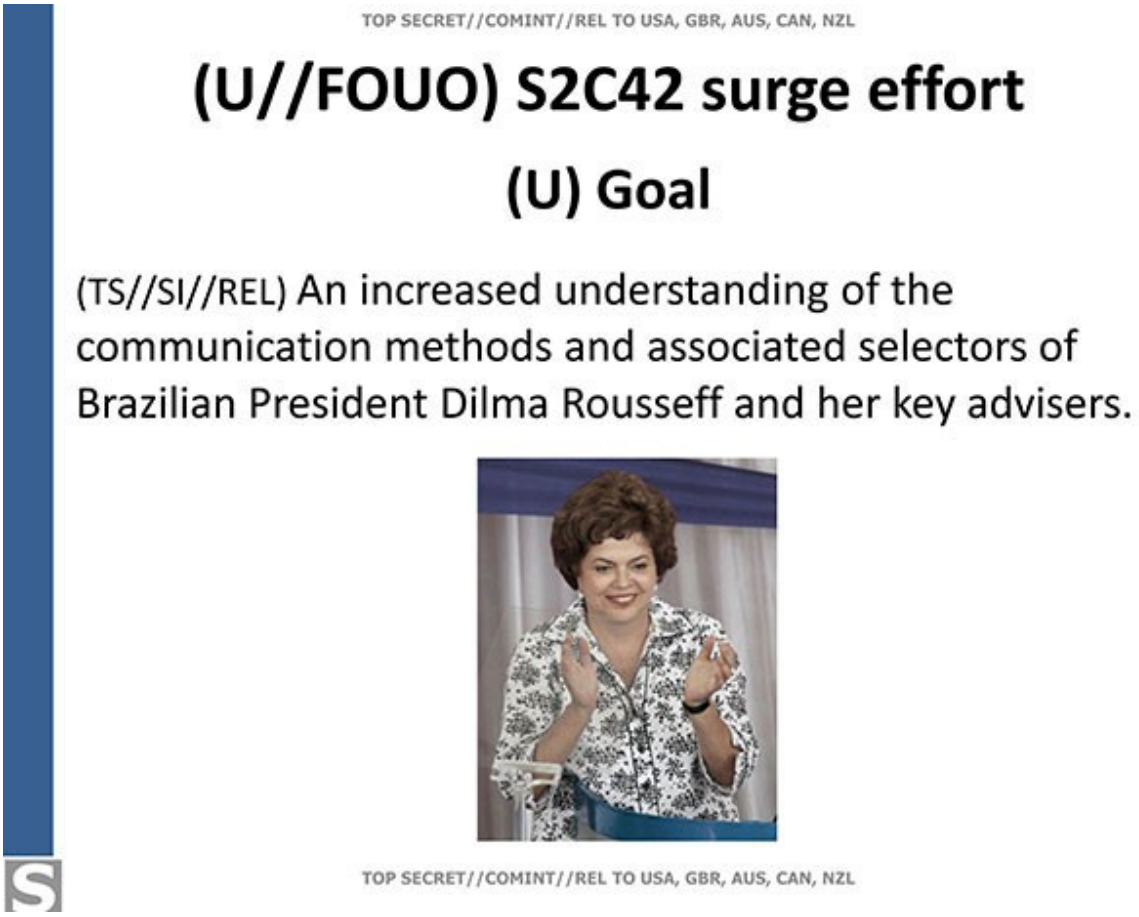
Além disto, em documentos sobre um determinado programa, o FAIRVIEW, há referência a uma empresa como sendo a “parceira chave” da NSA nos programas de vigilância. Esta empresa não havia sido identificada inicialmente na documentação Snowden. No entanto, a empresa considerada “parceira chave” pela NSA foi identificada, em 23 de outubro de 2013, pelo periódico *The Washington Post,* como sendo a AT&T (HEIL, 2013).

A NSA também vem coletando dados da Internet por meio de cooperação com agências de inteligência no exterior. Neste caso, as parcerias são geralmente feitas através de acordos, como é o caso do acordo dos chamados Cinco Olhos (Five Eyes, em inglês), cujos países já foram citados neste trabalho. Estes países cooperam entre si sob o comando da NSA, e o fazem através de suas agências de inteligência (ROSSI, 2013), como mostra os slides das apresentações que “vazaram”.

Em muitos dos slides, na barra superior, pode ser vista a indicação dos países que dividem o programa com a NSA (figura 2). A inscrição cita os Cinco Olhos por meio de uma sigla: US – Estados Unidos da América, AUS – Austrália, CAN – Canadá, GBR – Grã-Bretanha e NZL – Nova Zelândia. No caso em que existe a

cooperação com agências de inteligência, há o compartilhamento dos programas e das funções.

Figura 2: Slide de apresentação do PRISM: quem recebe as informações.



Fonte: http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html

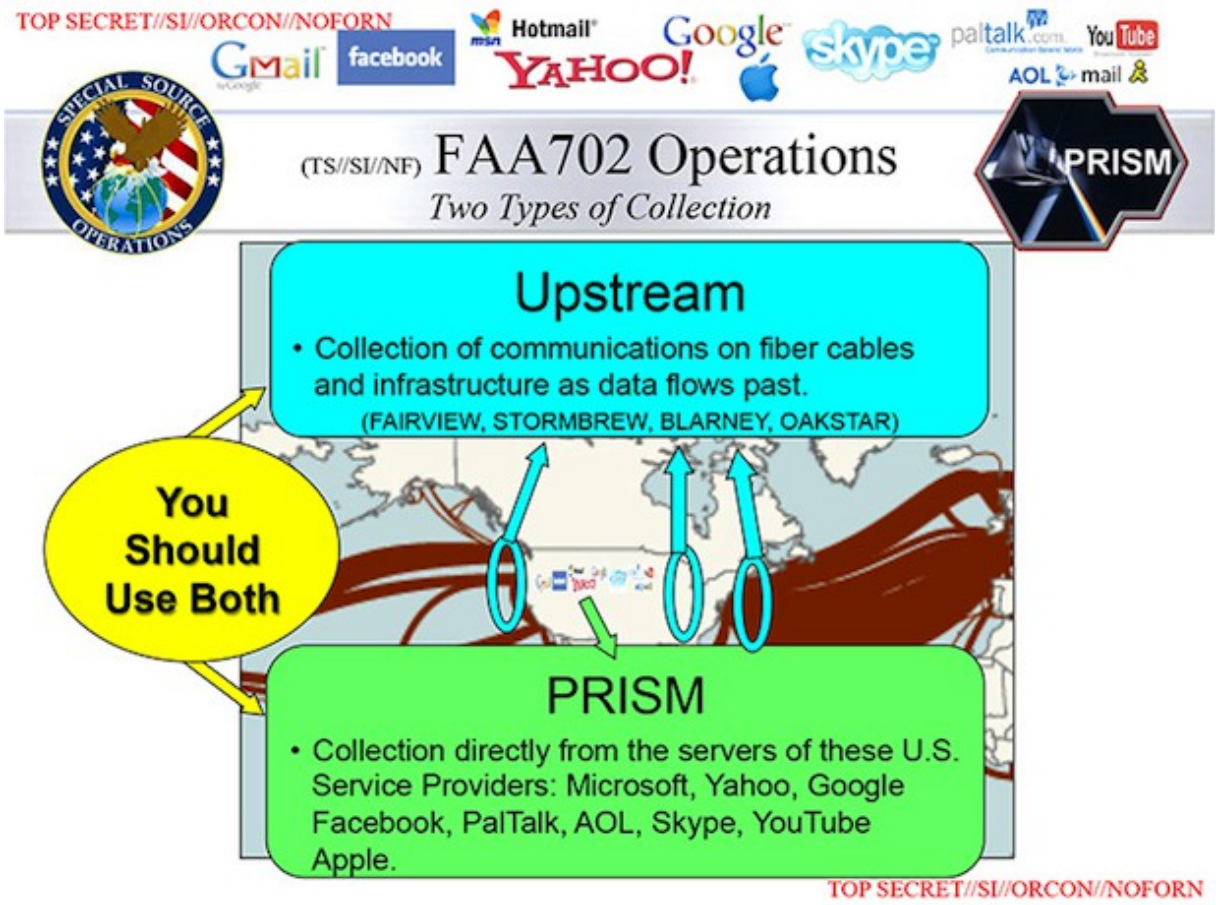
Outra forma de atuação da NSA para obtenção dos dados a serem utilizados pelo programa PRISM, é a coleta de dados por operações de interceptação dos cabos da Internet, a “Coleta Upstream”, já citada neste trabalho.

Conforme mostra um slide divulgado por Snowden, o PRISM e Coleta Upstream devem ser usados ao mesmo tempo: “Você deve usar ambos” (figura 3). Neste caso, a NSA intercepta os dados diretamente enquanto estes passam pelos cabos e pela infraestrutura da internet.

Em agosto de 2013, a imprensa norte-americana revelou que funcionários dos serviços de inteligência e contratados com acesso aos sistemas de vigilância e espionagem da NSA têm feito uso destes recursos de monitoramento para

impunemente espionar pessoas por motivos privados, sem qualquer restrição de acesso, como, por exemplo, espionar pessoas ligadas aos seus interesses amorosos (NSA..., 2013a), cônjuges (EMPLEADOS..., 2013), pessoas de interesse particular e outros, o que veio depreciar de forma ainda mais acentuada a validade do trabalho da aludida agência norte-americana.

Figura 3: Slide de apresentação do PRISM: Coleta Upstream.



Fonte: http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

A prática se tornou tão conhecida dentro da NSA que recebeu um código especial: LOVEINT (SNOWDEN, 2014b), termo atribuído em semelhança à terminologia de inteligência, tais como: SIGINT, COMINT ou HUMINT (NSA..., 2013b).

As companhias indicadas como participantes no PRISM distanciaram-se do programa após a divulgação pública do programa e de seus envolvimentos. Vários executivos disseram ao periódico britânico *The Guardian* que eles não possuíam conhecimento a respeito do PRISM ou algo semelhante, afirmando ainda que nunca teriam cooperado com um programa como este (LARDINOIS, 2013).

Em resposta às negativas das companhias quanto à NSA ser capaz de acessar diretamente os servidores destas, o periódico norte-americano *New York Times* reportou que suas fontes afirmaram que a NSA estava obtendo acesso aos dados das companhias usando os recursos legais, isto é, ordens judiciais que solicitaram conjuntos de dados específicos (SAVAGE, 2013).

Em um outro relatório secreto obtido por outro periódico norte-americano, o *The Washington Post*, o arranjo é descrito como capaz de permitir que “gerentes de coleta” enviem instruções, não para pessoas, mas para equipamentos instalados nas locações controladas pelas companhias, com o propósito de realizar coleta de dados (GELLMAN, 2013b).

Portanto, a divulgação do projeto PRISM gerou inúmeras incertezas e inseguranças na comunidade internacional, em relação aos serviços de internet e aos fabricantes de equipamentos de tecnologia da informação. E no Brasil, os reflexos acabaram atingindo muito mais os interesses do Estado do que os da sociedade como um todo.

4 OS IMPACTOS NO BRASIL

4.1 O MONITORAMENTO E A REAÇÃO BRASILEIRA

Ainda que brasileiros tivessem a convicção de que as nações realizam atividades de espionagem para protegerem-se de conflitos, ataques terroristas, narcotráfico e outras ameaças, não havia provas de que os governos estrangeiros realizavam atividades de inteligência voltadas para fins comerciais. Mas uma das discussões que os “Arquivos Snowden” priorizou nos encontros diplomáticos internacionais foi o emprego de recursos oficiais para benefícios econômicos.

Um dos exemplos de que o Brasil teria sido vítima deste monitoramento internacional é a espionagem canadense no Brasil, por meio do CSEC (Communications Security Establishment Canada), a agência canadense equivalente a NSA (MINISTÉRIO..., 2013). O CSEC é altamente secreto e opera quase como inexistente. Os documentos revelados por Snowden mostram como a agência canadense de inteligência, signatária do acordo com a NSA, foi a agência de inteligência que mais dirigiu seus recursos para a espionagem no Brasil.

Uma reportagem da Rede Globo que foi ao ar na televisão brasileira, em outubro de 2013, mostrou como espiões canadenses monitoraram o Ministério das Minas e Energia. Os metadados de telefonemas e e-mails envolvendo o Ministério foram alvo da CSEC, por meio do programa de software chamado OLYMPIA. O governo do Canadá não confirmou nem negou as acusações de espionagem: “O CSEC não faz comentários específicos sobre suas atividades de inteligência estrangeira ou de capacidades”, disse o diretor de comunicações do primeiro-ministro canadense, Jason MacDonald (MORAES, 2013a).

O Ministro de Minas e Energia à época, Edison Lobão, disse na reportagem que "o Canadá tem interesses no Brasil, sobretudo no setor de mineração. Eu não posso dizer se a espionagem serviu os interesses corporativos ou outros grupos."

Além disso, foi revelado que a presidente Dilma Rousseff também foi alvo de espionagem da NSA, por meio de suas comunicações (DOCUMENTOS..., 2013). O programa utilizado desta vez foi o “DNI selectors”, que segundo outro documento vazado por Snowden, captura tudo o que o usuário faz na internet, incluindo o conteúdo de e-mails e sites visitados.

Um gráfico presente em uma das apresentações mostra toda a rede de comunicações da Presidente Dilma Rousseff com seus assessores. No documento, não há extratos de mensagens ou ligações entre a presidente e seus ministros, mas na última página o documento diz que o método de espionagem usado é "uma filtragem simples e eficiente que permite obter dados que não são disponíveis de outra forma. E que pode ser repetido." Se pode ser repetido, tudo indica que foi levado a cabo (DOCUMENTOS..., 2013).

Conclui, ainda, dizendo que a união de dois setores da NSA teve sucesso contra alvos de alto escalão: Brasil e México, alvos importantes, e que sabem do perigo de espionagem e protegem sua comunicação. Novamente, se houve sucesso, é porque foram exemplos reais.

Não ficou claro se a interceptação das ligações da presidente Dilma foi feita apenas com acesso às redes de comunicação ou se houve participação de espiões em território brasileiro.

James Bramford, especialista que escreveu três livros sobre a NSA, disse que a NSA tem espiões nas embaixadas e consulados americanos pelo mundo: “Temos uma grande embaixada em Brasília e um consulado no Rio de Janeiro. A NSA opera nesses prédios”, afirmou (DOCUMENTOS..., 2013). Antenas nas embaixadas podem interceptar sinais de micro-ondas e telefones celulares, disse Bramford.

Fato é que, ainda em Hong Kong, quando se encontrou com Glenn Greenwald, Edward Snowden comentou os documentos que envolvem a espionagem à presidente Dilma: "a tática do governo americano desde o 11 de setembro é dizer que tudo é justificado pelo terrorismo, assustando o povo para que aceite essas medidas como necessárias. Mas a maior parte da espionagem que eles fazem não tem nada a ver com segurança nacional, é para obter vantagens injustas sobre outras nações em suas indústrias e comércio em acordos econômicos" (DOCUMENTOS..., 2013).

Um exemplo disto foi publicado na revista “Época”: trata-se de uma carta escrita pelo ex-embaixador americano no Brasil, Thomas Shannon, em 2009, quando ainda era subsecretário de estado. Ele agradece à NSA pelas informações repassadas à diplomacia americana antes da 5ª Cúpula das Américas – um encontro entre os chefes de estado do continente para discutir assuntos comerciais e diplomáticos da região. Na carta, Thomas Shannon escreveu que mais de 100 relatórios que eles receberam da NSA deram a eles uma compreensão profunda dos

planos e intenções dos outros participantes da cúpula e permitiram que seus diplomatas se preparassem para aconselhar o presidente dos Estados Unidos Barack Obama em como lidar com questões controversas.

“Em questões comerciais, saber o que os outros estão pensando antes das reuniões multilaterais é como jogar pôquer sabendo quais as cartas de todos na mesa”, disse Bramford (DOCUMENTOS..., 2013).

Outro documento diz que uma divisão inteira da NSA é dedicada à política internacional e atividades comerciais, com um setor encarregado de países que incluem o Brasil.

Um terceiro documento ultrassecreto enumera os desafios geopolíticos dos Estados Unidos para os anos de 2014 a 2019. O surgimento do Brasil e da Turquia no cenário global é classificado como risco para a estabilidade regional.

E o Brasil aparece de novo, junto com outros países, como uma dúvida no cenário diplomático americano: nosso país seria amigo, inimigo ou problema? Também são citados Egito, Índia, Irã, Turquia, México.

“Quando o país fica mais independente, mais forte, como o Brasil está (…) [sic], competindo com os Estados Unidos, empresas americanas. E por causa disso, o governo americano está pensando diferente sobre o Brasil”, afirmou Greenwald (DOCUMENTOS..., 2013).

Após uma reunião entre o Ministro da Justiça, José Eduardo Cardozo, e a presidente Dilma Rousseff, o governo brasileiro decidiu tomar três medidas: o Ministério das Relações Exteriores chamaria o embaixador americano no Brasil, Thomas Shannon, para que ele desse novos esclarecimentos; cobraria explicações formais do governo dos Estados Unidos e recorreria aos órgãos internacionais, como a ONU, para discutir a violação de direitos de autoridades e cidadãos brasileiros.

Eduardo Cardoso, que ainda reuniu-se com o vice-presidente Joe Biden, disse que se fossem comprovados esses fatos, eles estariam diante de uma situação que seria inadmissível, inaceitável, por que eles qualificariam como uma clara violência à soberania do nosso país. Complementou ainda que o Brasil cumpre fielmente com suas obrigações e que gostaria que todos os seus parceiros também as cumprissem e respeitassem aquilo que é muito caro para um país, que é a sua soberania.

Ele levou a proposta de que as comunicações somente fossem acessadas com autorização da Justiça e no caso de investigações criminais. A proposta não foi aceita. Procuradas à época, as embaixadas dos Estados Unidos e do México não se manifestaram.

A presidente Dilma cancelou uma visita planejada para os EUA, onde ela seria a convidada de honra para um jantar de Estado e ainda falou na Assembleia Geral da ONU, pedindo regulamentação internacional sobre privacidade de dados e limitação dos programas de espionagem visando a internet.

Também surgiram pressões para adiar o leilão dos direitos de exploração do Petróleo no campo de Libra, na Bacia de Santos, na região do pré-sal (VILAIN, 2013). O leilão foi marcado para outubro de 2013 e empresas americanas interessaram-se em participar. A verdade é que os Estados Unidos, China e Europa são dependentes do petróleo advindo de outros países, sendo os dois primeiros os maiores consumidores mundiais, fato que associado ao controle das reservas de petróleo e gás natural pelas Companhias Nacionais da OPEP, que não possuem interesse em um esgotamento rápido, resultem em um controle de produção e preços dos barris. A questão foi a de como o Brasil poderia se proteger da poderosa máquina de espionagem dos EUA e como iria se comportar diante do petróleo. Afinal, havia no ar a impressão de a retórica de que a espionagem serviria ao interesses do combate ao terrorismo já estava ultrapassada e que informações privilegiadas sobre atividades econômicas poderiam estar em mãos dos norte-americanos. A própria presidente Dilma Roussef afirmou que o motivo da espionagem não era a segurança, mas interesses econômicos e estratégicos.

Os documentos divulgados por Snowden mostraram ainda que empresas que atuavam no Brasil foram parceiras da NSA em operações executadas em nosso território (GREENWALD, 2013c). De acordo com estes documentos, apenas no mês de janeiro de 2013 a NSA tinha recolhido 2,3 bilhões de dados de usuários brasileiros (MAPA..., 2014).

Em virtuide disto, foi instaurada uma Comissão Parlamentar de Inquérito (CPI) destinada a ouvir representantes de companhias telefônicas e de internet, como Telefônica, GVT, Oi e TIM, e da Google Brasil, Facebook Brasil e Microsoft. A CPI buscou avaliar se houve participação de empresas na facilitação das interceptações da NSA para monitoramento de e-mails e telefonemas, independentemente do fato

das empresas negarem sua participação nos programas da agência norte-americana (ESPIONAGEM..., 2013).

Após sete meses de investigações, esta Comissão Parlamentar de Inquérito aprovou seu relatório final. O documento apontou “vulnerabilidade” e “despreparo” do Brasil em segurança cibernética, mas não identificou culpados pelas ações de espionagem no país (MENDES, 2014).

O relator da CPI da Espionagem, senador Ricardo Ferraço (PMDB-ES), afirmou que não foi possível identificar a “materialidade” das denúncias, isto é, quais informações foram violadas, quando, de que forma, entre outros detalhes. O parlamentar capixaba ressaltou, porém, que a espionagem foi comprovada pela comissão, ainda que não tenha sido possível identificar, ao longo das investigações, qual informação tenha sido violada. Ferraço acrescentou ser muito difícil materializar interceptação dessa natureza, mas que ficou evidente que houve espionagem, pois os indícios eram muito fortes.

O referido Senador, que analisou o inquérito da Polícia Federal sobre espionagens no Brasil, afirmou ainda em seu relatório ser “improvável” que a entidade comprove o delito e indique seu autor. Por isso, destacou o senador, os objetivos da CPI ficaram “voltados ao aprimoramento dos sistemas de segurança e contrainteligência” (MENDES, 2014).

“Os fatos tornados públicos por Edward Snowden e, ainda, os trabalhos desta CPI assinalam profunda vulnerabilidade do Estado brasileiro e de nossa população a ações de espionagem”, informou o senador Ferraço em seu relatório (MENDES, 2014).

O parlamentar cobrou mais investimentos do poder público em ações de contrainteligência, como são chamadas medidas tomadas por Estados ou organizações com o intuito de proteger informações estratégicas e atividades de inteligência de outras nações e organizações.

O relatório da comissão concluiu que diante do problema e da constatação de fragilidade em que se encontravam a sociedade e o Estado brasileiro, percebeu-se, no âmbito da Inteligência, a necessidade de mais investimentos e do aprimoramento do aparato brasileiro de contrainteligência.

Para Ferraço, espionagens ainda ocorrerão e “passarão desapercebidas”, caso não se desenvolva, “com urgência”, mecanismos de proteção ao conhecimento.

O relatório finalmente propôs um projeto de lei para regulamentar o fornecimento de dados de cidadãos ou empresas brasileiros a organismos internacionais. Pela matéria, pessoas físicas e jurídicas “têm direito à inviolabilidade e ao sigilo do fluxo de suas comunicações pela internet”, salvo em casos de ordens judiciais. Tal projeto de lei, elaborado e promulgado no país em abril de 2014, ficou conhecido como o “Marco Civil da Internet”, assunto que é tratado a seguir neste trabalho.

O aludido Senador finalmente acrescentou em seu relatório que um dos principais problemas apurados pela CPI em tela diz respeito à falta de controle e de transparência a respeito das requisições de dados de pessoais naturais e jurídicas brasileiras por autoridades governamentais e tribunais estrangeiros. E com este projeto de lei, espera-se suprir essa lacuna e permitir que o Poder Judiciário brasileiro exerça o controle necessário sobre esses procedimentos, divulgando de forma transparente essas requisições.

4.2 O MARCO CIVIL DA INTERNET

O governo já vinha trabalhando, há alguns anos, um projeto de lei, cujo propósito seria o de estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil. No entanto, em virtude da mencionada CPI da espionagem, houve uma intensificação dos trabalhos para que este viesse a ser transformado em lei, o que ocorreu em 23 de abril de 2014. Desta forma, o governo aprovou o Marco Civil da Internet, sob forma da lei ordinária nº 12.965/2014 (BRASIL, 2014).

Ainda que princípios importantíssimos como a neutralidade da rede tenha destaque na citada lei, não é objetivo deste trabalho ir além daquilo que tenha sido consequência direta ou indireta do episódio “Arquivos Snowden” para o Brasil.

Desta forma, em rápida leitura da lei, percebe-se de imediato a ênfase no respeito aos direitos de intimidade, de privacidade, de proteção dos dados pessoais, e do sigilo das comunicações privadas e dos registros, em nítida preocupação com o que ocorreu no episódio “Arquivos Snowden”, onde praticamente nada disto foi respeitado. Devido a importância do artigo relacionado a estes direitos, cabe reproduzir a parte dele que é importante para o propósito deste trabalho, *ipsi litteris*:

> Art. 7o O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I- inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II- inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III- inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
>
> [...]
>
> VI- informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
>
> VII- não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII- informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX- consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X- exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da

> relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
>
> XI- publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
>
> XII- acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
>
> XIII- aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Além disto, com o propósito de regulamentar os citados direitos, tem-se os artigos 10 e 11, cujos caput estão reproduzidos a seguir, ipsi litteris:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

O parágrafo segundo do artigo 11 ainda deixa claro que a pessoa jurídica sediada no exterior que prestar serviço ao público brasileiro deverá se sujeitar às mesmas regras das empresas sediadas em território nacional, *ipsi lilleris*:

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

É importante notar que a lei faz constar que mesmo as empresas estrangeiras deverão se sujeitar à legislação nacional, uma vez que estas estejam atuando com brasileiros. Isto se deve ao fato de que a internet não se sujeita aos limites territoriais do Estado brasileiro, e por isto torna-se necessário trazer para o ordenamento jurídico nacional todos os contratos estabelecidos com brasileiros usuários de internet.

Este último ponto reflete o interesse de que, uma vez que estas empresas estejam sujeitas às leis nacionais, os princípios previstos no Marco Civil da Internet sejam respeitados.

Outro ponto de destaque na lei é a guarda dos registros de atividades dos usuários da internet, reproduzidos nos parágrafos 1º e 2º do artigo 10, *ipsi litteris*:

> Art 10 […]

> § 1o O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7o.
>
> § 2o O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7o.

Nota-se que da mesma forma que passa a existir uma obrigação de guarda das informações de conexão e de atividade na internet por um tempo determinado, há também uma clara intenção de que estas informações não sejam coletadas de forma violar a privacidade do usuário, muitas vezes obrigando aos prestadores de serviço a disponibilizarem os dados de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal. E prevê ainda que estes dados sejam fornecidos apenas por meio de decisão judicial.

Logo vem à mente aquilo que Edward Snowden divulgou e que seria o carro-chefe da espionagem norte-americana: o PRISM. Naquele programa da inteligência estadunidense, as empresas de comunicação chegaram a estabelecer acordos com o governo norte-americano para passar-lhes metadados e demais informações de clientes de seus serviços de internet. E talvez esta seja uma forma de implementar uma proteção ao usuário, com obrigação extensível às empresas estrangeiras que prestam serviços a brasileiros.

O Marco Civil da Internet obriga ainda que os registros de conexão dos usuários devem ser guardados pelos provedores de acesso pelo período de um ano, sob total sigilo e em ambiente seguro. Essas informações dizem respeito apenas ao IP (o endereço lógico de conexão de um dispositivo de comunicação à internet), data e horas inicial e final da conexão. O artigo 13 da lei traz este dispositivo, *ipsi litteris*:

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

E conforme o artigo 15 da supracitada lei, o texto ainda cria a obrigação, aos provedores, de guarda, por seis meses, de registros de acesso a aplicações de internet, que são os que relacionam o IP ao uso de aplicações da internet, *ipsi litteris*:

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

A lei também estabelece que esta guarda de registros de acessos a aplicações de internet seja feita de forma anônima, ou seja, os provedores poderão guardar o IP, mas nunca as informações sobre o usuário, a não ser que haja consentimento do mesmo, conforme previsto no artigo 16, *ipsi litteris*:

> Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:
> I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7o; ou

A ausência de informações lógicas sobre o usuário impede que a privacidade do mesmo seja violada por uma simples leitura dos registros armazenados pelos provedores em seus equipamentos. A disponibilização desses dados, segundo o texto, só poderá ser feita mediante ordem judicial.

O documento ainda fixa princípios de privacidade sobre os dados que o usuário fornece aos provedores. Na internet, os dados hoje são coletados, tratados e vendidos quase que instantaneamente. A lei coloca no inciso II, ainda do artigo 16, como direito dos usuários que suas informações não pode ser usadas para um fim diferente daquele para que foram fornecidas, conforme estabelece a política de privacidade do serviço.

> Art 16. […]
>
> II – de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

É impossível não relacionar toda esta preocupação com privacidade com o evento “Arquivos Snowden”, quando até chefes de Estado foram vítimas de espionagem. Mas neste caso, ao contrário do que se poderia imaginar em relação ao que o Estado viesse a implementar, uma vez que estava demasiadamente preocupado com a sua segurança, os dispositivos da nova lei que implementam esta proteção à privacidade foram benéficos aos usuários de internet, interessados em manter sua liberdade.

O Marco Civil ainda estabelece outras regras importantes como a possibilidade de retirar-se um site do ar apenas após uma ordem judicial, evitando

uma possível censura, etc. Mas essas e outras questões não serão abordadas neste trabalho, cujo propósito é o de mostrar apenas os artigos da lei que foram influenciados pelo episódio “Arquivos Snowden”, conforme já registrado anteriormente.

No entanto, não se pode deixar de registrar uma discussão muito importante que ocorreu na época da edição da lei. Trata-se da tentativa do governo de emendar o projeto de lei, obrigando que o armazenamento dos dados fossem feitos em servidores presentes no território brasileiro, por empresas que operam no Brasil.

Com isto, as empresas prestadoras de serviço na internet teriam que respeitar as leis brasileiras, em que somente com autorização judicial seria possível proceder a uma quebra de sigilo de dados, uma vez que estes dados estariam fisicamente no país.

Em que pese haver o interesse de prover maior privacidade aos usuários de internet, esta proposta do governo de tornar obrigatório o armazenamento de dados de internautas em território nacional não garantiria esta privacidade desejada, e ainda ameaçaria prejudicar o desenvolvimento do setor de tecnologia.

Lembra ainda o professor Adriano Cansian, da Unesp de São José do Rio Preto, especialista em segurança da informação, que “do ponto de vista técnico é complicado assegurar a proteção de dados de internautas brasileiros pelo simples fato de estocá-los em território nacional”. Ele argumenta que essas informações poderão, em algum momento, passar pela rede, abrindo a possibilidade de espionagem (MORAES, 2013b).

O professor ainda destaca uma implicação legal, pois a falta de legislação específica poderia fazer com que eventuais crimes cometidos no Brasil passassem incólumes, já que grandes empresas possuem seus servidores locados em outros países: "(O projeto) Poderia trazer uma maior segurança jurídica ao facilitar a aplicação de leis nacionais (quando há violação de dados). É complexo falar em segurança quando se está fora da aplicação da lei", diz o professor, alertando sobre a necessidade de maior discussão sobre o tema. "E preciso dar um passo na proteção de dados individuais. Do ponto de vista do cidadão, o buraco é mais embaixo", diz, ao defender a discussão de uma legislação que vá além do Marco Civil e aborde o tema. "Temos quantidade imensa de dados pessoais em poder de instituições públicas e privadas e que podem ser até comercializados. Se alguém roubar, não existe legislação para isso hoje", diz (MORAES, 2013b).

Além disto, poderia o país sofrer com um aumento de custos decorrente desta obrigatoriedade e ainda dificultaria a inovação e criaria barreiras desnecessárias para novas empresas. Esta emenda não foi aprovada, mas nada impede que o governo tente emplacá-la no futuro.

Enfim, o Marco Civil da Internet representa um ganho para os brasileiros nas relações comerciais envolvendo produtos de internet, em que pese não tenha sido publicado exatamente da forma que o governo brasileiro desejava. No entanto, muitos dos artigos editados na referida lei, fortemente influenciados pelo episódio “Arquivos Snowden”, podem ser vistos como um bom avanço para a segurança das informações.

4.3 UMA ANÁLISE DE CONTEXTO

Todo país tem direito de preservar sua soberania. E os Estados Unidos da América, na condição de nação mais poderosa do mundo, é uma das que mais tem necessidade de possuir uma boa estrutura de inteligência, cujas atividades podem até andar na fronteira dos limites da atuação do Estado, mas que definitivamente tem legitimidade para atuar.

Neste campo da inteligência internacional não há espaço para ingênuos. Obviamente já se sabia que os norte-americanos realizavam trabalhos de espionagem. Os detalhes das operações é que eram muito bem guardados.

Conforme o princípio geral do Direito Internacional, segundo o qual devem pautar-se as ações dos membros que compõem o sistema internacional, a atividade de inteligência é vital para a proteção de um Estado contra ofensivas externas.

E a questão não é a possibilidade, nem a legalidade da atuação ou muito menos a violação do Direito Internacional ou interno, pois o imperativo de segurança levará determinados Estados a agir dessa forma e quem tiver condições, agirá. Muitos países no mundo não possuem as restrições legais que o Brasil possui e, mesmo que tenham, muitos outros atores continuarão agindo. No caso específico dos Estados Unidos da América, aquele país tem o costume de exercer a atividade de inteligência de maneira pautada na legislação nacional e internacional (SILVA JUNIOR, 2013).

Com a confirmação das interceptações telefônicas e coleta de dados dos usuários de internet realizados pelos norte-americanos, não se fez nada além de protestos diplomáticos isolados e exigência de pedido de desculpas pelos países espionados. Na prática, desde que o mundo é mundo, nada diferente foi feito no campo da inteligência em termos de conduta. A novidade ficou por conta do uso da tecnologia.

Se, por um lado, o caso evidencia a urgência do Estado brasileiro em ampliar sua capacidade de exercer a atividade de contrainteligência, por outro lado, torna pública a necessidade de robustecer-se os limites jurídicos do exercício da atividade de inteligência (SILVA JUNIOR, 2013).

Mas algo ficou muito claro às vistas do mundo: a diferença de postura entre as diversas nações em resposta à divulgação das ações de espionagem norte-americanas. Enquanto as nações que, supostamente, menos protegem suas

informações, reclamaram das ações norte-americanas, as nações que mais utilizam do expediente da inteligência nada falaram sobre os episódios, ou, pelo menos, não fizeram grandes protestos. O motivo é óbvio: estas nações também realizam suas atividades de inteligência. No entanto, a inteligência é uma atividade que não se desenvolve sob holofotes. Assim sempre foi e sempre será.

Da mesma forma que pessoas comuns utilizam serviços de internet de forma inofensiva, terroristas e indivíduos mal intencionados também estão na internet, no entanto utilizando-a para fins maléficos. Em vista desta necessidade de proteção contra os indivíduos perigosos, haveria justificativa para tal monitoramento. É a constante e necessária escolha entre a privacidade e a segurança.

Mas o que os Estados Unidos estão necessariamente investigando na internet? Que informações são merecedoras de proteção? O cidadão comum pode até desejar privacidade, mas os próprios termos de adesão dos serviços de internet já esclarecem que não há segurança absoluta sobre os dados, uma vez que há margem para monitoramento ou utilização destes últimos para fins comerciais. O cidadão comum pode até relegar a segurança em nome da praticidade, mas a proteção tem que ser obrigatória quando se tratar de informações de Estado. Desta forma, é de se concluir que não é um momento para atuação agressiva do serviço de inteligência brasileiro, mas, sim, de sua contrainteligência.

A contrainteligência torna-se ainda mais importante do que a própria atividade de Inteligência, pois a proteção dos dados é fundamental. São duas faces da mesma moeda. Ambas precisam de forte investimento. A contrainteligência deve possuir todas as condições necessárias para evitar a ações hostis.

Em se tratando de contrainteligência, os agentes de Estado devem ter a consciência de que são monitorados. Em virtude disto, há que se trabalhar sempre visando a segurança das informações. Para tal, e para apenas exemplificar, não se deve utilizar telefones celulares para comunicações importantes e nem mesmo e-mails para tal fim, em que pese existir o conceito de telefone e e-mails seguros, isto é, ferramentas oficiais, cuja preocupação com segurança seja diferenciada, mas há sempre que prevalecer a mentalidade de segurança.

Não é o propósito deste trabalho registrar ensinamentos ou orientações sobre segurança das informações, pois para tal, sugere-se um aprofundamento no tema a partir de literatura própria. Mas cabe o registro de que, em que pese exista a impressão de que a atividade de inteligência seja específica para profissionais de

inteligência, o que até pode proceder, a preocupação com a contrainteligência deverá ser uma preocupação de todo agente do Estado, em menor ou maior nível.

Registra-se ainda que muitos países, tidos como mais avançados do mundo, realizam atividades de inteligência similares ao que o Estado norte-americano realizou, além de não se descuidarem de sua contrainteligência.

Se informações importantes e sigilosas do Estado brasileiro caíram nas mãos da inteligência norte-americana, isto aconteceu porque existiram as condições para possibilitar esta ocorrência. Se houvesse a devida proteção destas informações, consideradas confidenciais em algum grau de sigilo, hoje não se falaria em ato de "traição" pelo governo norte-americano, pelo fato de terem obtido tais informações, afinal eles estão fazendo aquilo que lhes cabe. Não é pecado uma nação zelar pela sua própria segurança, seja por seus interesses comerciais, seja pela sua soberania. De qualquer forma, ficou patente a inexistência de proteção adequada às informações de Estado, sejam elas de maior ou de menor importância.

O fato do Brasil não dispensar a devida atenção às suas atividades de inteligência e contrainteligência, não lhe permite criticar que outra nação o faça, o que restou materializado no discurso já relatado do então Ministro da Justiça, José Eduardo Cardoso (DOCUMENTOS..., 2013). Além do Brasil reservar pouca atenção à área de inteligência, a mesma ainda sofre importantes restrições legais, além de faltar investimento e interesse político. Não há sequer uma melhor regulamentação das operações de inteligência e contrainteligência no país.

Além disto, é necessário enxergar a ação do Estado em proteger suas informações como um amplo programa de defesa cibernética. O Brasil precisa estar preparado para proteger o seu patrimônio de informação, entendido aqui como o somatório de seus ativos de informação, suas informações críticas, seus sistemas de informação, suas infraestruturas críticas, incluindo a de informação, tudo aquilo, enfim, que pode ser identificado como componente da sociedade da informação presente no espaço cibernético. Para tanto, será necessário adotar medidas para a proteção, mediante a elaboração de doutrina e a construção de estratégias de segurança e de defesa do espaço cibernético brasileiro, considerando ambos os conceitos complementares.

Oportuno ainda é fortalecer a estratégia de segurança cibernética, pois esta última deve assegurar, entre outros aspectos, a disponibilidade, a integridade, a

confidencialidade e a autenticidade das informações de interesse do Estado e da sociedade brasileira, aspectos da segurança institucional (MANDARINO, 2009).

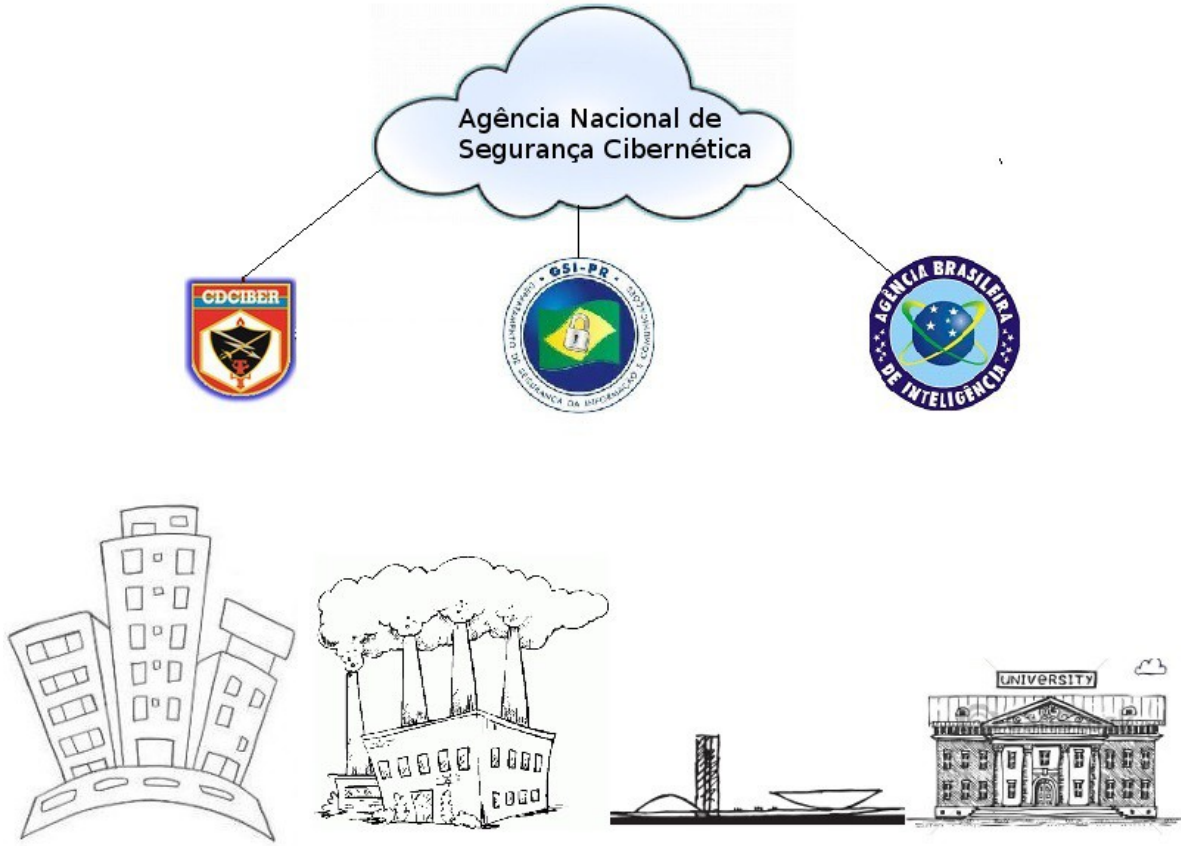
O governo brasileiro também pode ter cometido um equívoco ao misturar questões de Estado com assuntos típicos do direito privado na produção do “Marco Civil da Internet”. Além disto, não seria a melhor solução para o país uma possível emenda no referido Marco Civil que viesse a obrigar que pessoas jurídicas de direito privado atendam a requisitos supostamente protecionistas, em que um instrumento intrinsecamente global e sem fronteiras, como a internet, seja “domesticada”, com o risco de atender apenas a interesses do Estado, relegando a segundo plano o livre mercado e as liberdades individuais.

Portanto, com o objetivo de mitigar a ocorrência de incidentes como o que foi tratado nesta pesquisa, propõe-se uma solução prática baseada em ações integradas entre os agentes governamentais responsáveis pelas áreas sensíveis correlatas. Esta solução busca o menor impacto possível em despesa pública, pois utiliza a infraestrutura já existente no país e apresenta a necessidade de criação de apenas uma nova instituição pública, enxuta e com objetivo bem definido, como tratado a seguir (figura 4).

A Estratégia Nacional de Defesa atribui ao Exército Brasileiro o papel da defesa cibernética. Neste contexto, o principal ator é o Centro de Defesa Cibernética do Exército (CDCiber), uma unidade nova, mas extremamente importante para salvaguardar o país de atividades hostis desta natureza. O CDCiber coordena as ações de defesa cibernética das Forças Armadas, mas não está restrito à defesa nacional, pois também tem como atribuição proteger as redes governamentais e ainda pode contribuir para proteger as infraestruturas de informação como um todo.

Já em relação à segurança da informação dos órgãos de Estado, o principal ator envolvido seria o Gabinete de Segurança Institucional da Presidência da República, por meio do seu Departamento de Segurança da Informação (DSIC), que possui como atribuições, dentre outras: coordenar a execução de ações de segurança da informação e comunicações na administração pública federal; definir requisitos metodológicos para implementação de ações de segurança da informação e comunicações pelos órgãos e entidades da administração pública federal; e operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal.

Figura 4: Uma proposta de trabalho coordenado por uma agência central.



Além disto, o Centro de Pesquisas e Desenvolvimento para Segurança das Comunicações da Agência Brasileira de Inteligência (Abin), por sua experiência de mais de 30 anos em pesquisa no setor, seria importantíssimo na apresentação de soluções para segurança nas comunicações.

A atividade de contrainteligência, como já citado neste trabalho, estaria presente por meio da disseminação em cada unidade de serviço público de uma cultura de segurança, em que cada agente público realize a sua parte na proteção das informações sensíveis.

O país poderia ainda estudar a possibilidade da criação de uma instituição que trabalhasse com a regulação e com o gerenciamento do setor, de forma transcender as fronteiras de cada um dos órgãos públicos envolvidos, e assim permitir a interoperabilidade entre as unidades, requisito fundamental para o sucesso das ações. Tal instituição poderia funcionar nos moldes de uma agência reguladora, com finalidade estritamente técnica, preservando a subordinação administrativa de cada órgão público envolvido.

Por fim, há que se ressaltar que uma relevante vulnerabilidade existente no modelo estudado é a dependência de tecnologia estrangeira nos sistemas cibernéticos, algo que somente seria superado com desenvolvimento de tecnologia própria. Este desenvolvimento seria viável a partir de grandes investimentos público e privado no setor. É importante deixar registrado que não se defende um desenvolvimento generalizado de tecnologia, pois não haveria foco naquilo que seria mais importante, dificultando a obtenção de resultados. Mas poderia ser trabalhado um desenvolvimento pontual, com objetivo naquilo que seria a tecnologia mais sensível, principalmente as que teriam finalidades militares. É importante registrar também que esta vulnerabilidade acaba sendo oportunidade para a indústria de defesa do Brasil, em que produtos de utilização dual podem nortear o objetivo a se atingir nas pesquisas.

5 CONCLUSÃO

A presente pesquisa teve como objetivos: estudar o episódio intitulado “Arquivos Snowden”, identificar as principais informações e sistemas afetados, analisar sua repercussão e seus desdobramentos no Brasil e apresentar uma possível solução para reduzir problemas como os que afetaram o Brasil a partir do supracitado episódio.

O estudo do episódio “Arquivos Snowden” buscou abordar não somente o episódio em si, mas também seus antecedentes, de tal forma permitir entender sua motivação e seu objetivo.

Tão importante quanto estudar o citado episódio, foi identificar quais sistemas e informações norte-americanos foram comprometidos, pois em um cenário geopolítico multipolar, é necessário entender quais são os principais interesses da nação mais poderosa do mundo.

As repercussões e desdobramentos no Brasil foram estudados para entender se o país teve a reação adequada, coerente e compatível com sua condição de Estado de porte continental e possuidor de uma das maiores populações e economias do mundo. Neste contexto, foi feita uma análise específica da parte do Marco Civil da Internet que trata da segurança das informações.

Por fim, foi apresentada uma possível solução para as questões de segurança cibernética e segurança da informação, realizada a partir de uma análise do contexto atual destas áreas no país.

A partir do estudo realizado nesta pesquisa, conclui-se que o Brasil não protege adequadamente as informações de Estado. Além disto, o governo brasileiro demonstrou, por meio de sua reação, como suposta vítima, o quanto está despreparado para lidar com episódios como o que foi tratado neste trabalho, o qual não poderia se restringir ao campo da diplomacia. Desta forma, há que se trabalhar melhor a segurança das informações críticas para o Estado brasileiro, além mudar o comportamento ao lidar com situações como esta, de tal forma agir com o mínimo de compatibilidade com a importância e a grandeza que o Estado brasileiro exige.

Não há que se falar em desproporcionalidade nas ações desempenhadas pelo governo norte-americano em seu programa de monitoramento PRISM, muito menos em relação ao Brasil. Há total legitimidade em realizar tal atividade, pois os Estados Unidos da América, como nação mais poderosa do mundo, tem que se

preservar contra atos hostis, como as ações terroristas, as quais exigem antecipação de movimento e planejamento. E a complexidade do referido programa de monitoramento demonstrou o quanto o governo norte-americano se preocupa com as informações que circulam pelo mundo, uma vez que são elas que podem determinar como aquele país deve lidar com as suas questões de segurança, em que pese haja o efeito colateral de se obter informações que tratam de política, economia e diplomacia.

A produção do texto do Marco Civil da Internet foi mesmo influenciado pela divulgação das ações de espionagem internacional, mas não foi afetado de forma negativa, como já descrito neste trabalho, uma vez que a obrigação de que os servidores ficassem fisicamente em território brasileiro não logrou sucesso.

E ainda que tenha sido proposto um modelo com vistas a melhorar a questão da segurança das informações críticas de Estado, não é fácil produzir um plano de segurança em que a nação figure como o elemento sensível. No entanto, este modelo proposto de integração das atividades de segurança da informação, de contrainteligência e de segurança cibernética, por meio de um trabalho conjunto pelos órgãos governamentais que possuem competência normativa e experiência nas respectivas áreas de estudo, e coordenado por uma agência reguladora, pode ser o caminho para que o Brasil desenvolva a solução mais apropriada para a sua própria realidade.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2005.** Rio de Janeiro, 2005.

BALL, James. NSA collects millions of text messages daily in 'untargeted' global sweep. **The Guardian**, Londres, 16 jan. 2014 Disponível em: <http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep>. Acesso em: 22 jul. 2014.

BAUMAN, Ethan L. Memorando: Notificação ao Congresso Norte-americano. Renúncia de empregado da NSA**. MSNBC**, Nova Iorque, 10 fev. 2014. Disponível em: <http://msnbcmedia.msn.com/i/msnbc/sections/news/NSA_Snowden_Memo.pdf>. Acesso em: 21 jul. 2014.

BRASIL. Lei ordinária nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasília, DF, 24 abr. 2014. Seção 1, p. 1.

CAPRA, Tony. Snowden Leaks Could Cost Military Billions: Pentagon. **NBC News**, Nova Iorque, 6 mar. 2014. Disponível em: <http://www.nbcnews.com/news/investigations/snowden-leaks-could-cost-military-billions-pentagon-n46426>. Acesso em: 21 jul. 2014.

CARVALHO, Paulo S. M. de. Desafios estratégicos para a segurança e defesa cibernética. In: o setor cibernético nas forças armadas brasileiras. **Texto apresentado na Secretaria de Assuntos Estratégicos da Presidência da República**. Brasília, DF, 2011.

DHILLON, Gurpreet. **Information Security Management:** Global Challenges in the New Millennium**.** *Idea Group Publishing*, Hershey, 2001.

DIRECT NSA Partners: AT&T, Verizon, Microsoft, Cisco, IBM, Oracle, Intel, Qualcomm, Qwest & EDS. **Washington's Blog**, Washington, 14 maio 2014. Disponível em: <http://www.washingtonsblog.com/2014/05/direct-nsa-parnters-att-verizon-microsoft-cisco-ibm-oracle-intel-qualcomm-qwest-eds.html>. Acesso em: 22 jul. 2014.

DOCUMENTOS da NSA apontam Dilma Rousseff como alvo de espionagem. **G1.globo**, Rio de Janeiro, 09 set. 2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html>. Acesso em: 22 jul. 2014.

EMPLEADOS de NSA espiaban desde la agencia a sus parejas. **La Jornada**, México, 28 set. 2013. Disponível em: <http://www.jornada.unam.mx/2013/09/28/mundo/019n2mun>. Acesso em: 22 jul. 2014.

ESPIONAGEM da NSA inclui invasão a data centers de Google e Yahoo. **Jornal do Brasil**, Rio de Janeiro, 31 out. 2013. Disponível em: <http://www.jb.com.br/ciencia-e-tecnologia/noticias/2013/10/31/espionagem-da-nsa-inclui-invasao-a-data-centers-de-google-e-yahoo-diz-jornal/>. Acesso em: 22 jul. 2014.

EUA têm acesso direto aos servidores de Google, Facebook e Apple, dizem jornais. **Carta Capital**, 06 jun. 2012. Disponível em: <http://www.cartacapital.com.br/internacional/eua-tem-acesso-direto-aos-servidores-de-google-facebook-e-apple-diz-jornal-5976.html>. Acesso em: 21 jul. 2014.

FINN, Peter; HOROWITZ, Sari. U.S. charges Snowden with espionage. **The Washington Post**, Washington, 21 jun. 2013. Disponível em: <http://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html>. Acesso em: 21 jul. 2014.

GELLMAN, Barton; POITRAS, Laura. U.S. intelligence mining data from nine U.S. Internet companies in broad secret program. **The Washington Post**, Washington, 06 jun. 2013a. Disponível em: <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1>. Acesso em: 22 jul. 2014.

GELLMAN, Barton. U.S. surveillance architecture includes collection of revealing Internet, phone metadata**. The Washington Post**, Washington, 15 jun. 2013b. Disponível em: <http://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_print.html>. Acesso em: 22 jul. 2014.

GREENWALD, Glenn. Edward Snowden: the whistleblower behind the NSA surveillance revelations. **The Guardian***,* Londres, 9 jun. 2013a. Disponível em: <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Acesso em: 21 jul. 2014.

_____. **XKeyscore:** NSA tool collects 'nearly everything a user does on the internet'**. The Guardian**, Londres, 31 jul. 2013b. Disponível em: <http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data>. Acesso em: 22 jul. 2014.

GREENWALD, Glenn et al. Espionagem dos EUA se espalhou pela América Latina. **O Globo**, Rio de Janeiro, 09 jul. 2013c. Disponível em: <http://oglobo.globo.com/mundo/espionagem-dos-eua-se-espalhou-pela-america-latina-8966619>. Acesso em: 22 jul. 2014.

HARDING, Luke. **Os Arquivos Snowden:** a história secreta do homem mais procurado do mundo. São Paulo: LeYa Brasil, 2014.

HEIL, Emily. What's the deal with NSA's operation names? **The Washington Post**, Washington, 22 out. 2013. Disponível em: <http://www.washingtonpost.com/blogs/in-

the-loop/wp/2013/10/22/whats-the-deal-with-nsas-operation-names/>. Acesso em: 22 jul. 2014.

HERSZENHORN, David. Leaker Files for Asylum to Remain in Russia. **The New York Times**, Nova Iorque, 17 jun. 2013. Disponível em: <http://www.nytimes.com/2013/07/17/world/europe/snowden-submits-application-for-asylum-in-russia.html?_r=0>. Acesso em: 21 jul. 2014.

LARDINOIS, Frederic. Google, Facebook, Dropbox, Yahoo, Microsoft And Apple Deny Participation In NSA PRISM Surveillance Program. **Tech Crunch**, São Francisco, 06 jun. 2013. http://techcrunch.com/2013/06/06/google-facebook-apple-deny-participation-in-nsa-prism-program/>. Acesso em: 22 jul. 2014.

MANDARINO, Raphael. **Um estudo sobre a Segurança e Defesa do Espaço Cibernético Brasileiro**. Brasília, DF : [s.n.], 2009.

MAPA mostra volume de rastreamento do governo americano. **O Globo**, Rio de Janeiro. Disponível em: <http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/>. Acesso em: 22 jul. 2014.

MATSUURA, Sergio. Empresas de tecnologia negam colaboração com espionagem dos EUA. **O Globo**, Rio de Janeiro, 08 jul. 2013. Disponível em: <http://oglobo.globo.com/mundo/empresas-de-tecnologia-negam-colaboracao-com-espionagem-dos-eua-8961278>. Acesso em: 21 jul. 2014.

MAYER, Jane. Snowden Calls Russian-Spy Story "Absurd". **The New Yorker.** Nova Iorque. 21 jan 2014. Disponível em: <http://www.newyorker.com/online/blogs/newsdesk/2014/01/snowden-calls-russian-spy-story-absurd.html>. Acesso em: 21 jul. 2014.

MENDES, Priscilla. Relatório final da CPI da Espionagem aponta que Brasil está vulnerável. **G1.globo**, Rio de Janeiro, 09 abr. 2014. Disponível em: <http://g1.globo.com/politica/noticia/2014/04/relatorio-final-da-cpi-da-espionagem-aponta-que-brasil-esta-vulneravel.html>. Acesso em: 22 jul. 2014.

MICK, Jason. NSA is Recording Every Phone Call in at Least Five Countries. **Daily Tech**, 18 mar. 2014. Disponível em: <http://www.dailytech.com/NSA+is+Recording+Every+Phone+Call+in+at+Least+Five+Countries/article34548.htm>. Acesso em: 22 jul. 2014.

MINISTÉRIO de Minas e Energia foi alvo de espionagem do Canadá. **G1.globo**, Rio de Janeiro, 07 out. 2013. Disponível em: <http://g1.globo.com/politica/noticia/2013/10/ministerio-de-minas-e-energia-foi-alvo-de-espionagem-do-canada.html>. Acesso em: 22 jul. 2014.

MORAES, Sergio. Canadian spies targeted Brazil's mines ministry: report**. CBC News**, Ottawa, 07 out. 2013a. Disponível em: <http://www.cbc.ca/news/canadian-spies-targeted-brazil-s-mines-ministry-report-1.1927975>. Acesso em: 22 jul. 2014.

MORAES, Mauricio. Marco Civil: dados em servidores nacionais garantem privacidade? **BBC Brasil**, Brasília, 30 out. 2013b. Disponível em: <http://www.bbc.co.uk/portuguese/noticias/2013/10/131030_marco_civil_mm_dg.shtml>. Acesso em: 22 jul. 2014.

NOVOSTI, Ria. Putin talks Syria, gay rights in interview**. The Moscow News**, Moscou, 4 set. 2013. Disponível em: <http://themoscownews.com/news/20130904/191898252/Putin-talks-Syria-gay-rights-in-interview.html>. Acesso em: 21 jun. 2014.

NSA dishfire presentation on text message collection: key extracts**. The Guardian**, Londres, 16 jan. 2014. Disponível em: <http://www.theguardian.com/world/interactive/2014/jan/16/nsa-dishfire-text-messages-documents>. Acesso em: 22 jul. 2014.

NSA foi usada até para investigar amantes. **TecnoGeek**, 28 set. 2013a. Disponível em: <http://tecnogeek.com.br/nsa-foi-usada-ate-para-investigar-amantes/>. Acesso em: 22 jul. 2014.

NSA employees spied on their lovers using eavesdropping programme**. The Telegraph**, Londres, 24 ago. 2013b. Disponível em: <http://www.telegraph.co.uk/news/worldnews/northamerica/usa/10263880/NSA-employees-spied-on-their-lovers-using-eavesdropping-programme.html>. Acesso em: 22 jul. 2014.

REZENDE, Denis A.; ABREU, Aline F. **Tecnologia da Informação Aplicada a Sistemas de informações Empresariais**. São Paulo: Atlas, 2000.

RISEN, James. Snowden Says He Took No Secret Files to Russia**. The New York Times**, Nova Iorque, 17 out. 2013. Disponível em: <http://www.nytimes.com/2013/10/18/world/snowden-says-he-took-no-secret-files-to-russia.html>. Acesso em: 21 jul. 2014.

ROSSI, Clóvis. Cinco olhos, todos em você**. Folha de S. Paulo**, São Paulo, 09 jul. 2013. Disponível em: <http://www1.folha.uol.com.br/colunas/clovisrossi/2013/07/1308320-cinco-olhos-todos-em-voce.shtml>. Acesso em: 22 jul. 2014.

SAVAGE, Charlie. U.S. Confirms That It Gathers Online Data Overseas. **New York Times**, Nova Iorque, 06 jun. 2013. Disponível em: <http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html>. Acesso em: 22 jul. 2014.

SEIPEL, Hubert. **Transcript:** ARD interview with Edward Snowden**. La Fondation Courage**. 27 jan. 2014. Disponível em: <https://www.freesnowden.is/fr/2014/01/27/video-ard-interview-with-edward-snowden/>. Acesso em: 21 jul. 2014.

SERRA, J. Paulo. **Manual de Teoria da Comunicação**. Covilhã: Labcom, 2007.

SILVA JUNIOR, Carlos A. da. et. al. O direito internacional subjetivo à defesa nacional e as fronteiras paradigmáticas da atividade de inteligência no Século XXI. **World Citizen Magazine**, v. 1, n. 1. Brasília, DF: Universidade de Brasília, 2013.

SNOWDEN Docs Reveal NSA, DEA Teamed Up to Record Every Cell Phone Call in Bahamas**. Democracy Now**, Nova Iorque, 20 maio 2014a. Disponível em: <http://www.democracynow.org/2014/5/20/snowden_docs_reveal_nsa_dea_teamed> . Acesso em: 21 jul 2014.

SNOWDEN, Edward. Edward Snowden fala sobre o que é a vigilância da NSA, o acesso indiscriminado aos dados pelos funcionários e contratados da NSA. **Debates Munk**, Toronto, maio de 2014b. Disponível em: <http://www.munkdebates.com/snowden>. Acesso em: 22 jul. 2014.

VILAIN, Caroline S. Espionagem estadunidense sobre o Brasil e o leilão do campo de libra uma análise geopolítica. **Revista Economia e Desenvolvimento**, Santa Maria, v. 15, n. 2, 2013.