UNIVERSIDADE FEDERAL FLUMINENSE
INSTITUTO DE ESTUDOS ESTRATÉGICOS
PÓS-GRADUAÇÃO EM ESTUDOS ESTRATÉGICOS E RELAÇÕES INTERNACIONAIS

A ESPIONAGEM ELETRÔNICO-CIBERNÉTICA E A REAÇÃO DO ESTADO BRASILEIRO ÀS REVELAÇÕES DE EDWARD SNOWDEN (2013-2023)

GABRIEL LEONCIO CORRÊA

Niterói - RJ
2023

GABRIEL LEONCIO CORRÊA

A ESPIONAGEM ELETRÔNICO-CIBERNÉTICA E A REAÇÃO DO ESTADO BRASILEIRO ÀS REVELAÇÕES DE EDWARD SNOWDEN (2013-2023)

Trabalho de conclusão de curso de MBA apresentado ao Instituto de Estudos Estratégicos da Universidade Federal Fluminense com parceria ao Centro de Instrução Sylvio de Camargo (Marinha do Brasil) como requisito parcial para a obtenção do título de MBA em Relações Internacionais.

Orientadora: Profa. Dra. Raquel dos Santos Missagia

Niterói - RJ
2023

Folha de Aprovação de Trabalho de Conclusão de Curso em Relações Internacionais (Monografia)

Título do Trabalho: Espionagem eletrônico-cibernética: A reação brasileira, no que tange as políticas públicas, frente as revelações de Snowden

Aluno: Gabriel Leoncio Corrêa

Avaliadores

Avaliador 01: ----

Avaliador 02: Profa. Dra. Raquel dos Santos Missagia (orientadora)

Notas dos Avaliadores	
Nota 1	
Nota 2	

À minha esposa, pela compreensão quanto à minha ausência durante a confecção deste trabalho e pela paciência na leitura de meus esboços.
À professora Raquel Missagia pela orientação, paciência, correção e condução em todo o percurso.

RESUMO

Muito debate surgiu após as revelações de Edward Snowden, um espião que trabalhou para a CIA e para NSA. Segundo este agente, o governo dos EUA possui um sistema de monitoramento que abrange todo o planeta e reúne informações de pessoas comuns e de

governos inteiros. O objetivo deste trabalho é analisar como tais informações impactaram o cenário internacional, com foco nas atitudes internas do governo brasileiro no que tange às políticas públicas. Para isso, o trabalho foi executado sob a metodologia exploratória e foi dividido em quatro partes. Na primeira, serão abordados conceitos básicos para a compreensão do tema, como Guerra Eletrônica, Inteligência de Sinais e Guerra Cibernética, com foco em como essas disciplinas estão interligadas e como podem ser úteis para a espionagem internacional. Na parte seguinte serão demonstradas as principais revelações de Snowden, com foco na coleta de dados em massa no campo eletrônico e cibernético, além de vincular esses acontecimentos ao conceito de inteligência estratégica. A terceira parte analisará o impacto causado nas relações internacionais ao abordar as atitudes da ONU, a consequente reação do governo americano e de outros agentes que, aparentemente, não cooperaram tanto quanto podiam na defesa da privacidade e no combate à espionagem em massa. Na última parte serão abordadas as atitudes do governo brasileiro com relação a sua política pública, o ponto principal será mostrar como esta nação utilizou seus recursos nacionais e influência internacional para reduzir os danos relacionados à espionagem eletrônico-cibernética.

Palavras-chave: Espionagem; Informação; Inteligência Estratégica; Guerra Eletrônica; Guerra Cibernética; Edward Sownden.

ABSTRACT

Much debate arose following the revelations of Edward Snowden, a spy who worked for the CIA and NSA. According to this agent, the US government has a monitoring system that covers the entire planet and gathers information from ordinary people and entire governments. The objective of this work is to analyze how such information impacted the international

scenario, focusing on the Brazilian government's international attitudes regarding public policies. To achieve this, the work was divided into four parts. In the first, basic concepts for understanding the topic will be covered, such as Electronic Warfare, Signals Intelligence and Cyber Warfare, focusing on how these disciplines are interconnected and how they can be useful for international espionage. The following part will demonstrate Snowden's main revelations, focusing on mass data collection in the electronic and cybernetic field, in addition to linking these events to the concept of strategic intelligence. The third part will analyze the impact on international relations when addressing the UN's attitudes, a consequential consequence of the American government and other agents who, apparently, did not cooperate as much as they could in defending privacy and combating mass espionage. In the last part, the Brazilian government's attitudes towards its population security will be addressed. The main point will show how this nation used its national resources and international influence to reduce damage related to electronic-cybernetic espionage.

Keywords: Espionage; Information; Intelligence; Electronic Warfare; Cyber Warfare; Edward Snowden

LISTA DE ILUSTRAÇÕES

FIGURAS

SUMÁRIO

INTRODUÇÃO

Por muitos séculos o acúmulo de riquezas materiais como ouro, diamante, petróleo etc. foi um símbolo de riqueza e poder. Atualmente, a informação e os meios pelos quais ela circula foram alçados a um novo patamar de importância. Nesse sentido, é relevante citar a venda da rede social Twitter por 44 bilhões de dólares[1]- A título de comparação esse mesmo valor equivale a mais de 435 milhões de barris de petróleo (Brent) em 2022[2]. A venda de uma rede social por um preço tão elevado revela a importância das informações que trafegam pelas plataformas virtuais. Dentro do escopo de análise deste trabalho busca-se compreender a relação entre privacidade e meios de comunicação na atualidade. Um indivíduo utiliza voluntariamente os sistemas de telefonia e internet, seus dados são transmitidos diariamente por cabos, antenas e satélites, a mesma coisa pode ser dita sobre determinadas informações e mensagens governamentais. Empresas, Estados e pessoas comuns se renderam aos benefícios da tecnologia, mas poucos estão realmente cientes de seus riscos. Em 2013, um espião americano divulgou à imprensa um sistema de espionagem sem precedentes que envolve todo planeta, abrangendo desde pessoas irrelevantes até chefes de Estado. Esse fato foi muito repercutido no meio internacional e até mesmo Ângela Merkel e a ex-presidente Dilma Rousseff ascenderam como vítimas desse caso.
Edward Joseph Snowden foi espião e prestou serviços tanto para Cia quanto para NSA e optou por expor ao mundo "o serviço de vigilância em massa de populações inteiras protagonizado pelos Estados Unidos" (Snowden, 2019. p.1). Sua explanação abrange principalmente o PRISM, um programa americano de vigilância em larga escala, e outros deste nível "incluindo o Xkeyscore, o Upstream, o Quantuminsert, o Bullrun e o Dishfire" (BAUMAN, 2015. p.1). O presente trabalho visa identificar se a revelação deste sistema de espionagem trouxe impactos na forma como os Estados formulam suas estratégias de segurança cibernética focando especialmente em analisar a consequente atitude do governo brasileiro frente às novas ameaças, como também apresentar os caminhos tomados pela presente república. Desta forma, esta pesquisa objetiva identificar quais medidas o governo brasileiro tomou, no que tange às políticas públicas, para combater a espionagem internacional.

Não há como compreender a espionagem eletrônico-cibernética intergovernamental sem uma base sólida no que tange às áreas que compreendem os meios envolvidos para que essa espionagem seja possível. Elas são: a Inteligência de Sinais, a Guerra Eletrônica e a Guerra Cibernética. Desta forma, o primeiro capítulo do presente trabalho versa sobre esses conceitos fundamentais necessários ao entendimento do contexto como um todo. É tratada a definição de Guerra Eletrônica e sua abrangência, tanto no âmbito convencional quanto satelital. O mesmo tipo de abordagem toma-se com relação à guerra cibernética, ao demarcar suas fronteiras, métodos e suas peculiaridades. Em seguida, ambos os conceitos são relacionados ao enfatizar como estão interconectados de forma indissociável. Por fim, é definido espionagem e demonstrado como essa utiliza esses recursos para o levantamento de dados. As principais fontes de pesquisa deste capítulo serão as obras de David Adamy, de Adam T. Elsworth e Daniel Moore.
O segundo capítulo trata de eventos relevantes no que tange à espionagem realizada pelo governo americano, especificamente aquela exposta por Edward Snowden. É levado em

[1] https://www.bbc.com/portuguese/internacional-63422571. Acesso em: 12 jul. 2023.
[2] https://www.infomoney.com.br/economia/projecao-do-departamento-de-energia-ve-petroleo-em-queda-em-2023-e-2024/#:~:text=O%20pre%C3%A7o%20do%20petr%C3%B3leo%20Brent,US%24%20101%20atingida%20em%202022..

consideração os eventos descobertos até o momento de forma a detalhar a maneira como o governo americano tem agido ou, pelo menos, agiu até 2013. Não é do intuito da presente pesquisa expor qualquer juízo de valor com relação à pessoa de Edward Snowden. Não faz diferença nessa abordagem as controvérsias sobre sua pessoa, seja ele um agente duplo, um traidor, um espião arrependido ou um atual agente americano com o objetivo de mostrar as capacidades de seu governo para fins coercitivos. O objetivo central deste capítulo é a exposição dos acontecimentos, documentos e até o testemunho do citado ex-agente, sem entrar em viés de opiniões controversas e desnecessárias a uma análise cujo objetivo fim é a postura do governo brasileiro frente à ameaça já exposta. Neste é abordado primeiramente a espionagem realizada em redes de telefonia celular ao redor do mundo, em seguida da coleta de dados governamental e o programa PRISM. Por fim será levantado o conceito de Inteligência Estratégica que traz luz aos motivos governamentais para realização desse tipo de espionagem em larga escala. A conceituação desse tipo de inteligência será o suficiente para mostrar que dificilmente haverá fim a coleta de dados em massa e o Brasil precisa estar ciente disso.

O terceiro capítulo mostrará, de forma breve, o impacto das revelações de Snowden no cenário internacional, e vincula esse tipo de espionagem a inteligência estratégica. Será demonstrado, resumidamente, como esse tipo de espionagem estratégica é importante pata as grandes nações e perigosa para os dados do governo, podendo comprometê-lo. O foco está em observar como a comunidade internacional reagiu, elencando as reuniões da ONU, inclusive o posicionamento brasileiro, suas medidas e os desdobramentos internacionais quanto a relação entre Estado, sociedade civil e privacidade do indivíduo, além de observar as atitudes americanas e da União Europeia frente a esta reação. Tendo sido eficaz ou não, as medidas e debates internacionais, no mínimo, deixaram claro à população civil e aos Estados que seus dados não estão seguros na internet e isso é um conhecimento de grande valia.

O quarto capítulo elencará a reação brasileira frente a essa problemática. Será relacionada a posição do Brasil na ONU com suas medidas em território nacional. As legislações brasileiras no que tange à cibernética são abordadas de maneira separada. Primeiramente é observada as leis sobre o assunto, anteriores a Snowden e as leis criadas após suas revelações. A análise compara ambas as fases e deixa evidente o avanço brasileiro, mas também demonstra como nossa legislação é frágil com relação a esse assunto. São analisadas também a cartilha produzida pelo Senado Federal, intitulada “rede vulnerável”, e a CPI da espionagem, além de observas as medidas do governo para tentar reduzir a dependência americana do campo eletrônico e cibernético no que tange aos cabos submarinos.

Dessa maneira, pôde-se concluir que este trabalho demonstra que o Brasil necessita focar no fortalecimento de sua proteção eletrônico-cibernética, com atenção a inteligência estratégica, ao focar em uma política de Estado consolidada e efetiva que envolva tanto a sociedade como as instituições públicas e privadas. Isso não somente desenvolveria o setor de defesa brasileiro como asseguraria segurança quanto às relações do Brasil com os demais países do globo.

CAPÍTULO 1. CONCEITOS BÁSICOS

Este capítulo trata dos conceitos básicos necessários ao entendimento do assunto em questão. Primeiramente será observado, de forma resumida, como as comunicações atuais são dependentes do espectro eletromagnético e, em seguida, definido Guerra Eletrônica e Inteligência de Sinais, que compreendem as formas de aquisição de informação do citado espectro, elencando sua relevância. Será demostrado que tais disciplinas devem ser observadas em conjunto e que toda comunicação no espectro eletromagnético está sujeita a interceptação.
O segundo tópico aborda a Guerra Cibernética. Primeiramente, é definido o conceito 'campo cibernético' no que tange ao ambiente onde ocorre as ações cibernéticas para, em seguida, tratar das peculiaridades envolvidas no assunto principal. Ficará evidente que a guerra cibernética é indissociável do espectro eletromagnético e, consequentemente, todas as disciplinas abordadas nesse capítulo não podem ser observadas separadamente. Em seguida será exposto, de maneira resumida, como funciona o sistema de internet e como a coleta de dados por parte das Big Techs acontece diariamente, formando bancos de dados gigantescos. A espionagem utiliza todos esses conceitos e técnicas para o levantamento de informações em todos os níveis. A contraposição eficaz a essa coleta de dados é de vital importância e tem como condição *sine qua non* entender o que está envolvido, tanto no campo eletromagnético quanto no campo cibernético.

1.1 Introdução à comunicação

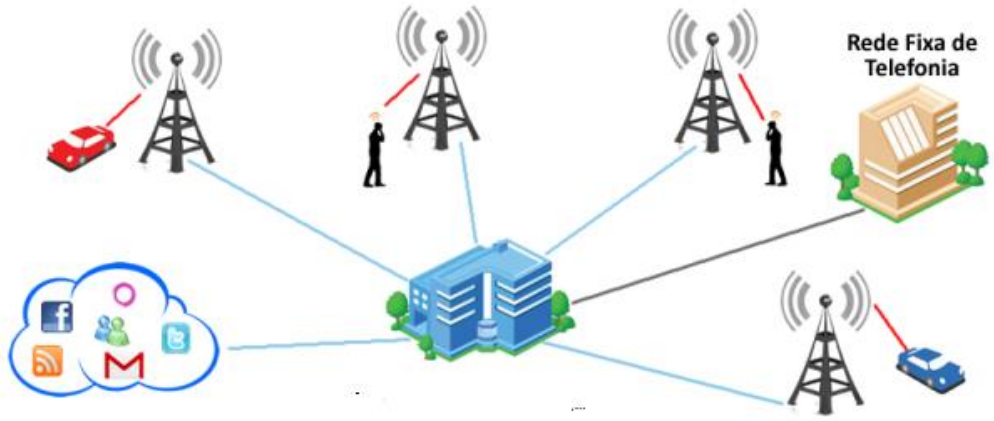
Como é de conhecimento geral, a comunicação a distância pode ser feita através de ondas eletromagnéticas e estas são propagadas de antenas para antenas. Sendo um pouco mais específico, observe que o sistema de telefonia celular e internet é um conjunto complexo de cabos de fibra ótica, antenas (conectadas a torres de rádio e central de dados) e, em muitos casos, até satélites. Esse sistema é feito com uma rede integrada e seu objetivo, como bem argumenta David Goodman (1990, p.1) "é coletar informações de diversas fontes e entregá-las a destinos designados". A rede a qual Goodman se referia é a RDIS que foi substituída (na maioria dos locais) por outras redes integradas até chegar ao que chamamos hoje de telefonia móvel avançada (4G e 5G) [3] ou ao MPLS (uma solução baseada em rede de dados). De forma resumida, em uma ligação, ou acesso aos "dados móveis" o sinal sai do celular de um indivíduo e vai até a torre de telefone mais próxima, essa passa a comunicação por meio de cabos até a torre mais adjunta ao destinatário para que seja propagado o sinal (Silva, 2003, p.79). Quando o celular está em outra região para saber onde se encontra um destinatário é utilizado o centro de comutação móvel (CCM) [4], este faz o registro dos cartões SIM de sua região e os conecta a um conjunto de torres, quando o usuário sai da região controlada por seu CCM as torres de outras regiões enviam constantemente a localização deste usuário para que ele possa receber uma chamada. Desta forma, quando fazemos uma ligação, o sinal vai até o CCM do destinatário, que o localiza e envia a chamada. Esses centros podem conter milhões de registros de chamadas (Ma, 2007. p.1). Isso significa que a localização em massa de diversos aparelhos celular é rastreada independente do GPS estar ou não ativado. Repare que o acesso ao CCM terá como benefício o posicionamento de todos os aparelhos móveis da

[3] Para uma boa base sobre a evolução dos sistemas de telefonia veja o artigo: SILVA, ITALA L. C. S. **Do 1g ao 5g: evolução das redes de telefonia móvel**. UFRB: Bahia, 2016

[4] Para maiores esclarecimentos veja: https://www.simbase.com/iot-glossary-dictionary/mobile-switching-center. Acesso em: 20 de julho de 2023.

região, além disso, por também se tratar de dados móveis, tal centro estará conectado à internet, formando um grande sistema armazenador de dados com acesso à WEB, conforme a figura abaixo.

Figura 1.1 – Integração dos sistemas de comunicação



Fonte: https://www.ecsintl.com/wp-content/uploads/2018/11/TelefoniaMovel.pdf

Como todas as informações passam por esse centro, isso permite a um invasor não apenas a observação das informações como enviar mensagens fraudulentas ou fazer chamadas não autorizadas. Outros tipos de ligações podem ser estabelecidos como a linha direta através de satélites, que também ocorre por ondas eletromagnéticas aliada a tecnologias de localização ou através de serviços de internet como o WIMAX ou outros (Silva, 2016, p.62). Não é ~~d~~o objetivo da presente obra especificar detalhadamente todo o funcionamento desses modos de comunicações, mas é necessário entender que quando um celular acessa a internet ou faz uma ligação os dados são propagados por um sinal de rádio até as torres, estas agem como um sistema integrado, enviando massas de dados, para os locais onde estão seus destinatários. Esses dados podem circular de forma convencional, ou se tratando de internet, por IP, através de fibras óticas. Com relação aos aplicativos de redes sociais e outros do gênero, é necessário entender que a comunicação entre dois celulares é feita através desses aplicativos, em suas bases de dados. Tudo vai do usuário para o Centro de Comutação, em seguida o servidor do aplicativo, em seu *Data Center*[5], faz o processo inverso para o destinatário. É importante tomar ressalva deste fato porque a comunicação não fica restrita apenas a localização do usuário do recebedor, ao contrário, ela é propagada tanto no espaço quanto por cabos e, quando necessário, chega a outros países, tudo está em conjunto em um grande sistema, vinculado a empresas privadas.
Assim, existem diversos pontos do processo de comunicação, seja satelital ou convencional, cuja propagação dos dados se dá por meio de ondas eletromagnéticas. Não é difícil imaginar que qualquer agente ou governo possa fazer investidas no que tange à aquisição desses dados, e é nesse momento que surgem os conceitos de inteligência de sinais (SIGINT) e Guerra eletrônica (GE).

1.2 Guerra eletrônica e Inteligência de Sinais

SIGINT é visto como conjunto de Inteligência eletrônica e inteligência de comunicações (Adamy, 2001, p.4). Segundo Richard Wiley a Inteligência Eletrônica é definida como “a interceptação, análise e uso de sinais de radar para obter informações sobre as capacidades e

[5] Veja: <https://www.cisco.com/c/en/us/solutions/data-center-virtualization/what-is-a-data-center.html>

intenções do inimigo" (Wiley, 2006, p.1). O foco desta é a emissão radar (ou emissores similares, normalmente chamados de Não-Com), que podem ser trafegadas por meios convencionais ou por satélites, perceba também que Wiley parece restringir sua definição ao ambiente do conflito ou da guerra, visto que usa o termo "inimigo". Mesmo fato se aplica a inteligência de comunicações (COMINT) que é a interceptação e análise dos "sinais de comunicação do inimigo com o objetivo de extrair inteligência das informações transmitidas" (Adamy, 2001, p.5). Peter Mathews parece seguir o mesmo caminho ao afirmar que a inteligência de sinais (SIGINT) é "um aspecto da coleta de inteligência militar baseada na interceptação e decodificação das transmissões sem fio de um inimigo" (Mathews, 2013, pp. 5-6).

Torna-se claro que objetivo da SIGINT é obter conhecimentos vitais, através do espectro eletromagnético, sobre determinado agente ou governo, para decifrar suas intenções. Abaixo, ficará evidente que apesar dos teóricos normalmente vincularem esses conceitos a guerra, atualmente eles também são aplicáveis fora desse contexto, em meio não militar. Além disso, essa coleta de ondas, embora esteja vinculada a um inimigo, não restringe a atuação desta inteligência a um nível tático (não obstante existir essa possibilidade). A Inteligência de Sinais está preocupada com adquirir e analisar o máximo de informações possível do espectro eletromagnético para uso futuro.

A Guerra Eletrônica, apesar de muitas vezes apresentar um caráter voltado para o nível tático, tem funcionalidades que se aplicam a outros níveis. Observe o posicionamento do famoso teórico David Adamy ao defini-la como "a arte e a ciência de preservar o uso do espectro eletromagnético (...) enquanto nega seu uso ao inimigo" (Adamy, 2001 .p.3). Corroborando com isso, Elsworth elabora uma definição visando o controle do espectro eletromagnético e ataque através de ondas (Elsworth, 2010. p.xi). Não é de grande valia aos fins deste trabalho os aspectos relacionados ao ataque eletrônico para executar um bloqueio, especificamente, pois são poucos os casos em que estes saem do nível tático e não são de grande contribuição para fins de espionagem[6], contudo, vinculado a Guerra Cibernética, como veremos abaixo, um ataque pode ser muito útil a coleta de dados. As demais atribuições da GE são claramente relevantes mesmo sob uma perspectiva exclusiva do campo eletromagnético. Perceba que quando Adamy e Elsworth falam sobre preservação do uso do espectro eletromagnético, estão se referindo a capacidade de interceptar e analisar sinais para registro (Elsworth, 2010. p.60). Nesse sentido a partir do momento em que um indivíduo, força ou governo está atuando em determinado local com a "preservação do espectro", significa que ele consegue colher ondas para fins de ponderações imediatas e posterior trabalho de análise. É perceptível que existem muitos fatores envolvidos nessa coleta de dados, como por exemplo, a necessidade de que o sinal eletromagnético do emissor esteja a uma distância em que a coleta de dados seja possível, assim, a potência recebida do sinal deverá ser maior que a sensibilidade da antena que está efetuando a busca (Adamy, 2009, p. 237). Existem também outras preocupações como o correto direcionamento do receptor e a não confusão com sinais parecidos ou falsos (Genova; James, 2018, p.115).

[6] Um ataque eletrônico (MAE) é o uso do espectro eletromagnético para impedir ou restringir o uso do espectro por parte do inimigo. O ataque eletrônico também é vinculado a uma arma cuja destruição é causada apenas por ondas eletromagnéticas. Para um bom exemplo, no campo da GE, de uma arma eletromagnética cujas implicações sobem ao nível político veja as recentes armas a laser desenvolvidas pelos chineses para destruir satélites em: Kan, Shirley. China's Anti-Satellite Weapon Test. Para as implicações resultantes do uso deste tipo de armamento veja o artigo High-Energy Laser Weapons: Overpromising Readiness (p.36) da revista The US Army War College Quarterly: Parameters. Vol.48. N°4. Art.6.

Nenhum desses fatores é impeditivo, contudo, dependendo do emissor a localização do agente poderá variar bastante, caso se esteja buscando a interceptação de sinais HF[7], o responsável pela coleta poderá estar em seu próprio país, a milhares de quilômetros de distância, devido a reflexão ionosférica (Adamy, 2004,p. 107-108), para um sinal VHF ou UHF, como o de celular, será necessário uma maior proximidade (Adamy, 2004.p. 113-116), se tratando de emissões proveniente de um satélite será necessário estar na direção em que o satélite aponta, o que irá requerer esforço adicional ao agente de inteligência, mas nada que traga grandes dificuldades (Adamy, 2004,p. 113-116). Para proteger-se desse tipo de interceptação é possível efetuar determinadas formas de criptografia de sinal[8], mas isso não impede a coleta de dados em si, apenas dificulta a compreensão do receptor (Poisel, 2002, p. 157).

Tudo isso é suficiente para afirmar que, tecnicamente, por se tratar de ondas eletromagnéticas, independente dos meios (sejam eles através de antenas convencionais ou satelital), frequência do sinal ou tipo de criptografia, sempre haverá uma maneira de receber esse sinal, contanto que o receptor esteja posicionado no local certo. A menos que alguém seja ingênuo o suficiente para acreditar que exista algum tipo de criptografia de sinal indecifrável, a comunicação a distância através de ondas eletromagnéticas deve ser observada como vulnerável e seria necessário muito cuidado e análise quando se opta por usar o espectro eletromagnético, pois dificilmente tal forma de comunicação alcançaria um patamar cuja designação "seguro" seja aplicada a ele. Ainda que se opte por tecnologias militares como saltos de frequências, encriptação ou modulações diversas, tudo pode ser captado e, consequentemente, analisado, cedo ou tarde o conteúdo da mensagem virá à tona.

Fato relevante a ser citado como exemplo é que a empresa Huawei foi autorizada a construir um pagode branco de 70 pés em Washington, tal arquitetônica asiática supostamente seria um marco turístico, contudo, foi descoberto pelo governo americano que a estrutura estaria dotada de antenas para efetuar inteligência de Sinais em plena capital americana. O monumento seria localizado em altura privilegiada com acesso eletromagnético ao Capitólio[9].

A singela diferença entre SIGINT e GE está nos propósitos para qual o sinal é recebido. O primeiro visa simplesmente recolher emissões para determinados fins de inteligência, com muito detalhamento, para posterior utilização nos campos táticos, estratégico ou políticos, enquanto o segundo busca a superioridade, uso desimpedido e preservação do espectro eletromagnético, o que pode ser elevado para o nível estratégico ou superior. Outras preocupações da GE se restringem ao campo tático da realização de um conflito. Deve-se ressaltar que a diferença entre essas disciplinas tende ao desaparecimento, pois se "tornam cada vez mais vagas à medida que a complexidade dos sinais aumenta" (Adamy, 2001, p.4).

Em face do exposto, é possível afirmar que os conceitos relacionados a Guerra Eletrônica e a Inteligência de Sinais, em conjunto, podem ser utilizadas com o propósito de interceptação, análise e interpretação de sinais eletromagnéticos como, por exemplo, rádio, telefone, satélite, internet ou radar, com o objetivo de obter informações relevantes sobre as intenções ou atividades de indivíduos, organizações ou governos para determinados fins nos diversos níveis das Relações Internacionais. Está envolvido aqui todo e qualquer acesso não autorizado de informação que se propague por qualquer meio no espectro eletromagnético, em qualquer

---

[7] HF significa High Frequency, VHF significa Very High Frequency e UHF Ultra High Frequency. Para uma percepção técnica veja o excelente resumo fornecido na obra Adamy, David L. - Electronic Warfare Pocket Guide. p.5.

[8] A criptografia é uma maneira de modificar a onda transmitia para dificultar a compreensão da mensagem ou dificultar a percepção de que o que está sendo transmitido seja de fato uma mensagem, como muito bem salientou Frater, Michael R. Electronic Warfare for the Digitized Battlefield-Artech Print on Demand (2001). p. 62-64.

[9] Uma matéria elucidativa sobre o assunto foi publicada pela CNN em: https://www.cnnbrasil.com.br/internacional/fbi-conclui-que-equipamentos-da-chinesa-huawei-podem-interceptar-comunicacao-do-departamento-de-defesa-dos-eua/.

lugar do mundo. Assim, os conceitos de SIGINT e GE são de extrema relevância para fins de inteligência estratégica (como ficará claro no decorrer desta obra, particularmente no capítulo segundo).
Outro ponto importante é que o citado aumento de tecnologia trouxe outras consequências. As comunicações se tornaram amplamente digitais, com muita emissão de dados em banda larga. É muito difícil desvincular o ambiente eletromagnético da guerra cibernética, como muito bem salientou Elsworth "A distinção entre Guerra Cibernética e Guerra Eletrônica está se tornando cada vez mais confusa" (Elsworth, 2010). Isso significa que a superioridade eletromagnética dará ao governo em questão extensa gama de conhecimento que, por se tratar de dados, pode envolver vídeos, fotos, mensagens de texto ~~e~~ etc. Para Elsworth aspectos da aquisição de informação, seja através de inteligência de sinais ou Guerra Eletrônica, não estão mais vinculados apenas a mensagens de voz, como no passado, dado o grande avanço tecnológico, a cibernética se tornou fundamental, não é à toa que parte significativa de sua obra sobre GE é dedicado ao campo cibernético (Elsworth, 2010, p. 13-37). Ele afirma que a confluência entre essas duas disciplinas "é uma tendência crescente, à medida que os dois domínios se tornam cada vez mais interligados" (Elsworth, 2010, p. 12). Mas o que exatamente seria a guerra Cibernética (GC)?

1.3 Guerra Cibernética

Alguns teóricos, como Olen L. Kelley definem Guerra Cibernética (GC) como "O uso da tecnologia para controlar e interromper o fluxo de informações (...) é uma forma de guerra da informação que envolve o uso de redes de computadores para alcançar objetivos militares" (Elsworth, 2010. p.12-13). Novamente, como ocorre com a Guerra Eletrônica e a Inteligência de Sinais, apesar da utilização do termo "militar" e da aparente vinculação de Kelley exclusivamente com um conflito armado e sua utilização no nível tático, não podemos restringir seu uso nesse sentido. Esta disciplina deve ser considerada de maneira mais ampla, como muito bem salientou Kenneth J. Knapp ao definir GC, no que tange ao ambiente cibernético, como "uma variedade de tipos de conflito que abrangem dimensões políticas, econômicas, criminais, de segurança, civis e militares". Knapp nem mesmo tenta diferenciar guerra cibernética de guerra de informação e parece sugerir que são termos intercambiáveis, ou com a primeira fazendo parte da segunda, o que faz sentido, visto a ênfase natural da GC no que tange a manipulação e aquisição de dados. Ele entende a Guerra Cibernética como "ações destinadas a proteger, explorar, corromper, negar ou destruir informações ou recursos de informação para obter uma vantagem significativa" (Janczewski, 2008, p.18).
Seguindo uma linha parecida, Blaise Cronin e Holly Crawford (1999) não fazem diferenciação entre Guerra Cibernética e Guerra de Informação, afirmando que são uma variante comum, profundamente ligada à Guerra Eletrônica. Eles elaboram sua definição de GC com conceitos de infiltração, degradação, subversão e coleta de dados dos sistemas de informação do alvo. Contudo, afirmam que observar de tal disciplina somente no contexto militar, como parece sugerir diversas obras sobre o assunto, acaba "obscurecendo o fato de que muitos dos princípios e suposições subjacentes têm aplicação muito além dos contextos militares convencionais" (Cronin; Crawford, 1999, p. 257).
Os temas debatidos neste capítulo devem ser compreendidos dentro de um espectro mais amplo, que não se restringe aos temas militares. Essa percepção é adensada por eventos que demonstram a intensificação da atuação eletrônico-cibernética, "causando problemas sociais potencialmente sérios e criando novos desafios para o sistema de justiça criminal" (Cronin; Crawford, 1999, p. 257). Para eles, observar a Guerra Cibernética e Eletrônica como exclusivamente tática ou militar é prova de uma visão "míope" da realidade, pois foram projetadas para "garantir o domínio militar contínuo dos EUA na era pós-Guerra Fria"

(Cronin; Crawford, 2006, p.1). Essa última expressão demonstra como a Guerra Eletrônico-cibernética é de importância fundamental, estando ligada naturalmente as Relações Internacionais, em um nível político. A conceituação dessa disciplina abaixo do nível estratégico é uma atitude retrógrada, Amit Sharma pontuou muito bem ao afirmar que a Guerra Cibernética deve ser vista "como principal meio de alcançar grandes objetivos estratégicos na ordem mundial contemporânea" (Czosseck; Geers, 2009. p. 4).

O campo da Guerra Cibernética voltado exclusivamente à coleta de informações chamaremos de Espionagem Cibernética (alguns autores fazem completa distinção entre a Espionagem e a Guerra Cibernética[10], mas sua dicotomia está pautada em um conceito de Guerra Cibernética que se restringe exclusivamente ao conflito militar, neste trabalho não seguiremos esta linha argumentativa, dado o exposto acima). Com relação a esse tipo de espionagem[11], Moore afirma que, ao coletar os dados, ela "raramente resulta em escalada ao nível de hostilidades abertas" (Moore, 2022, p. 35). De fato, até o momento, esse tipo de atitude não chegou a desencadear uma guerra física, mas tem causado muitas tensões complicadas.

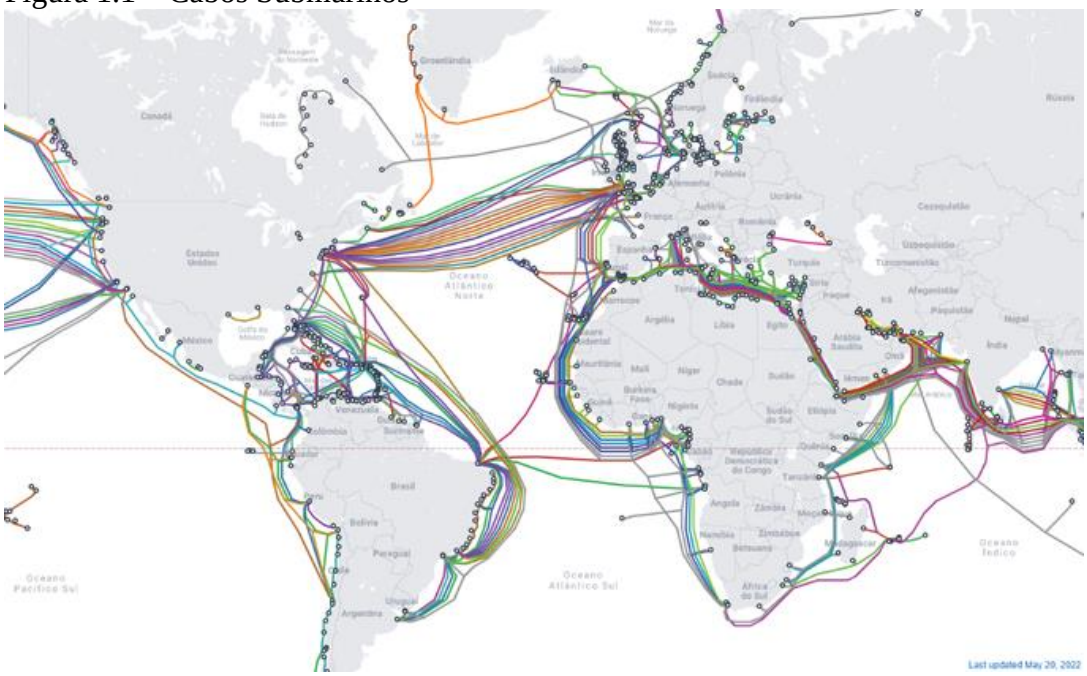
Veja por exemplo, o caso divulgado pela FyreEye, em 2020, ocorrido no SolarWinds Orion. Por ser um dos sistemas de análise da dados mais utilizados do mundo é de conhecimento geral que a citada plataforma é voltada para o monitoramento dedados e análise de desempenho, nesse sentido, uma empresa que adquire o produto pode utilizá-lo para monitorar os servidores, switches, roteadores, aplicativos e qualquer outros dispositivos conectados à rede. Para isso, é necessário amplo acesso e armazenamento de todas as informações propagadas em determinada rede, se tornando, por razões obvias, um alvo para Hackeres. Houve um ataque cibernético a esta plataforma voltado para coleta de dados, segundo a FyreEye a espionagem logrou êxito em ter acesso a uma vasta gama de informação de "inúmeras organizações públicas e privadas em todo o mundo" (FyreEye, 2022). O caso tomou tamanha proporção em empresas públicas de grande porte que o congressista americano Jason Crown afirmou que tal espionagem era equiparada ao dano ocasionado em Pearl Harbor (Moore, 2022, p. 36), e o senador Dick Durbin afirmou com todas as letras que uma coleta de dados desse vulto era "uma declaração de guerra" (Wolf; Pieterson, 2020). Não é difícil imaginar que a tensão internacional causada pela espionagem pode contribuir para gerar tensões políticas. Alguns autores afirmam que, por ser uma prática comum entre as grandes nações, não haverá retaliações[12], a tendência, porém, com o aumento da tecnologia, é elevar o nível e a quantidade das informações coletadas, podendo chegar a episódios sensíveis e vitais à segurança de determinada nação. Ao analisar aa história Moore (2022) afirma que a espionagem sempre existiu e raramente foi pretexto para conflito, no entanto essa constatação pode se mostrar falha para o futuro, principalmente porque no passado a forma de adquirir informações era precária. Esse viés interpretativo inibe a percepção de que atualmente muito pode ser perdido, quando se trata de banco de dados governamental e informações confidenciais. Visto todo esse entorno, dificilmente a espionagem continuará sendo tratada como algo comum, apesar de ser uma atuação praticamente rotineira. Certamente estará presente, mas ainda carecemos de elementos para construir cenários prospectivos sobre o desenrolar das consequências da espionagem no mundo contemporâneo.

1.4 Peculiaridades do espaço cibernético integrado

[10] Do original: "as primary means of achieving grand strategic objectives in the contemporary world order".
[11] Como o ambiente cibernético e o eletromagnético estão profundamente vinculados, a presente obra tratará da espionagem que envolve os campos da Guerra Cibernética, Eletrônica e da Inteligência de Sinais, em conjunto, com o termo espionagem Eletrônico-Cibernética.
[12] Moore (2022 p.27-40) parece afirmar que como todos os países praticam espionagem, dificilmente alguma nação irá utilizar a coleta de dados como pretexto para guerra.

Todo o sistema de comunicação atual é feito através de cabos e/ou ondas eletromagnéticas. Neste entorno, além das considerações já citadas sobre a coleta de dados por meio de antenas, a interceptação da informação pode ser feita com crimpagem física dos cabos ou mediante *malwares* que podem ser enviados pelo espectro eletromagnético (o que caracterizaria o ataque eletrônico - Conceito de Guerra Eletrônica vinculado a Guerra Cibernética), ou através das próprias *Big Techs*. O sistema de comunicações, como um todo, é sumariamente vulnerável, primeiramente, por causa das considerações já feitas com relação ao espectro eletromagnético e, em segundo lugar, porque boa parte dos cabos submarinos passam por países que sediaram grandes escândalos de coleta de dados. Veja, por exemplo, a imagem abaixo sobre a rota dos cabos submarinos:

Figura 1.1 – Cabos Submarinos



Fonte: https://www.gov.br/anatel/pt-br/dados/infraestrutura/cabos-submarinos

Segundo o Ministério das Comunicações mais de 90% de toda transmissão entre nações é feita através de cabos submarinos[13] e, de acordo com a imagem acima, pouquíssimos cabos nacionais não seguem direta, ou indiretamente, para os Estados Unidos. Normalmente, para acessar a internet um indivíduo comum utiliza navegadores, estes, na prática, levam seus dados além das fronteiras internacionais, conforme assevera Tozetto (2013):

> Quando um brasileiro inicia seu navegador de internet e digita o endereço de um site que está hospedado em um servidor na Europa ou na Ásia, o computador empacota a solicitação e a despacha pela rede, com o endereço do servidor de destino. As informações são transmitidas por meio da conexão de banda larga públicas ou privadas e, ao chegar às fronteiras do País, seguem seu caminho por meio de cabos submarinos. Nas "estradas" da internet, o pacote de dados percorre milhares de quilômetros até chegar ao servidor de destino. Depois de processar a solicitação, o servidor gera um novo pacote de dados com as informações solicitadas pelo usuário e o despacha de volta pela internet. (Tozetto, 2013) [14]

[13] Disponível em <https://www.gov.br/anatel/pt-br/dados/infraestrutura/cabos-submarinos>
[14] Disponível em <https://nic.br/noticia/na-midia/apos-espionagem-dos-eua-brasil-tenta-acelerar-construcao-de-cabos-submarinos/>

Isso significa que um simples clique num navegador para abrir um site percorre distâncias continentais, tanto por meio eletromagnético quando por meio de cabos. A pergunta que surge ao observar isso é: "Quem é o responsável por esses cabos?". Como o custo é elevado há um conjunto de empresas que fazem esse tipo de serviço. Normalmente, *Big Techs* como o Google ou a Meta fazem consórcios para bancar o lançamento e empresas especializadas, como a Seaborn Network ou a Huawei Marine Networks cuidam da parte técnica, mas as grandes empresas acabam como proprietárias. Perceba que o Google, por exemplo, é o proprietário do cabo Firmina que liga o Brasil, Argentina e Uruguai aos Estados Unidos[15] e a empresa americana SubCom juntamente com a chinesa Huawei são fornecedores de vasta gama desses cabos ao redor do mundo[16]. O usuário da internet deve estar ciente que, esteja ele usando ou não um navegador do Google, existe grande possibilidade de que seus dados estejam sendo trafegados por algo que pertence, ou que teve o apoio do Google (ou empresas similares), para passar a existir. Independentemente do que acessamos, muito provavelmente, nossos dados passam por território americano e nossos computadores, com todos os nossos arquivos, estão conectados nesse sistema complexo.

Em tese, para um observador comum, ao levar em consideração os princípios das disciplinas acima, não parece ser de grande dificuldade ao governo americano, por exemplo, coletar de dados, visto sua posição privilegiada, com acesso a dois oceanos e vasta gama de cabos submarinos em sua região, ainda mais se houver a ajuda das grandes *Big Techs*.

Com relação a essas empresas, destaca-se que no próprio termo de serviço do Google afirma-se que manterá os direitos de propriedade intelectual de um usuário, mas também assevera que pode compartilhar e divulgar seus sados, contando que não fira esse direito citado[17]. Nesse sentido o óbvio acontece, tudo que é posto no Google, ele terá o direito utilizar, sem ferir a propriedade intelectual. Não fica claro os limites para essa utilização (apesar da afirmação que será utilizado para fins de propaganda e coisas desse gênero, nada expõe um limite nesse tipo de utilização, nem restringe seus fins para determinado curso):

> Também coletamos o conteúdo que você cria, de que faz upload ou que recebe de outras pessoas ao usar nossos serviços (...) Coletamos informações sobre os apps, navegadores e dispositivos que você usa para acessar os serviços do Google. As informações que coletamos incluem identificadores exclusivos, tipo e configurações de navegador, tipo e configurações de dispositivo, sistema operacional, informações de rede móvel, incluindo nome e número de telefone da operadora e número da versão do aplicativo. Também coletamos informações sobre a interação de apps, navegadores e dispositivos com nossos serviços, incluindo endereço IP, relatórios de erros, atividade do sistema, além de data, hora e URL da sua solicitação. Coletamos essas informações quando um serviço do Google no seu dispositivo entra em contato com nossos servidores, por exemplo, quando você instala um app da Play Store ou quando um serviço verifica se há atualizações automáticas[18].

Ademais,

> Se você estiver usando um dispositivo Android com apps do Google, o dispositivo entrará em contato periodicamente com os servidores do Google para fornecer informações sobre o dispositivo (...) Se você usa nossos serviços para fazer e receber chamadas ou enviar e receber mensagens, podemos coletar informações (...) Quando você usa nossos serviços, coletamos informações sobre sua localização (...) Em algumas circunstâncias,

---

[15] Disponível em <https://www.submarinecablemap.com/submarine-cable/firmina>

[16] Basta entrar no site confiável ao lado e escolher o cabo, você poderá constatar as empresas que são proprietárias e as que são lançadoras dos cabos submarinos. Disponível em <https://www.submarinecablemap.com>

[17] Disponível em https://policies.google.com/terms?hl=pt-BR#footnote-your-content Acessado em: 20/07/2023. Está escrito que, com relação a seus dados compartilhados, o Google "hospede, reproduza, distribua, comunique e use seu conteúdo".

[18] Disponível em: https://policies.google.com/privacy?hl=pt-BR Acessado em: 20 jul. 2023.

> o Google também coleta informações sobre você de fontes de acesso público (...) Também podemos coletar informações sobre você de parceiros confiáveis[19]

Com esse tipo de termo de serviço o Google pode, dependendo do caso, coletar praticamente todas as informações de um celular android ou computador e os fins dessa coleta não fica claro ao usuário. Seus termos dão apenas exemplos de como os dados podem ser utilizados, sem restringir sua atuação com palavras como "apenas", usa-se expressões amplamente vagas e não conclusivas. O ponto relevante a este trabalho não é somente o acesso irrestrito do Google (ao afirmar claramente que irá vasculhar os dispositivos), mas o armazenamento de suas informações em um grande banco de dados vinculado a uma "conta pessoal". Tal concentração e organização de dados, se efetuada conforme está escrito, facilita, em muito, a coleta de informações por parte de terceiros, seja permitida ou não. Não há necessidade de expor todos os termos de serviços das redes sociais e de aplicativos vinculados a Microsoft[20], Apple[21], entre outros, basta dizer que direta ou indiretamente escreveram de forma bem parecida com o Google.

Não é o intuito deste trabalho levantar qualquer suposição ou acusação contra essas empresas, basta apenas ressalvar que um agente ou governo (como o americano, por exemplo), caso tenha oportunidade de coletar dados destas *Big Techs* e de outros sistemas, como os de telefonia, logrará acesso a informações em massa de muitos indivíduos espalhados por todo o planeta. Ao alinhar isso aos conceitos de Guerra Eletrônico-cibernética e Inteligência de Sinais expostos neste capítulo, é possível vislumbrar um sistema de espionagem sem fronteiras, onde toda a informação, tanto propagada pelo espectro eletromagnético quanto trafegada por meio de cabos submarinos ou terrestres sejam interceptadas e pesquisadas em um sistema integrado. Contanto que haja antenas posicionadas em locais estratégicos e coleta de dados cibernéticos das centrais com maior volume de dados, não haverá limites para aquisição de informação. Esse monitoramento que pode se tornar ilimitado é uma capacidade estratégica relevante, contudo desperta muitas questões sobre quais são os limites do poder estatal frente ao direito de privacidade de cada indivíduo. No próximo capítulo apresentamos de forma sintética as denúncias realizadas por Edward Snowden.

[19] Ibidem.
[20] Disponível em <https://privacy.microsoft.com/pt-br/privacystatement>
[21] Disponível em <https://www.apple.com/legal/privacy/br/>

CAPÍTULO 2. DOCUMENTOS REVELADOS POR EDWARD SNOWDEN E A INTELIGÊNCIA ESTRATÉGICA

Existe grande possibilidade de que e-mails, ligações, SMS ou uso de Chats de aplicativos de indivíduos comuns estejam sendo armazenados em um grande banco de dados pesquisável (Snowden, 2019.p.9). Existem muitos debates sobre a preservação da privacidade de dados dos usuários da rede global de comunicação, mas essa discussão também deve refletir sobre os limites desse tipo de espionagem, principalmente no que tange às informações governamentais.

Edward Snowden prestou serviços para CIA e para NSA, em 2013 divulgou grande quantidade de documentos oficiais que evidenciavam um sistema de monitoramento e coleta de informações feito pelas grandes potências. Todo o globo estava envolvido como alvo, desde pessoas comuns até chefes de estado. Ele disponibilizou esses documentos a determinados jornalistas de sua confiança (Snowden, 2019, p..278-283) e isso causou sérios problemas diplomáticos e internos aos EUA. Segundo ele:

> Durante esse período de sete anos, participei da mudança mais significativa da história da espionagem estadunidense – da vigilância direcionada a indivíduos à vigilância em massa de populações inteiras. Ajudei a tornar tecnologicamente viável que um único governo coletasse todas as comunicações digitais do mundo, que as armazenasse por eras e fizesse buscas nelas à vontade (Snowden, 2019. p.1).

O presente capítulo trata de descrever os mais relevantes casos de espionagem eletrônico-cibernética com base nos documentos oficiais da NSA, e de outras agências, que Snowden vazou à imprensa. É digno de nota que muitos desses documentos causaram impactos significativos que podem ser vistos claramente nas declarações do ex-presidente Obama, nas reuniões da ONU, e nas novas leis criadas sobre este tema. Primeiramente serão abordados os casos vinculados a criptografia e acesso a telefones móveis, abrangendo: a invasão que roubou milhões de chaves de criptografia de grandes empresas de telefonia celular, o que fornece a agências de espionagem amplo acesso a ligações ao redor do mundo; os computadores Quantum que efetuam quebra de quase todo tipo de criptografia, incluindo dados bancários; o Projeto *Dishfire* que coleta (ou coletava) milhões de SMS diariamente, além de ter acesso à localização de quem estiver com o celular na mão, detalhes do cartão de crédito, entre outras coisas; e a petição judicial secreta para amplo acesso aos dados da Verizon, AT&T e BELL (gigantes empresas de telefonia celular), incluindo não apenas os dados em solo americanos, mas de todas as suas subsidiárias e parceiras em todo mundo.

Em seguida são descritos os casos direcionados a governos e organizações internacionais, que incluirão: o gualdripar de dados da embaixada da Índia; a coleta não autorizada de dados da ONU; os emblemáticos eventos da interceptação das chamadas telefônicas de Ângela Merkel e da ex-presidente Dilma Rousseff, que incluiu a tomada de dados governamentais e de empresas estatais sensíveis, como a Petrobras; e o famoso programa PRISM, juntamente com o *Upstream Collection*. Por fim, esse contexto é analisado a partir do conceito de Inteligência Estratégica que traz luz aos motivos por trás de tamanho sistema de espionagem.

Todas os episódios acima são importantes para se ter real noção da profundidade e acesso à informação dessas agências de espionagem. Esses eventos são tratados resumidamente, e sua relevância para esta obra é observada quando todos eles são postos em conjunto. Não será abordado profundamente o caso brasileiro, este será descrito com maior profundidade no capítulo 4.

2.1 O fim da Segurança

Conforme exposto nos conceitos de Inteligência de Sinais, as chaves de criptografia são parte fundamental da segurança das comunicações, sem elas, qualquer agente ou governo que tenha antenas posicionadas em local estratégico pode ter acesso a todo conteúdo do tráfego eletromagnético de forma simples e imediata. Apesar das chaves criptográficas darem certa segurança, não se pode ter total confiança nelas, ainda mais considerando os escândalos que envolvem as grandes empresas voltadas para área.

Os documentos da NSA sugerem uma invasão feita por essa agência de inteligência em conjunto com a sua contraparte britânica, a *Government Communications Headquarters* (GCHQ), por meio de um *malware*, aos sistemas de computadores da empresa holandesa Gemalto (a maior fabricante de cartões SIM do mundo). É digno de nota que as empresas de telefonia celular não costumam produzir cartões SIM, então, grande parte delas (das mais diversas nações) recorrem à gigante holandesa (Scahill, 2016).

Aparentemente, essas agências de inteligência britânica e americana efetuaram a cópia do banco de chaves de criptografia de praticamente todos os países em que os chips são utilizados. Isso permite o monitoramento tanto de chamadas de voz quanto de envio de dados, tendo potencial para interceptações singulares em tempo real ou a banco de dados de um centro de comutação. Em 2013, essa empresa produzia 2 bilhões de cartão SIM por ano em pelo menos 85 países (incluindo para as principais empresas brasileiras[22]). De maneira prática, essas agências poderiam ter acesso à boa parte das chamadas de telefonia celular do planeta sem nenhum tipo de mandado judicial (Scahill, 2016).

A Gemalto só tomou conhecimento do caso quando os documentos vazaram. Após esse fato, um de seus maiores gestores afirmou: "Estou perturbado, bastante preocupado com o que aconteceu - disse Paul Beverly, vice-presidente executivo da Gemalto, ao "The Intercept" (Scahill, 2016)[23]. Snowden, em entrevista ao *Reddit Ask Me Anything*, afirmou que "a única maneira de lidar com o comprometimento da segurança é recolher e substituir cada SIM vendido pela Gemalto"[24] (Zetter, 2015).

As agências de inteligência acreditavam ter a posse de nada menos que toda a rede da Gemalto a sua disposição e possuíam a capacidade de processar entre 12 e 22 milhões de chaves por segundo (Scahill, 2016). Como a Gemalto está sediada em Amsterdam, após tomar conhecimento deste caso, o porta voz de inteligência do D66 (holandês) Gerard Schouw respondeu: "É inacreditável. Inacreditável. Não queremos que os serviços secretos de outros países façam coisas como esta" (Scahill, 2016).

Por se tratar de ondas eletromagnéticas, ao obter essas chaves, o agente que busca a informação passará a operar apenas com recepção, sem necessidade de acionamento de nenhum tipo de sistema (conforme já explanado no capítulo 1), isso significa que não existe possibilidade de ser rastreado ou descoberto por meio de computadores, seja da Gemalto ou das empresas telefônicas. A única maneira de ser identificado é fisicamente, na estação de coleta ou se o agente for delatado. Se não houver emissões, o sigilo da espionagem será absoluto (a menos, é claro, que o espião em questão deixe suas antenas em locais plenamente visíveis, mas não se espera esse tipo de amadorismo de prestadores de serviços da NSA ou da GCHQ).

Conforme os conceitos básicos de Guerra Eletrônica (veja capítulo 1), é fácil perceber que a interceptação de chamadas de telefonia celular exigiria uma proximidade relevante entre

---

[22] A TIM fechou esse tipo de parceria com a Gemalto (Disponível em: https://g1.globo.com/economia/noticia/2013/02/press-release-from-business-wire-gemalto-23.html) a Vivo (Souza, 2013), a Claro (Disponível em: https://www.securetechalliance.org/claro-brazil-selects-gemalto-for-mobile-network-optimization/) e a OI (TELETIME, 2007)

[23] Do original: "I'm disturbed, quite concerned that this has happened," Paul Beverly, a Gemalto executive vice president, told The Intercept.

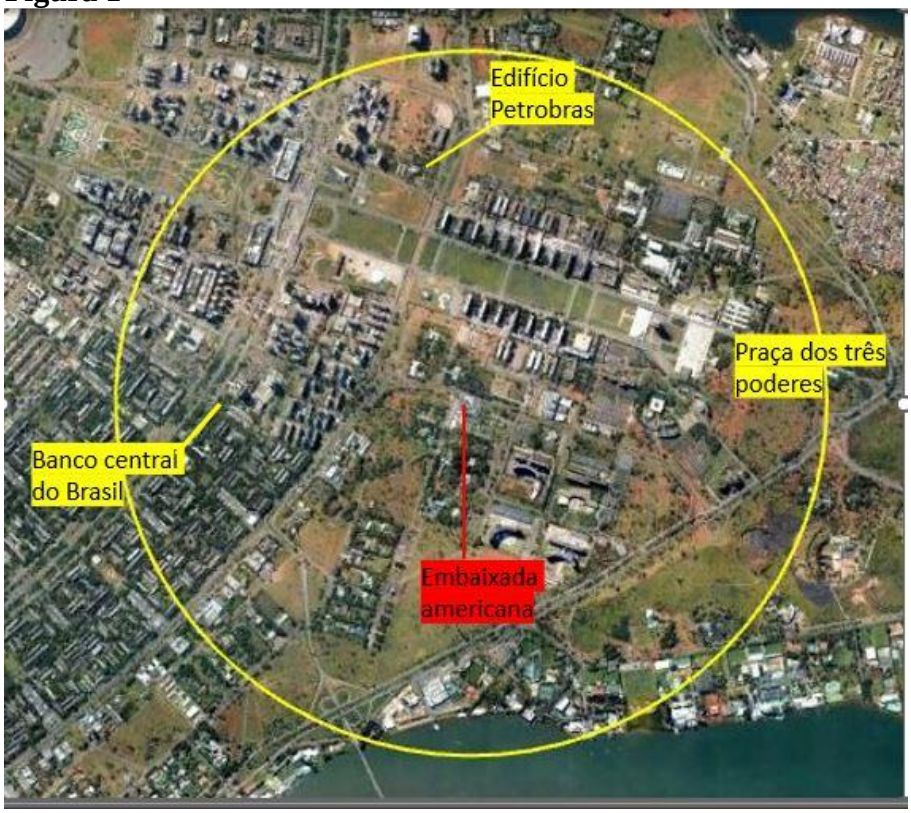
[24] Do original: "the only way to address the security compromise is to recall and replace every SIM sold by Gemalto".

o interceptador e o alvo, visto tratar-se de sinais VHF ou UHF, isso poderia trazer algumas dificuldades aos agentes da NSA, dado a necessidade de deslocamento até os locais de interceptação. Porém devemos lembrar que a imensa maioria das chamadas passam pelos Centros de Comutação, além disso, os Estados Unidos possuem embaixadas em muitos países, dificilmente alguém reclamaria de uma antena sendo colocada em um local que precisa se comunicar com diversas outras embaixadas em todo mundo. No campo da produção de inteligência estratégica uma embaixada é um ponto relevante na aquisição de dados. Como muito bem asseverou Scahill e Begley (2015):

> As agências de inteligência colocam antenas de alta potência, conhecidas como "ninhos de espionagem", no topo das embaixadas e consulados dos seus países, que são capazes de aspirar dados enviados de ou para telemóveis nas áreas circundantes. O Serviço de Coleta Especial conjunto NSA/CIA é a entidade líder que instala e equipa esses ninhos para os Estados Unidos. Uma embaixada situada perto de um parlamento ou de uma agência governamental poderia facilmente interceptar as chamadas telefónicas e as transferências de dados dos telemóveis utilizados por funcionários governamentais estrangeiros.

Nesse sentido, um exemplo bastante interessante é a distância entre a embaixada americana em Brasília e a praça dos três poderes, de apenas 1,3 Km (aqui, deve-se incluir os prédios dos ministérios, a sede do Supremo Tribunal Federal, o palácio do planalto, entre outros), conforme imagem abaixo (raio do círculo de 2 Km):

Figura 1 -



Fonte: Google Earth

Além disso, na própria figura, podemos observar que em um raio de apenas 2 Km desta embaixada encontra-se o Banco Central, o palácio da Petrobras e outras áreas que poderiam ser consideradas como sensíveis à segurança nacional no que tange ao tráfego de informações. Atualmente, na pior das hipóteses (5G - maior frequência), o sinal de um telefone celular convencional percorre em média 1,6 Km (Drullis, 2023). É possível concluir, a partir dos conceitos expostos no capítulo 1, com significativa parcela de certeza, que as chamadas feitas por celular comum de todos os parlamentares brasileiros, até mesmo do

presidente da república, estão ao alcance da NSA ou de qualquer agência de inteligência americana, basta haver o desejo de adquiri-las e a instalação de uma antena com um sistema adequado[25]. É possível que todas as chamadas convencionais realizadas por senadores, ou pelo chefe de estado brasileiro estejam comprometidas. Se houver a posse das chaves de criptografia dos atuais cartões SIM do Brasil, o monitoramento é executado de maneira extremamente simples e indetectável.

Na hipótese de, por algum fortúnio, não se detiver as chaves, haverá a necessidade de quebrar a criptografia. É nesse ponto que devemos observar o próximo grande passo no que tange à espionagem.

De acordo com documentos fornecidos pelo ex-contratado da NSA, Edward Snowden, o esforço para construir "um computador quântico criptologicamente útil" – uma máquina exponencialmente mais rápida que os computadores clássicos – faz parte de um programa de pesquisa de US$ 79,7 milhões intitulado "Penetrando Alvos Difíceis". Grande parte do trabalho é realizado sob contratos confidenciais em um laboratório em College Park, Maryland (Rich; Gellman, 2014) [26]

A matéria citada foi publicada no do *The Washington Post*, com base nos documentos fornecidos ao jornalista Gellman, onde é afirmado que esse tipo de computador pode descobrir qualquer chave de criptografia. De forma resumida e simplificada, um computador quântico não é como um convencional (dependente da linguagem binária), pois ele trabalha com base em *qubit*, que, ao contrário do *bit* utilizado em máquinas comuns, podem ser zero e um ao mesmo tempo. Assim emerge a possibilidade de "evitar fazer cálculos desnecessários" (Rich; Gellman, 2014). Como muito bem salientou o doutor em ciência da computação Conrado Gouvêa "O poder dos computadores quânticos vem do fenômeno chamado entrelaçamento que ocorre quando se opera com múltiplos *qubits* ao mesmo tempo" (Gouvêa, 2023). Isso significa que métodos, como a famosa força bruta, por exemplo, que testa milhões de combinações uma a uma até encontrar a correta, acontecerá rapidamente, e possibilitará a quebra de praticamente qualquer chave de segurança.

Em adição a tudo isso, é digno de nota outro programa da NSA chamado *Dishfire.* Documentos revelados ao jornal *The Guardian* sugerem a interceptação de pelo menos duzentas milhões de mensagens SMS por dia. Isso pode não parecer muita coisa, mas, a partir dos metadados de cada uma, foi possível extrair diversas informações, dentre elas a "localização, redes de contato e detalhes de cartão de crédito" (Greenwald et al, 2014). Os dados também foram compartilhados com a GCHQ dando acesso a informações sobre viagens realizadas pelo usuário, gestões financeiras e até transações monetárias entre muitos outros dados pessoais.

Diante desse vazamento, o porta voz da NSA deu uma entrevista ao jornal The Guardian e afirmou que "As capacidades da agência foram direcionadas apenas contra "alvos válidos de inteligência estrangeira"[27]" (Greenwald et al, 2014). Resumidamente pode-se dizer que o *Government Communications Headquarters* não tem permissão para pesquisar o conteúdo de mensagens enviadas por cidadãos britânicos sem um mandado, porém, o Dishfire

[25] Com isso não é afirmado categoricamente que a NSA está coletando dados dessas chamadas, mas sim que, como o sinal percorre uma distância maior que a distância entre a localização do planalto e a embaixada americana (veja figura 1), o sinal de celular convencional dos parlamentares estão ao seu alcance para serrem coletados caso assim a embaixada americana deseje.

[26] Do original: According to documents provided by former NSA contractor Edward Snowden, the effort to build "a cryptologically useful quantum computer" — a machine exponentially faster than classical computers — is part of a $79.7 million research program titled "Penetrating Hard Targets." Much of the work is hosted under classified contracts at a laboratory in College Park, Md.

[27] Do original: The agency's capabilities were directed only against "valid foreign intelligence targets" and were subject to stringent legal safeguards, she said.

tem o objetivo de coletar grande volume de SMS, não apenas de alvos específicos, sob o pretexto de que todos podem ser um alvo no futuro. (Greenwald et al, 2014).

Os documentos também afirmam que:

> o Dishfire coleta praticamente tudo o que pode, para que você possa ver o SMS de um seletor que não é direcionado (...) Também é possível pesquisar no conteúdo em massa (por exemplo, por um nome ou número de telefone residencial) se o número do celular do alvo não for conhecido. (...) Os analistas são alertados para serem cuidadosos ao pesquisar conteúdo para termos relacionados a cidadãos do Reino Unido ou pessoas que residem atualmente no Reino Unido, pois essas pesquisas podem ser bem-sucedidas, mas não seriam legais sem um mandado ou autoridade de direcionamento semelhante. (GREENWALD et al, 2014)[28]

No decorrer do documento afirma-se que é permitida a observação de dados de telefones do Reino Unido, contanto que a pesquisa seja a determinado evento, não direcionado a uma pessoa específica. Recomenda-se ao analista que tenha cuidado quando usar o botão do formulário, pois "o banco de dados retornará o conteúdo das mensagens do Reino Unido – o que, sem um mandado, faria com que o analista tivesse acesso "ilegalmente ao conteúdo do SMS" (Greenwald et al, 2014)[29]. Tudo isso demonstra que a coleta é feita, apesar das restrições que envolvem o cidadão britânico, em todo caso, nem mesmo quem reside nesse país pode escapar da coleta, o que poderia ser dito dos brasileiros? O porta-voz do Government Communications Headquarters (GCHQ) afirmou tão somente que a agência não infringe as leis da Inglaterra. Em 2014, ao tomar conhecimento dos fatos, gigantes da telefonia, como a Vodafone manifestaram indignação (Greenwald et al, 2014).

Dado o exposto fica claro que, apesar das agências afirmarem que não quebram as leis de seus países, e que efetuam apenas buscas em dados de inteligência estrangeiros, todo conteúdo está armazenado em algum lugar e pode ser pesquisado com simples utilização de *softwares*. Outro ponto é que poucas coisas ficaram claras com relação a extensão sobre os dados estrangeiros e o que seria considerado um assunto de segurança nacional. Fato é, as mensagens (com localização, dados bancários, dentre outros inúmeros dados) estão disponíveis para pesquisas por agências de difícil fiscalização e isso, por si, só é um risco muito grande para a sociedade e para o Estado. Apesar das declarações defensivas da NSA e do GCHQ, o programa *Dishfire* deve ser observado pelos governos, que não têm acesso a este banco de dados, em sua pior hipótese, ou seja, como um risco à segurança cibernética e um fator desmotivador a utilização de meios que possam ser interceptados por este método que, no mínimo, irá armazenar todas as informações.

Outro caso relevante foi a petição judicial secreta da NSA para coleta de dados em massa de algumas das maiores empresas de telefonia celular. "A ordem, cuja cópia foi obtida pelo Guardian[30], exige que a Verizon forneça à NSA informações sobre todas as chamadas telefônicas em seus sistemas, tanto dentro dos Estados Unidos quanto entre os Estados Unidos e outros países." [31] (Greenwald, 2013). A coleta realizada em massa, independentemente de

---

[28] Do original: "Dishfire collects pretty much everything it can, so you can see SMS from a selector which is not targeted". "It is also possible to search against the content in bulk (e.g. for a name or home telephone number) if the target's mobile phone number is not known." However, a note from GCHQ's operational legalities team, dated May 2008, states agents can search Dishfire for "events" data relating to UK numbers – who is contacting who, and when.

[29] Do original: the database will return the content of the UK messages – which would, without a warrant, cause the analyst to "unlawfully be seeing the content of the SMS"..

[30] Do original: The order, a copy of which has been obtained by the Guardian, requires Verizon on an "ongoing, daily basis" to give the NSA information on all telephone calls in its systems, both within the US and between the US and other countries. A ordem judicial na integra pode ser observada no seguinte link: https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order

[31] A ordem judicial na integra pode ser observada no seguinte link: https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order

haver ou não suspeitos, foi um armazenamento de informações totalmente indiscriminado, incluindo outros dados, como localização de ambos os lados da chamada, inobstante a empresa envolvida. Estava incluso na ordem judicial a proibição da companhia telefônica em vigência de divulgar a existência dessa ordem, mantendo a espionagem em massa oculta da população. Nesse ínterim, James Clapper, diretor de inteligência nacional, que outrora afirmava em pleno Congresso que a NSA não efetuava a garimpagem de milhões de dados americanos, foi "forçado a se desculpar e admitir que sua declaração havia sido "claramente errônea" (Brooke, 2023).

A Verizon não foi a única, a gigante da telefonia AT&T, por meio de outra petição judicial secreta forneceu à NSA acesso "a bilhões de e-mails conforme eles fluíam em seu território doméstico de redes"[32] (Angwin et al, 2015), isso incluía todos os clientes internacionais da AT&T abrangendo até mesmo a rede de comunicações da Organização das Nações Unidas (ONU).

Esse tipo de petição judicial abre diversas dúvidas, dentre elas, os limites de uma corte americana sobre os dados que passam em seu território. Ficou claro, no primeiro capítulo, que boa parte dos cabos submarinos de internet passam pelo território americano e muitos destes são pertencentes a empresas dos Estados Unidos. É importante destacar que, visto as diversas atitudes dúbias acima, onde nem mesmo a privacidade das comunicações da ONU foram respeitadas, haja certa desconfiança quanto a proteção da privacidade atual. Deve-se lembrar que grandes empresas brasileiras de telecomunicações, como a claro, por exemplo, possuem parcerias de *Roaming* de dados com a *Verizon* e com a AT&T (Claro, 2023[33]). Em todo caso, surge certa desconfiança de todo dado que passa pelo "território doméstico de redes" americano.

Ao citar os cabos submarinos, destaca-se o programa XKEYSCORE. Este em 2013 estava conectado diretamente aos cabos de internet em pelo menos 150 pontos do globo, inclusive no Brasil, e conta com mais de 700 servidores que armazenam os dados em um grande banco de dados com possibilidades de filtragem e pesquisa, podendo ter acesso pelos agentes em diversas partes do mundo. Este programa já foi utilizado, inclusive, para "espionar candidatos ao cargo de diretor-geral da Organização Mundial do Comércio e membros do governo das Ilhas Salomão" (Marquis-Boire; Greenwald, 2015). O XKEYCORE, apesar das poucas informações disponíveis sobre ele, é um forte indicador para a desconfiança na privacidade e segurança dos cabos submarinos.

Visto todo esse teatro de espionagem em massa nas redes de telefonia celular é digno de nota que o governo brasileiro e a população de maneira geral precisam estar cientes de que seus dados não estão seguros. O uso da tecnologia é um elemento fundamental do mundo globalizado, contudo aumentou o grau de vulnerabilidade ao qual cada país está exposto.

2.2 Os casos cibernéticos globais e direcionados a governos

O *Boundless Informant* é um sistema computacional que, em tese[34], traz dados relevantes de inteligência de praticamente todos os países do globo, incluindo dados governamentais e militares. O programa visa categorizar registros em metadados de comunicações, projetado para "para dar aos funcionários da NSA respostas a perguntas como: "Que tipo de cobertura temos no país X" e "quase em tempo real, solicitando a infraestrutura

[32] Do original: billions of emails as they have flowed across its domestic networks.
[33] Veja: https://www.claro.com.br/roaming-internacional/estados-unidos-da-america.
[34] Os documentos de Snowden sugerem que o programa também abrange o território americano. O Governo americano negou a acusação de monitorar os próprios cidadãos com esse programa. Esses problemas internos dos EUA não são o foco aqui e são muito controversos. Então trataremos este programa apenas em seu aspecto internacional.

SIGINT [inteligência de sinais]" [35] (The guardian, 2013). Foram coletadas por este programa 97 bilhões de metadados[36], sendo 14 bilhões do Irã. Este é um sistema indiscriminado de recolhimento de registros em massa da internet, que funciona como um *datamining* (nome dado a uma ferramenta de mineração de dados que visa extrair informações relevantes ou valiosas a partir de um imenso conjunto de informações digitais – de maneira simplificada, funciona como um grande filtro – apesar de não se limitar nesta definição) que não deixa de fora nem seus aliados (The guardian, 2013).

Vejamos, por exemplo, o caso da Índia. Os documentos revelados por Snowden sugerem que a agência de segurança nacional americana acessou os computadores da embaixada indiana. Além disso, em "março de 2013, a NSA coletou 6,3 bilhões de informações das redes de internet deste país e 6,2 bilhões de informações de redes telefônicas durante o mesmo período." [37] (Gosh, 2013). Foi utilizado tanto o *Boundless Informant* quanto o PRISM (este será abordado mais a frente), e os dados variaram desde informações não relevantes até categorias designadas como nuclear, espacial, militar e política. A coleta abrangeu até mesmo o escritório de missões da India na ONU, localizado em Nova York e gualdripou "registros de tráfego de Internet, e-mails, telefone e conversas de escritório – incluindo documentos oficiais armazenados digitalmente" (Gosh, 2013).

Nesse contexto é necessário citar os casos voltados a chefes de estado. Vejamos primeiramente o caso envolvendo a Chanceler da Alemanha, Angela Merkel. Em um relatório de inteligência de sinas da NSA foram relatadas interceptações de chamadas de funcionários de altos cargos do governo alemão há décadas, incluindo chamadas pessoais de Merkel, ademais, diversos funcionários, do alto escalão alemão, estavam marcados como alvo de monitoramento de longo prazo, incluindo o chefe de gabinete da chanceler. Nas chamadas divulgadas encontra-se o telefonema de Merkel com o príncipe herdeiro dos Emirados Árabes Unidos para tratar da crise financeira internacional que ocorrera (The guardian, 2015). Outra interceptação relevante foi divulgada pela WikiLeaks, contendo a reunião de assuntos ligados ao meio ambiente e mudanças climáticas, feita entre a chanceler alemã e o secretário-geral da ONU, Ban Ki-Moon (Wikileaks, 2016). O então vice-chanceler alemão elogiou o trabalho dos jornalistas que divulgaram os arquivos disponibilizados por Snowden e, por muito pouco, a Alemanha não o recebeu em asilo político para testemunhar em um inquérito parlamentar na Alemanha para averiguar a atuação da NSA em seu território[38] (Greenwald, 2015).

Em 2013, a chanceler alemã pareceu defender os Estados Unidos mesmo quando soube que a NSA estava realizando coleta de dados em massa dos cidadãos alemães, mas a partir do momento da divulgação de que até suas ligações pessoais eram interceptadas, Merkel "ficou furiosa" (Wright; Kreissl, 2013, p. 13). A chanceler exigiu um acordo de não-espionagem com os Estados Unidos até o final do ano corrente e o fato foi de tamanha magnitude que degradou as relações entre os dois países. Em seguida o presidente Obama afirmou que "seu governo estava conduzindo uma revisão completa das atividades de inteligência" (Wright; Kreissl, 2013, p. 13).

Os documentos não se restringiram a Merkel, apesar da repercussão e reação no caso alemão ter sido mais emblemática, muitos outros estão nessa lista, até mesmo três ex-

[35] Do original: it is designed to give NSA officials answers to questions like, "What type of coverage do we have on country X" in "near real-time by asking the SIGINT [signals intelligence] infrastructure.".
[36] Com este termo refere-se as informações "meta" que informam sobre seus dados indicados.
[37] Do original: In March 2013, the NSA collected 6.3bn pieces of information from internet networks in India and 6.2bn pieces of information from the country's telephone networks during the same period, the Hindu said.
[38] De acordo com a matéria citada, os Estados Unidos ameaçaram cortar a divulgação e dados de inteligência com a Alemanha caso o governo acolhesse Snowden em asilo político.

presidentes da França durante o exercício do poder[39]. Dentre os casos mais emblemáticos, no que tange a inteligência de Sinais e cibernética, podemos citar:

> O Chefe de Gabinete do Alto Comissariado da ONU para Refugiados (ACNUR) para interceptação de longo prazo (...); o Diretor da Divisão de Regras da Organização Mundial do Comércio (OMC), Johann Human, e direcionou seu telefone suíço para interceptação de longo prazo; roubou telegramas diplomáticos italianos sensíveis detalhando como o primeiro-ministro de Israel, Benjamin Netanyahu, implorou ao primeiro-ministro da Itália, Silvio Berlusconi, para ajudar a consertar seu relacionamento com o presidente dos Estados Unidos, Barack Obama, que se recusava a conversar com Netanyahu; interceptou os principais ministros do comércio da UE e do Japão discutindo sua estratégia secreta e linhas vermelhas para impedir que os EUA os "extorquissem" na OMC em Doha (as negociações posteriormente fracassaram); visou explicitamente cinco outros altos funcionários econômicos da UE para interceptação de longo prazo, incluindo seus números de telefone franceses, austríacos e belgas; visou explicitamente os telefones do embaixador da Itália na OTAN e outros altos funcionários italianos para interceptação de longo prazo; e detalhes interceptados de uma reunião privada crítica entre o então presidente francês Nicolas Sarkozy, Merkel e Berluscon, onde este último foi informado de que o sistema bancário italiano estava pronto para "estopar como uma rolha". "(WikiLeaks, 2016)[40]

A abrangência da interceptação telefônica realizada naquele período foi bastante ampla, o Brasil, maior país da América Latina, não ficou de fora. Os documentos da NSA sugerem que a garimpagem de dados envolveu a presidência da república, diversas embaixadas brasileiras e a Petrobras. A presidente Dilma Rousseff afirmou que “Informações empresariais, muitas vezes de alto valor econômico e mesmo estratégico estiveram na mira da espionagem (...) representações brasileiras, dentre elas a missão permanente junto as nações Unidas e a própria presidência” (Rousseff, 2013). Snowden, por meio de uma carta aberta, ofereceu ajuda ao Brasil, no que tange a proteção cibernética e eletrônica em troca de asilo político, mas não foi atendido (Watts, 2013).

Também podemos citar como casos internacionais relevantes o programa PRISM e o *Upstream Collection,* ambos voltados ao campo cibernético. O primeiro possibilita a NSA efetuar coleta de dados em massa da Microsoft, Yahoo, Google, Facebook, Apple e muitos outros. Tal garimpagem incluía e-mails, fotos pessoais, todas as conversas realizadas em chats, chamada de vídeo e áudio, todo histórico de navegação na internet, o acervo de arquivos guardados em nuvem, entre uma vastidão de outros dados (Snowden, 2019.p. 249). Isso significa que praticamente tudo o que um usuário comum acessa ou produz na internet por meio das grandes *Big techs* estava sendo armazenado em um banco de dados pesquisável com um acesso irrestrito a NSA.

O *Upstream Collection*, também é muito evasivo, ele permite:

> A captura rotineira de dados diretamente da infraestrutura de internet do setor privado – os switches e roteadores que desviam o tráfego da internet no mundo todo por meio de satélites em órbita e cabos de fibra ótica de alta capacidade que passam sob o oceano. Essa coleção de dados era administrada pela Unidade de Operações Especiais da NSA, que construiu um equipamento de interceptação telefônica secreta e o embutiu nas instalações

---

[39] Veja: https://g1.globo.com/jornal-nacional/noticia/2015/06/wikileaks-divulga-que-nsa-espionou-ultimos-tres-presidentes-da-franca.html.

[40] Do original: “singled out the Chief of Staff of UN High Commissioner for Refugees (UNHCR) for long term interception targetting his Swiss phone; singled out the Director of the Rules Division of the World Trade Organisation (WTO), Johann Human, and targetted his Swiss phone for long term interception; stole sensitive Italian diplomatic cables detailing how Israel's Prime Minister Benjamin Netanyahu implored Italy's Prime Minister Silvio Berlusconi to help patch up his relationship with US President Barack Obama, who was refusing to talk to Netanyahu; intercepted top EU and Japanese trade ministers discussing their secret strategy and red lines to stop the US "extort[ing]" them at the WTO Doha arounds (the talks subsequently collapsed); explicitly targetted five other top EU economic officials for long term interception, including their French, Austrian and Belgium phone numbers; explicitly targetted the phones of Italy's ambassador to NATO and other top Italian officials for long term interception; and intercepted details of a critical private meeting between then French president Nicolas Sarkozy, Merkel and Berluscon, where the latter was told the Italian banking system was ready to "pop like a cork".

> dos prestativos fornecedores de serviços de internet no mundo todo. Juntos, o PRISM (captura direta dos servidores dos principais provedores de serviços) e o Upstream Collection (captura direta da infraestrutura da internet) garantiam que as informações do mundo, tanto armazenadas quanto em trânsito, fossem monitoradas (Snowden, 2019, p. 250).

O Jornal *The Guardian* teve acesso aos documentos oficiais que falam sobre o programa PRISM e verificou a autenticidade. Estes afirmam que a coleta de dados acontece diretamente dos servidores de provedores de internet. A implicação disto é que provavelmente existe o consentimento das grandes *Big Techs* para o compartilhamento de dados com a NSA. O governo não negou a existência do programa, ao contrário, elaborou leis que restringem seu acesso, enquanto a Microsoft e a Apple negaram o conhecimento de tal garimpagem em seus servidores. Em todo caso, independente de consentimento o PRISM é capaz de capturar as informações de forma unilateral, tanto em tempo real quanto relativo a dados armazenados. O programa contava com um orçamento de 20 milhões de dólares anualmente, voltados para coleta de dados e os documentos afirmam que a viabilidade de sua execução se dá pelo fato de grande parte da internet estar em solo americano. Aparentemente o programa estava baseado na lei 702 de vigilância estrangeira[41] e foi aprovado após alguns debates (Greenwald; Macaskill, 2013). Além disso, este programa também é capaz de organizar os dados gerados pelos outros programas citados neste capítulo, incluindo "gravações de chamadas telefônicas, mensagens de texto, imagens de webcams (...)" (Bauman, 2015).

O PRISM armazena e organiza tudo que foi garimpado pelos mais diversos sistemas de espionagem, além de ser ele mesmo um grande coletador de dados em massa que conta com todo o histórico das *Big Techs* por meio de um registro permanente de dados, o que possibilitava o acesso a quase tudo que já foi feito na internet (Kristiansson, 2023, p. 4). Como não houve informações precisas sobre a coleta de dados da própria população americana, o programa foi muito debatido no senado americano, principalmente com relação a lei 702 que concede permissão da espionagem apenas a estrangeiros[42]. A grande repercussão desse programa gerou respostas em formas de lei (tanto nos EUA quanto na Inglaterra, devido a cooperações entre a NSA e a GCHQ) que serão analisados no próximo capítulo, aqui ressalta-se apenas que seu foco principal é na proteção dos dados de cidadãos nacionais.

Foi demonstrado acima o roubo de chaves de criptografias, a interceptação de chamadas telefônicas convencionais, além da criação de computadores com auto índice de processamento de dados visando a quebra de chaves criptográficas. Ao aliar isso aos dois últimos programas citados perceber-se-á dificuldade de uma conversa ou interação a distância alcançar o status de privada. Tanto o espectro eletromagnético quanto o espaço cibernético são amplamente vulneráveis e a única saída parece ser a não utilização desses meios, algo bastante improvável atualmente.

Sob uma ótica realista das relações internacionais, vivemos em um mundo onde a real confiança na integridade das relações com outros governos é questionável, quanto mais se considerarmos as grandes empresas privadas internacionais que, normalmente, tem o lucro como maior agente governante. Dificilmente o tráfego de voz ou dados será um meio seguro e privado, mesmo se considerarmos os chefes de estado. É nítido que um maior investimento nacional precisa ser feito com relação aos meios de telecomunicação e internet, afinal, o vasto acesso dos programas de vigilância americanos são possíveis porque as grandes *Big Techs* são americanas. O investimento tanto do governo quanto das empresas privadas em um sistema de

---

[41] Veja no site do FBI que essa lei estará em vigência até dezembro de 2023 - https://www.fbi.gov/investigate/how-we-investigate/intelligence/foreign-intelligence-surveillance-act-fisa-and-section-702#:~:text=FISA%20Section%20702%20is%20an,takes%20action%20to%20reauthorize%20it.

[42] O programa PRISM estava em voga no senado em 2016 e o The Guardian fez cobertura do processo. Veja em: https://www.theguardian.com/world/2016/apr/22/james-clapper-nsa-spying-us-data-collection-senate-hearing.

comunicação nacional parece ser a melhor forma para reduzir a coleta de dados. Utilizar telefones chineses e americanos, além de conceder acesso à internet com cabos que, em sua maioria, passam por solo americano, ou são construídos por chineses, não parece ser o meio mais seguro, aliás, apesar das declarações levemente positivas feitas pelas autoridades inglesas e americanas, é pouco provável que a espionagem acabou depois do grande vazamento deste século.

2.3 A importância da espionagem à luz da inteligência estratégica

Por inteligência estratégica entende-se a coleta de dados, cujo interessado é o Estado, e envolve questões que contemplam ameaças ou oportunidades política e estratégica de determinada nação (McDowell, 2009, p. 6). Apesar de sua abrangência e nível elevado, é uma disciplina que observa a realidade de forma "macro", envolve vasta gama de dados, além de possuir implicações com finalidades práticas que reverberam no nível tático e operacional. O diferencial desta para os demais tipos de inteligência é o fim da coleta, que está voltada a assuntos relativos ao interesse de determinada nação (McDowell, 2009, p. 8-9).

A inteligência estratégica é "necessária para a formação da política de defesa nacional e dos planos militares, tanto a nível nacional como internacional" (McDowell, 2009, p.78). A implicação disto é que tal coleta e análise se torna imprescindível, por tratar de um assunto vinculado à sobrevivência do Estado. Evidentemente, é de grande importância para o auxílio à tomada de decisão, pois fornece subsídios necessários para que o agente estatal observe a realidade de maneira coerente e atualizada. Desta forma, não se trata de um assunto marginal ou dispensável, ao contrário, deve ser observado como disciplina de primordial relevância e, consequentemente, seus métodos de aquisição de informação serão de vital importância à nação.

Após breve análise dos programas apresentados acima é possível identificar a estreita relação entre a espionagem da NSA e a produção de inteligência estratégica. Muitos dados podem trazer benefícios econômicos como, por exemplo, as informações de grandes estatais voltadas para o petróleo, como aconteceu com a Petrobras (justamente enquanto estava em voga a extração de alta profundidade do pré-sal). Isso pode ser muito lucrativo, porém, devemos ter um olhar mais amplo e perceber assuntos atinentes a níveis de poder. O levantamento de dados estratégicos assim como descobertas de vulnerabilidades da principal estatal do maior país da américa latina tem, sem sombra de dúvidas, muito valor.

Por se tratar de algo extremamente proveitoso, é difícil mensurar o tamanho da vantagem estratégica proporcionada a uma nação que tenha acesso a conversas particulares de toda uma população, incluindo os chefes de estados de outros países. Conhecer as intenções e posicionamentos de presidentes ou ditadores antes de começar determinado acordo ou relação traz, inequivocamente, vantagens significativas. Em um exercício de história contrafactual, por exemplo, pode-se levantar a hipóteses sobre os estranhos rumos que a história poderia tomar se Adolf Hitler tivesse acesso irrestrito às chamadas entre Roosevelt e Churchill, ou a todos os alinhamentos entre seus generais. Muito além da guerra, a espionagem de comunicações em massa pode proporcionar aos Estados vantagens estratégicas importantes. Assaz não é do objetivo deste artigo versar sobre possibilidades de chantagens e troca de informações sensíveis, acima destas coisas, a espionagem eletrônico-cibernética proporciona informação atualizada de todo o globo, sendo de grande proveito a inteligência estratégica e, consequentemente, fornecendo subsídios valiosíssimos à tomada de decisão.

Veja, por exemplo, o caso de Israel no ataque do Hamas a seu território ocorrido no presente ano de 2023. Alguns analistas enxergam uma grande falha da inteligência israelita na coleta de dados do Hamas que efetuou dezenas de infiltrações em solo israelense em uma grande operação, como afirmou incisivamente Peter Martin (2023): O ataque (...) pode

representar um dos maiores fracassos da inteligência israelense desde a guerra de Yom Kippur". Tanto o exemplo citado da guerra de Yom Kippur quanto o caso atual são casos claros em que a coleta de dados em massa poderia de ser de grande valia. Os exemplos são inúmeros e não caberia neste trabalho citá-los. Ressalta-se apenas que a coleta em massa trás possibilidades para defesa de um país além da imaginação.

Os Estados Unidos e outras potências[43] alcançaram um nível de espionagem tão avançado que todos os cidadãos do mundo, independentemente de sua influência, devem estar cientes da vigilância constante que ocorre a qualquer momento de suas vidas, simplesmente por estarem com seus celulares ligados no bolso. É importante destacar que a união de dados e informações de todos os cidadãos de um país constitui a população nacional e, como é amplamente reconhecido, essa população é um dos pilares do Estado. Um telefonema aparentemente comum, como o de uma dona de casa para sua neta no Natal, não tem relevância internacional por si só, mas quando se considera o conjunto de todas as comunicações efetuadas em um país inteiro, elas se tornam, por razões já mencionadas, elementos cruciais para a produção de informação estratégica. Desde questões culturais até posicionamentos políticos e estratégicos podem ser levantados pelo monitoramento das comunicações de determinado país. Não é necessário elencar os diversos usos que tais dados podem ter[44], mas cabe ressaltar que o acesso irrestrito de dados pessoais em massa ao redor de todo o planeta cria um campo de possibilidades estratégicas bastante amplo a quem possui essa capacidade[45]. É importante enfatizar que todo esse volume de dados resulta em ganhos significativos no que diz respeita à inteligência estratégica. Essa razão, por si só, justifica que os Estados busquem preservar essa capacidade de espionagem. A capacidade de acessar e analisar informações em larga escala deve ser tratada com bastante atenção, não apenas por indivíduos, mas também por governos e organizações internacionais. Sendo relevante equilibrar as questões relacionadas com a segurança dos Estados e a proteção da privacidade e dos direitos individuais.

Do que foi exposto neste capítulo, concluímos que a inteligência de sinais e cibernética, aliada a espionagem resulta em inteligência estratégica em massa, de elevado valor estratégico. Nos casos mencionados, essa inteligência assume uma importância ainda maior, uma vez que abrange as comunicações de uma vasta porção do planeta, incluindo líderes políticos. Não se trata de algo trivial, no qual uma nação que possui essa capacidade simplesmente optaria por abandoná-la ou descartá-la por motivos morais ou éticos. Pelo contrário, essas informações são vitais para orientar a tomada de decisões em âmbito nacional e internacional.

Diante de algo de tamanha importância, surge a pergunta: o que teria peso suficiente no cenário internacional para impedir a prática desse tipo de espionagem? Neste ponto, é fundamental examinar o impacto dessas descobertas nas relações internacionais e a reação do Ocidente diante dessas revelações.

As implicações são profundas. A divulgação de tais práticas de espionagem em larga escala pode abalar consideravelmente as relações entre nações. A confiança mútua, um pilar

---

[43] Outros países possuem programas que "envolvem a colocação de interceptores nos grandes cabos de fibra óptica que ligam os diferentes centros de Internet. No Reino Unido, informações dão conta de que o programa Tempora, do GCHQ1, teria colocado 200 interceptores em cabos que se estendem das ilhas britânicas à Europa Ocidental e aos Estados Unidos. A DGSE2 francesa teria, supostamente, colocado interceptores semelhantes em cabos submarinos fora de sua base militar, no Djibouti. Dentre outras atividades, foi dito que o BND3 alemão interceptou diretamente o maior centro de Internet da Europa, o DE-CIX4, em Frankfurt. O FRA5 sueco grampeou os cabos submarinos que conectam os países bálticos e a Rússia" (Bauman, 2015).

[44] Para bons argumentos sobre a importância da coleta em massa, que serviu de base para minhas afirmações, veja: Kristiansson, Jacob. Digital Surveillance in the name of National Security.

[45] Para bons argumentos sobre a importância da coleta em massa, que serviu de base para minhas afirmações, veja: Kristiansson, Jacob. Digital Surveillance in the name of National Security.

das relações internacionais, pode ser minada quando se descobre que aliados estão realizando espionagem indiscriminada. Países afetados por essas ações podem se sentir violados em sua soberania e privacidade. Além disso, a comunidade internacional pode pressionar por regulamentações mais rígidas e acordos internacionais que limitem a espionagem em larga escala. A diplomacia e o diálogo podem ser afetados, e os países podem buscar formas de se proteger contra essas práticas, o que poderia incluir o desenvolvimento de tecnologias de criptografia mais robustas e medidas de segurança cibernética mais avançadas.

Portanto, as consequências da divulgação de práticas de espionagem em massa são profundas e podem moldar as relações internacionais de maneira significativa, levando a uma revisão das políticas de segurança, privacidade e regulamentação tanto a nível nacional quanto internacional.

CAPÍTULO 3. REAÇÕES E CONSEQUÊNCIAS INTERNACIONAIS

O presente capítulo analisa a reação e as consequências internacionais frente às revelações de Snowden. O foco se dará em expor brevemente as regulações surgidas em consequência dessas revelações. Em primeiro lugar, será tradada a reunião da ONU de 2013 e em seguida os debates surgidos nos Estados Unidos e na Inglaterra. Como o assunto é extremamente extenso, o foco principal neste artigo não será uma exposição exaustiva desses tópicos, mas destacar exclusivamente os aspectos que possuem relevância para o contexto brasileiro.

Para tal, o primeiro tópico está voltado à exposição e breve análise dos debates e ações da ONU no que tange à descoberta da espionagem eletrônico-cibernética em massa. Neste tópico destaca-se a contribuição brasileira e os pontos principais dos avanços no que diz respeito ao direito de privacidade logo após a revelação de Snowden. Os debates realizados no âmbito da ONU são bastante extensos, assim por uma questão de tempo e objetivos deste trabalho optou-se por não realizar uma descrição histórica desta série, priorizando a apresentação dos principais pontos destes debates entre os anos de 2013 e 2020.

O segundo tópico trata das repercussões americanas, inglesas e da União Europeia. Muitos tribunais existiram, muitas propostas de leis e muito debate. Neste capítulo analisaremos apenas as principais regulações. Não será do objetivo deste capítulo esgotar exaustivamente as novas lei americanas e de demais países envolvidos. Tão somente será exposto o suficiente para entendermos o que afeta diretamente o Brasil. Nesse sentido, o foco estará na coleta de dados estrangeiros.

Em primeiro lugar é necessário entender que as assembleias da Organização das Nações Unidas foram "um meio de reconstituir as promessas da política moderna internacional, não só através da proteção da autonomia do indivíduo, mas também através da afirmação da responsabilidade dos Estados em protegê-la". Isso significa que, em tese, para este autor, a ONU deve agir em proveito das autonomias dos indivíduos e colocar nos respectivos Estados o dever de salvaguardar seus próprios cidadãos. Os diversos posicionamentos visíveis, após a coleta de dados em massa, principalmente dos representantes do governo brasileiro, buscaram colocar no Estado a responsabilidade da proteção dos dados de seus cidadãos (Bauman, 2015). Em 2013, a presidente Dilma declarou o desejo de tratados internacionais para reduzir a espionagem em massa e alegou que tomaria medidas internas em nosso país para salvaguardar os brasileiros da coleta de dados, dando ênfase que este seria um assunto de importância fundamental, atrelados aos direitos humanos (Dilma, 2013).

O argumento contra a coleta de dados em massa foi, então, baseado nos direitos humanos e na liberdade de expressão. Em contrapartida, alguns estudiosos americanos parecem argumentar que o direito do Estado a autodefesa pode ser mais valorizado que o direito do cidadão à privacidade, principalmente nos Estados Unidos. Seguindo essa linha de raciocínio a utilização de tecnologias que permitem a coleta em massa de dados pode ser vista como justificável, por se tratar de algo cuja finalidade é beneficiar o próprio cidadão (Kristiansson, 2023).

Neste sentido, podemos expor a problemática da seguinte forma: de um lado temos pensadores que entendem que a salvaguarda do cidadão tem como condição *sine qua non* a coleta de dados em massa, visando a segurança e defesa estatal. De outro, aqueles que afirmam que por se tratar de direitos humanos, o Estado não deveria abdicar dos direitos básicos de seus conterrâneos para protegê-los, se tornando eles mesmo o vilão[46].

O presente trabalho não defenderá um viés específico desta discussão, mas deixará evidente que, para os Estados Unidos, a visão majoritária do Estado é a garantia da segurança e coleta de dados com fins estratégicos, sob o suposto combate ao terrorismo, frente à garantia de privacidade dos estrangeiros. Isso significa, como ficará claro abaixo que não existe paz no espaço cibernético internacional.

3.1. Principais repercussões imediatas na ONU

A descoberta dos documentos expostos por Snowden levaram Navi Pillay, a comissária de direitos humanos nas Nações Unidas, a argumentar fortemente a favor da segurança de privacidade cibernética para defesa dos direitos humanos e a defesa dos que combatem essas atitudes. Ela argumentou que:

> O caso de Snowden mostrou a necessidade de proteger as pessoas que divulgam informações sobre questões que têm implicações para os direitos humanos, bem como a importância de garantir o respeito pelo direito à privacidade (...) O direito à privacidade, o direito de acesso à informação e a liberdade de expressão estão intimamente ligados. O público tem o direito democrático de participar nos assuntos públicos e esse direito não pode ser efetivamente exercido apenas contando com informação autorizada. (Nações Unidas, 2013).

Pillay não assumiu uma posição totalmente contrária à vigilância, ao contrário, ela defendeu que para fins de segurança nacional existem possibilidades legais de vigilância que podem ser realizadas pelos Estados, porém "a vigilância sem salvaguardas adequadas para proteger o direito à privacidade, na verdade, tem o risco de impactar negativamente sobre o desfrute dos direitos humanos e liberdades fundamentais" (Nações Unidas 2023). Nesta declaração é

[46] Kristiansson (2023) faz uma análise de ambos os lados e demonstra quais viéses argumentativos servem para embasar e justificar a cada um.

notório que a opinião da comissária de direitos humanos não é de total restrição da coleta de dados, mas de equilíbrio entre o direito estatal de defender os indivíduos e o dever de respeitar o cidadão. Como o debate, já exposto acima, está centralizado na dicotomia entre segurança nacional e privacidade individual, a declaração de Pilley da busca por um equilíbrio parece ser uma solução, porém, como demonstrou recentemente Jabob Kristiansson (2023), esse equilíbrio encontra sérias dificuldades e o governo americano continua a combater o terrorismo por métodos de vigilância questionáveis.

Outro ponto relevante é que a assembleia geral das Nações Unidas aprovou no final de 2013 uma resolução conjunta, proposta pelo Brasil e pela Alemanha, para salvaguarda dos direitos humanos no que tange à confidencialidade de dados digitais. A ONU instruiu as nações a não medirem esforços para impedirem a prática de atitudes que violem o sigilo digital. A resolução chamada "direito à privacidade na era digital" está preocupada tanto com a coleta de dados no campo cibernético quanto no campo eletromagnético e atrela o direito à privacidade digital com a disciplina dos direitos humanos. Emergiu nessa resolução o fato que as informações digitais são privadas, independentemente de estarem ou não na internet e isso foi um avanço significativo de conceitos no que tange à propriedade digital. Além disso, foi solicitado aos Estados a apresentação de resultados quanto aos avanços no combate à vigilância em massa e que executem inspeções em seus próprios territórios, a fim de impedir agências privadas ou governamentais de realizarem as práticas citadas. Os Estados devem agir de maneira transparente e evidenciar de forma clara quando ocorrer a necessidade de coleta de dados digitais (Nações Unidas, 2013).

Nesse contexto, Pillay levantou uma declaração importante, ao afirmar que o posicionamento das Nações Unidas é condenar as práticas de vigilância em massa como rompimento do "artigo 12 da Declaração Universal dos Direitos Humanos" e do "artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos", onde há forte fundamentação para que "ninguém deverá ter suas correspondências violadas, estar sujeito a interferências na vida privada, familiar ou domiciliar e que todos têm o direito à proteção da lei contra tais interferências ou ataques" (Nações Unidas, 2013). Repare que o posicionamento da ONU visa enquadrar (ou incluir) a privacidade digital no contexto de artigos que versam sobre a privacidade de correspondências, ou seja, como o direito à privacidade pessoal e familiar já era previsto, tal inclusão do campo cibernético, nesta forma de expressão, sugere indiferença entre os dados físicos, eletromagnéticos ou digitais na já prevista salvaguarda da intimidade pessoal.

O "relatório especial sobre a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão" de David Kayne, manifestado em 2014, expôs claramente que a espionagem indiscriminada de vasta quantidade de civis viola o direito à privacidade e é uma afronta aos direitos humanos que precisa ser combatida (United Nations, 2018) [47]. Desta vez foi abordado o assunto de forma direta, de modo muito mais enfático do que na declaração de Pillay, e deixa bem evidente o posicionamento condenatório das Nações Unidas frente ao assunto.

Ainda em 2014, as Nações Unidas promulgaram o "*The right to privacy in the digital age*". Este documento foi originário do debate realizado durante a vigésima-sétima sessão do Conselho de Direitos Humanos da ONU e atrelou formalmente a privacidade digital e o combate a vigilância indiscriminada no meio internacional, as "liberdades fundamentais consagrados na Declaração Universal dos Direitos Humanos e tratados internacionais relevantes de direitos humanos", após a aprovação da assembleia geral de dezoito de dezembro de 2014 (United Nations, 2014). Neste documento foi reiterada a responsabilidade das nações em:

[47] O relatório está em árabe, porém, a versão em inglês pode ser adquirida no mesmo link através do hiperlink disponível nesta página das Nações Unidas: "Access English: A_HRC_38_35-EM PDF".

> Discutir e analisar, com base no direito internacional dos direitos humanos, questões relacionadas com a promoção e proteção do direito à privacidade na era digital, salvaguardas processuais, supervisão e soluções internas eficazes, o impacto da vigilância sobre o direito à privacidade e outros direitos humanos , bem como a necessidade de examinar os princípios da não arbitrariedade e da legalidade, e a relevância das avaliações de necessidade e proporcionalidade em relação às práticas de vigilância. (United Nations, 2014 tradução nossa[48])

Além desta, uma nova resolução aprovada em dezembro de 2020, de mesmo título (*The right to privacy in the digital age)*, incrementa a anterior e adiciona novos avanços como a questão da intimidade digital ao incluir no combate à vigilância ~~a~~ fatos relacionados aos abusos sexuais de mulheres ou crianças e a utilização ilegal de suas imagens (além de adicionar outros assuntos, como o *cyberbulling*, que fogem do escopo deste trabalho) (United Nations, 2020). Tal evolução demostra que aquilo que foi iniciado com a descoberta dos documentos expostos por Snowden~~,~~ segue em progresso para os futuros aperfeiçoamentos necessários, além de expor que a existência de atualizações para abranger assuntos mais recentes e contemporâneos no debate internacional, como é o caso, por exemplo, das questões que envolvem a importância da privacidade no combate ao *cyberstalking*[49] (United Nations, 2020). É possível afirmar que o ano de 2013 marcou o início de uma nova era no que tange à percepção da necessidade de se debater, no cenário internacional, a favor da privacidade, a consequente liberdade de expressão e de direitos humanos no espaço eletrônico-cibernético. Com relação aos tempos de guerra, as Nações Unidas debateram sobre a possibilidade de coleta de dados nesses períodos. Esses debates geraram a resolução 2277 de 2016 que afirma a possibilidade de coleta de dados no campo eletrônico-cibernético em conflitos armados, e versa sobre a importância da salvaguarda dos dados civis (United Nations, 2016).

Dado o exposto neste tópico, fica notório o importante papel da ONU nesta problemática em salvaguardar os direitos humanos, aumentar a conscientização estatal sobre a relevância da transparência dos governos no que tange a sua coleta de dados e levantar debates mais extensos com relação ao campo eletrônico-cibernético. Ademais, dar maior visibilidade no cenário internacional a essas questões. Existem muitos pontos positivos, mas seriam eles satisfatórios para a resolução da questão?

É difícil dizer se essas medidas foram verdadeiramente eficazes para acabar de vez com a coleta em massa, principalmente quando se trata de potências como os Estados Unidos. Como relatado pelo jornal O Globo, o então presidente Obama, pouco tempo após a reunião da ONU citada no início deste tópico, afirmou "em um discurso de bonitas palavras, mas de poucas medidas práticas (...) que os serviços secretos americanos não vão mais espionar amigos e aliados, mas sem mencionar quais as garantias" (2014), além disso, Obama "deixou claro que vai continuar monitorando os governos de outros países (...) e negou um pedido de desculpas" (O GLOBO, 2014). Novamente, é necessário refletir sobre a real eficácia das ações da ONU para frear as atitudes americanas, principalmente, quando este país está lidando com um assunto que julga indispensável a sua segurança. Como isso, não se levanta aqui uma crítica às Nações Unidas em si (que, como visto acima, tomou medidas a favor dos direitos humanos) mas sim evidenciando a característica anárquica do sistema internacional. Para melhor esclarecimento, observemos as consequências no cenário americano e europeu.

---

[48] Do original: Discuss and analyse, based on international human rights law, issues relating to the promotion and protection of the right to privacy in the digital age, procedural safeguards, effective domestic oversight and remedies, the impact of surveillance on the right to privacy and other human rights, as well as the need to examine the principles of non-arbitrariness and lawfulness, and the relevance of necessity and proportionality assessments in relation to surveillance practices..

[49] O termo se refere ao padrão de comportamento digital caracterizado por repetições diversas e intencionais, que visam o assédio (de todo tipo) ou perseguição.

3.2 Repercussões americanas e europeias

A divulgação dos documentos da NSA por Snowden teve aparentes consequências à capacidade americana de efetuar busca de dados, dentre elas, ressalta-se a mudança de localização dos grandes bancos de informação em nuvem. O ponto em questão é que o simples fato de haver dados armazenados em solo americano se tornou fator de desconfiança para os usuários, assim, os grandes clientes de dados (organizações) passaram a optar por armazenadores de nuvens que estivessem fora dos Estados Unidos. Um bom exemplo disso é o Dropbox e o Twitter que transferiram toda a sua base de dados para a Irlanda (a exceção das contas dos cidadãos americanos). Isso deu início a uma transação geopolítica no que tange ao domínio dos dados, passando parte significativa dos sistemas de nuvens para Europa (Irion, 2015).

Pode-se dizer que boa parcela desta migração é devido à política de sigilo de dados dada ao cidadão europeu que fornece relativa proteção ao território (Irion, 2015). Transparece-se, então, que a busca pela privacidade fez emergir um novo polo de armazenamento de dados, que visa reduzir a probabilidade de atitudes aparentemente arbitrárias, como os mandados judiciais secretos já mencionados anteriormente, entre outros. Cabe ressalta que esse movimento aproximou os bancos de dados da agência inglesa *Government Communications Headquarters* (GCHQ).

Com relação ao Reino Unido os políticos debateram vigorosamente sobre o "Communications Data Bill, uma lei que exigiria que ISPs e provedores de telecomunicações mantivessem registros de metadados por apenas 12 meses" (Laudau, 2013), mas foi somente em 2016 que a proposta de mudança veio com certa substância (entrou em vigor em 2018) ao com a *Regulation EU 2016/679 of the European Parllament.* Este regulamento "protege os indivíduos quando seus dados estão sendo processados pelo setor privado e pela maior parte do setor público" (EUR-Lex, 2022). Essa regulação trata de uma variedade normativa, sobre as empresas atuantes na União Europeia (ainda que sediadas no exterior), que objetivam a proteção dos direitos humanos na salvaguarda dos dados pessoais, contanto que essa salvaguarda não atrapalhe a luta contra o terrorismo (Consilium EU, 2023).

Sendo um pouco mais específico, devemos perguntar se um estrangeiro pode se sentir tão seguro quanto os nacionais da UE ou dos EUA. Veja, por exemplo, a conhecida frase do ex-presidente americano, ao se dirigir aos cidadãos de seu país. Obama afirma que "os sistemas de vigilância não significam que os telefonemas dos cidadãos são ouvidos"[50]. Essa declaração não significa muita coisa, ainda mais se percebermos que o problema não é alguém estar ouvindo os telefonemas, afinal, dificilmente o governo terá capacidade para dispor agentes ouvindo as ligações de milhões de pessoas. O problema é o armazenamento e análise de dados em massa. Contra isso não foram encontrados muitos impedimentos. Ademais, em 2015, dois anos depois da divulgação dos casos citados, até mesmo os próprios cidadãos americanos enfrentavam a desconfiança da vigilância, como asseverou Castro e Mcquinn (2015) "os decisores políticos dos EUA não conseguiram tomar medidas suficientes para resolver estas preocupações de vigilância". A falta de respeito à privacidade de seus próprios conterrâneos gera dúvidas quanto a vontade de proteger aqueles que não habitam na região.

Outra questão são as próprias empresas de tecnologia. Não parece interessante às gigantes da internet que seus usuários não se sintam seguros ao acessar seus serviços. Como boa parte dos escândalos envolveram as próprias *Big Techs*, devemos refletir sobre como isso poderia afetar os seus negócios. Muitas dessas empresas, como a Apple, Facebook, Google, Microsoft entre outras elaboraram um manifesto intitulado *Global Government Surveillance*

[50] Fonte: https://g1.globo.com/mundo/noticia/2013/08/obama-vai-pedir-ao-congresso-mudancas-no-ato-patriota.html.

Reform coalition, no qual "insta os governos de todo o mundo a adotarem leis e práticas de vigilância que sejam consistentes com as normas estabelecidas de privacidade, liberdade de expressão e Estado de direito" (Reform government surveillance, 2013).

A competitividade americana se tornou menor no cenário internacional, pois os outros agentes estatais se aproveitaram de toda essa problemática para, através da propaganda antiamericana e investimento em sistemas supostamente seguros, trazer os clientes para suas empresas de dados. Em 2015, estudiosos imaginavam que em curto prazo, as empresas americanas perderiam capital e a tendência seria que no longo prazo os concorrentes criassem medidas protecionistas que restringissem a atitude americana (Castro; Mcquinn, 2015).

Os ingleses também saíram prejudicados. Ao observar os britânicos, Owen Bowncott asseverou que um tribunal inglês que investigou a vigilância global na internet concluiu que os serviços de inteligência da Inglaterra estão construindo um gigantesco banco de dados, com informações coletadas em massa na internet, através do programa Tempora[51], onde há grande probabilidade de troca de dados com o PRISM. A preocupação principal deste tribunal é a vigilância do cidadão inglês, que estava sendo executada por ambos os programas, o que seria contra a constituição da Inglaterra (Bowncott, 2014). Perceba que o assunto em voga nos tribunais ingleses e americanos, particularmente, é a proibição da espionagem interna irrestrita. Os dados estrangeiros tiveram pouca importância. O movimento é pela salvaguarda de seus próprios cidadãos. Algumas raras falas, como a de Obama: "para os outros em todo o mundo, quero deixar claro, mais uma vez, que os Estados Unidos não estão interessados em espionar as pessoas comuns" [52,] podem intuir certa disposição do governo americano em deixar os dados pessoais de fora de suas buscas. Porém, mais uma vez a expressão é dúbia e não acarreta conclusões relevantes ao fato em questão, pois, como já dito, o problema é o armazenamento em massa. A problemática em questão envolve sistemas de filtragem e produção envolvendo populações inteiras, oferecer disponibilidade de dados pessoais ao alcance de um simples clicar de um botão.

Visto tamanha repercussão dos documentos vazados, principalmente com relação ao PRISM (por envolver redes sociais com bilhões de usuários), em 2015, finalmente, foi aprovado no senado e assinado por Obama o *USA Freedom Act*. Esta é uma lei que visa restringir o acesso à informação das agências de inteligência sem mandados ou motivos ~~o~~ suficientes. Ela proíbe expressamente a "coleta indiscriminada em grande escala, como todos os registros de um Estado, cidade ou código postal inteiro" [53] (Judiciary Committee, 2015). Desta forma, a lei tenta garantir que a coleta em massa, tendo completudes estatais como alvo, não ocorrerá, salvo motivos de segurança nacional. Porém, vale ressaltar que esse tipo de proibição é uma restrição, não um fim ao programa, além disso, muito pouco é informado sobre os critérios para que algo seja considerado relevante ao ponto de ser investigado, nem sobre os dados estrangeiros.

Bauman (2015) sugere que para cada alvo em potencial de terrorismo, é possível que mais de dois milhões e meio de pessoas tenham seus dados coletados e analisados. Apesar da objetivação geral do programa visar o combate ao terrorismo, aparentemente, ele vai muito além. Nathan Oliveira parece concordar com isso e afirma: "Podemos observar que os EUA se utilizam da vigilância como um recurso de poder para obter informações e ganhar vantagem (...) são capazes de mapear informações cruciais sobre recursos estratégicos de

---

[51] Este programa conta com a interceptação, por parte da GCHQ, aos cabos de fibra ótica para acesso à internet trafegada no mudo inteiro. Veja: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

[52] Fonte: https://g1.globo.com/mundo/noticia/2013/08/obama-vai-pedir-ao-congresso-mudancas-no-ato-patriota.html.

[53] Do original: prohibiting large-scale, indiscriminate collection, such as all records from an entire state, city, or zip code.

potências econômicas" (2020). Dizer que será vigiado somente o que for relevante ao país não resolve o problema, como também traz sérias dúvidas sobre sua abrangência. Em 2018 foi aprovado novamente tanto o PRISM quanto o *Upstream Collection* a despeito da imposição de restrições e da mudança de foco em direção aos coleta de dados relevantes à inteligência estrangeira (Hautela, 2018). É fácil perceber que esses programas não são algo que uma nação simplesmente desliga e pede desculpas, como ressaltou Jacob Kristiansson, eles são vitais e "garantiram a segurança nacional" (2023. p.25).

De acordo com as informações apresentadas, é possível afirmar que a NSA ainda consegue coletar dados de pessoas que não estão diretamente ligadas a atos descritos como terroristas. Desde que sejam consideradas "relevantes" para a investigação podem ser monitoradas, mas não foi divulgada nenhuma diretriz específica sobre como determinar quem é "relevante" para uma investigação. A ausência de critérios objetivos faz como que esse processo de produção de informação estratégica não encontre muitos limites quando efetuado para além das fronteiras nacionais.

No início de 2023 foi feito um acordo de privacidade de dados entre Estados Unidos e União europeia onde, em tese, o tráfego de informações virtuais entre as duas regiões seguirá o Regulamento Geral de Proteção de Dados (GDPR sigla em inglês). Esta atitude é uma consequência do assunto tratado pelo Tribunal de Justiça da União Europeia no processo Schrems II (esse tribunal questionou a transferência ilegal de dados pessoais da UE para os EUA revelados por Snowden). Devido à espionagem ocorrida, o tratado de transferência de dados intitulado *Privacy Shield* havia sido anulado e, desde então, muito debate ocorreu, até que finalmente, em 2023 foi realizado o acordo supracitado unindo essas duas regiões no campo cibernético novamente (Reform government surveillance, 2023).

O tratado da UE estabelece normas para proteção pessoal de pessoas singulares, no que diz respeito a seus dados privados e proteção nas transferências de informações pessoais para países terceiros, inclusive no que tange os fins comerciais (InfoCuria, 2020). Esse foi um importante passo no que tange à privacidade, mas esse tipo de proteção é dada somente aos seus nacionais, salvo casos específicos (InfoCuria, 2020). Outro ponto relevante é que a coleta, como já mencionado, infringia leis internacionais e internas. Não foi criado um meio "físico" de restrição, mas normativo, que (logicamente) pode ou não ser cumprido. Não foram encontradas por essa pesquisa interferências na capacidade ontologicamente, mas apenas as citadas restrições legais que não são plenamente impeditivas.

Em palavras que demonstram os supostos danos da divulgação de Snowden a NSA, Michael Hayden, ex-diretor da NSA e da CIA e John Bolton, ex-conselheiro de segurança nacional, foram a público e manifestaram indignação:

> Michael Hayden (...), diz: "Foi muito ruim para os Estados Unidos. Nós espiamos. OK. Isso é o que fazemos." A NSA, acrescentou, "perdeu muito acervo", por causa de Snowden. "Não é uma solução. É um problema". Questionado se Snowden deveria voltar para casa e ser perdoado, Hayden responde: "Deus, não. Ele foi para Hong Kong e depois foi para a Rússia. O que você acha disso? Isso diz muito sobre ele, eu acho" (...). John Bolton (...) diz: "Esse tipo de vazamento pode ter um enorme impacto negativo, não apenas em questões de defesa, mas também em questões diplomáticas[54] (The guardian, 2023).

De fato, apesar de não ter sido possível atingir o completo fim da vigilância, a espionagem americana e inglesa não saiu de graça, principalmente no contexto dos EUA.

[54] Do original: Michael Hayden (…) says: "It was very bad for the United States. We spy. OK. That's what we do." The NSA, he added, "lost a lot of collection", because of Snowden. "It's not a solution. It's a problem." Asked if Snowden should be allowed to return home and be pardoned, Hayden replies: "God, no. He went to Hong Kong and then went to Russia. What do you think about that? It tells you a lot about him, I think." John Bolton, a former national security adviser, adds: "That kind of leak can have a huge negative impact, not just on defence issues but on diplomatic issues as well.

Problemas com a Alemanha, desgaste internacional e novas leis de agências reguladoras como a União Europeia e a ONU causaram restrição a coleta de dados em massa. A migração dos bancos de dados de nuvem para Europa parece ser um dificultador na busca de informações, e ocasionador de perdas econômicas, ainda mais ao considerarmos a nova lei já citada de 2023. Porém, devemos ressaltar que o maior golpe em suas capacidades não foi no meio físico, mas mental. Com "mental" refere-se os cidadãos ontologicamente, que passaram a ter maior clareza de pensamentos e perceber a existência inevitável da coleta de dados. A partir do momento que os cidadãos passaram a não utilizar nuvens que estão sediadas nos EUA, ocorreu grande migração para a Europa. O exposto acima demonstra que a atitude populacional trouxe severas consequências a facilidade de busca de informações, uma verdadeira mudança na geopolítica de dados. O serviço de vigilância sofre severas perdas quando o cidadão sabe que está sendo vigiado e passa a tomar mais cuidado em sua utilização da internet e das nuvens.

Porém, não se deve entender que dificuldades à coleta e questões vinculadas ao lucro empresarial sejam um marco de total segurança cibernética. Devemos lembrar que a espionagem em massa é um assunto relacionado ao poder e ao auxílio à tomada de decisão. Não se trata de algo simples ou dispensável. Como asseverou Snowden e, logo depois, Greenwald:

> O governo dos EUA ainda está espionando de maneiras que são, em alguns casos, piores ou mais extremas do que conseguimos revelar na reportagem de Snowden. A tecnologia melhorou e uma das coisas que o estado de segurança dos EUA é especialista em fazer, e tem feito desde que foi criado no final da Segunda Guerra Mundial, é garantir que os americanos tenham sempre um novo inimigo a temer e tenham sempre uma razão para acreditar que é necessário que o governo seja capaz de operar em segredo e espionar e tenha poderes ilimitados[55]. (The guardian, 2023).

Após o vazamento, no Reino Unido aconteceram três análises de atitudes governamentais que podemos elencar como principais. Uma pela Comissão de Inteligência e Segurança do parlamento inglês, em que quase nada foi realizado no que tange a expor as reais intenções da coleta de dados em massa. Outra foi feita por um revisor independente de legislação sobre o terrorismo, chamado David Anderson, que sugeriu uma série de melhorias no que tange à privacidade de dados, onde muitas foram atendidas pelo governo. A terceira foi feita pelo Ministério do Interior que convocou uma reunião (com agentes de segurança e até mesmo jornalistas) onde foi feita a análise do caso e produzidas diversas recomendações. Tais relatórios em conjunto foram basilares para a regulação citada de 2016 que estabeleceu os tipos de coleta permitidos. O problema foi que apesar da alteração que rege a maneira pela qual a interceptação era autorizada, ela não proibiu efetivamente a coleta em massa (Brooke, 2023).

Pode-se dizer, de maneira resumida, que os debates voltados para a relação entre direitos humanos e privacidade de dados cibernéticos na União Europeia e na Inglaterra estabeleceram um precedente em toda a Europa em que a coleta de dados em massa precisa ser mais transparente e sob regulações judiciais. Isso fez com que em 2023 as atitudes de coleta do MI5, descobertas recentemente, fossem consideradas ilegais pelo *Investigatory Powers Tribunal*. Tudo isso só foi possível por causa das revelações de Snowden, porém, tais restrições não são, de forma alguma, o fim da espionagem eletrônico-cibernética em massa (Brooke, 2023).

---

[55] Do original: The US government is still spying in ways that are in some instances worse than or more extreme than what we were able to reveal in the Snowden reporting. "The technology has improved and one of the things that the US security state is expert at doing, and has been since it was created at the end of world war two, is ensuring that Americans always have a new enemy to fear and always have a reason to believe that it's necessary the government be able to operate in secret and spy and have unlimited powers.

> À medida que a tecnologia evolui, a vigilância também evolui. Os Estados encontraram novas formas de espionar os cidadãos, especialmente através dos telemóveis que todos transportamos. Spywares intrusivos como o Pegasus, vendido pela empresa de vigilância israelense NSO Group, podem transformar o telefone de uma pessoa em uma máquina de vigilância 24 horas por dia [56]. (Brooke, 2023).

Ao que parece, boa parte da vigilância on-line continua e de forma ainda mais aberta, através das grandes empresas de tecnologia (Brooke, 2023). Os termos de serviço do Google já citados neste trabalho falam claramente da coleta de dados. Apesar disso, devemos perceber que uma coisa é a empresa afirmar que irá coletar os seus dados sem nenhum tipo de transparência absoluta sobre o que será feito com eles, em uma relação com um usuário que escolheu voluntariamente que seus dados pessoais ficassem nessa situação (mesmo se alguém não ler os termos de serviço dos aplicativos, pode-se dizer que não ler é uma opção voluntária). Outra, totalmente diferente, é a coleta indiscriminada em que não houve, pelo menos indiretamente, algum tipo de aceitação. Aparentemente, é uma situação melhor do que a anterior. Em todo caso, isso é um assunto que nos faz refletir o quanto a população, apesar de estar um pouco mais ciente dos riscos de vazamentos de dados, continua a consumir e utilizar essas plataformas.

Os Estados Unidos e a Inglaterra não são os únicos países a efetuar espionagem cibernética, ao contrário, por vezes são vítimas. Os exemplos são inúmeros, destaca-se aqui apenas que a China, através do *Volt Typhoon*, realizou coleta de dados em massa na ilha de Guam (ilha do pacífico, pertencente aos EUA, com forte potencial turístico) e adquiriu informações secretas de pelo menos três bases militares americanas. A investida chinesa nesta ilha, próxima de Taiwan, além de adquirir informações sensíveis, visava "interromper a infraestrutura crítica de comunicação entre os Estados Unidos e a região da Ásia durante crises futuras". Vasta gama de informação foi coletada, o que inclui pessoas comuns, de setores de educação, comunicações e transporte (Veja, 2023).

Assim, destaca-se que as revelações de Snowden têm grande valia para a população (sem efetuar algum tipo de juízo de valor sobre sua pessoa), pois, independentemente de quem esteja efetuando a coleta de dados, quando o cidadão é mais consciente dos riscos da internet, ele poderá tomar mais cuidado com seus próprios dados. Além disso, o caso chinês demonstra que não se trata de um assunto marginal. É de conhecimento geral os problemas envolvendo Taiwan, China e Estados Unidos. Ao interpretar os fatos deste assunto expostos acima, é possível perceber que com bases militares americanas tão perto de Taiwan os chineses, aparentemente, buscaram informações importantes para sua tomada de decisão (efetuando inteligência estratégica), além da tentativa de corte citada. A privacidade de dados de um cidadão comum, como um professor do maternal, por exemplo, não parece, a luz de tudo o que já foi dito, ser um fator impeditivo para um país como a China, com uma possível guerra como pauta em questão.

O fato chinês torna-se importante para demonstrar como este mundo, dotado de relações internacionais anárquicas, é marcado por uma atitude de prevenção, que busca estar cada vez mais preparado para o conflito. E o que poderia ser tão valioso quanto a coleta de dados em massa de governos e populações inteiras? A atitude chinesa e americana não parece ser ontologicamente diferente, ao estar frente a um possível conflito escolheu-se recorrer a coleta de dados em massa. O que poderia ser forte o suficiente, dentro do cenário internacional, para impedir que um país efetue aquilo que ele julga vital à sua segurança? O

[56] Do original: As technology evolves, so too does surveillance. States have found new ways to spy on citizens, particularly using the mobile phones we all carry around. Intrusive spyware such as Pegasus, sold by the Israeli surveillance company NSO Group, can turn a person's phone into a 24-hour surveillance machine.

mundo anárquico parece ter como consequência a busca por informações relevantes e isso dificilmente corroborará com os direitos humanos e direito à privacidade.

Dado o exposto em todo esse tópico, fica nítido que, apesar das novas regulações, tratados internacionais e ações voltadas para os direitos humanos, o estrangeiro (cidadão não americano, como os brasileiros) não possui aparatos suficientes para ter certeza absoluta da confidencialidade de seus dados. Pior se torna a questão, se levar em consideração que as agências de espionagem, como já citado, ignoraram a própria constituição vigente em seus países e armazenaram dados nacionais. Nesse contexto é normal que surjam desconfianças, ainda mais quando dificilmente exista alguma consequência forte o bastante no cenário internacional para frear a espionagem. Ademais, é necessário perceber que os Estados Unidos não são os únicos interessados em realizar inteligência estratégica por meio da coleta em massa. Países como Inglaterra e China parecem estar bastante envolvidos com esse ramo.

CAPÍTULO 4. O BRASIL PÓS SNOWDEN

O discurso de Dilma na ONU teve grande repercussão na mídia internacional (The guardian, 2013). Petições para tratados internacionais e promessas com relação às futuras atitudes de seu próprio país foram feitas (conforme será descrito abaixo). De fato, foi um discurso necessário em um contexto em que a própria presidente havia sido vítima de espionagem. Agora, uma década após esse discurso, é possível avaliar de forma mais abrangente o real impacto da inteligência estratégica americana e a atual situação da população brasileira em relação à proteção da privacidade digital. Nesse contexto, examinaremos de que maneira o Brasil reagiu a esses desafios e quais foram os resultados e avanços no que concerne às políticas públicas destinadas a salvaguardar a privacidade digital.

Este capítulo debaterá sobre as mudanças ocorridas nas políticas públicas do Brasil após a divulgação da espionagem em massa revelada por Edward Snowden. Inicialmente, no primeiro tópico, serão tratadas as leis brasileiras referentes à proteção cibernética que estavam em vigor antes dos documentos apresentados por Edward Snowden. Neste, será analisado se a legislação oferecia uma base adequada para a defesa da privacidade no meio digital. O enfoque principal estará na famosa "lei de acesso à informação" (lei 12.527 de 18 de novembro de 2011) e lei contra invasão de dispositivo informático (lei n. 12.737/2012). O objetivo geral deste tópico não é mostrar exaustivamente as referidas leis, mas tornar evidente a existência (ou ausência) de robustez legislatória para garantia da privacidade cibernética.

O segundo tópico versa sobre as atitudes do governo efetuadas após 2013 para a tentativa de garantir a salvaguarda dos dados pessoais e governamentais. Aqui é debatido as novas regulações, principalmente o marco civil da internet (lei n. 12.965/2014) e a lei de proteção de dados (Lei nº 13.709/2018). Ademais trata-se da Comissão parlamentar de inquérito (CPI) sobre a espionagem, da principal cartilha do Senado Federal sobre o assunto (intitulada rede vulnerável), a questão tentativa, de redução da dependência dos Estados Unidos, no que tange aos cabos submarinos e a conscientização populacional com relação a coleta de dados em massa.

4.1 A privacidade digital no Brasil antes de 2013

Precedente às revelações de Edward Snowden, o Brasil, em 2011, havia promulgado a Lei de Acesso à Informação. Esta legislação estabeleceu um conjunto de diretrizes focadas, principalmente, em facilitar o acesso da população à informação governamental. Além disso, esta lei promove transparência na divulgação de dados pelo governo (Brasil, 2011). No decorrer deste texto legislativo, pouco é encontrado sobre o sigilo dos produtores de dados ou das informações pessoais dos usuários da internet, porém, é possível encontrar algumas definições úteis, como a de "informação privada" e versa brevemente sobre o sigilo de dados (Brasil, 2011). Trata-se, então, de aspectos basilares, ou iniciais, que são um ponto de partida potencialmente relevante para o desenvolvimento futuro desta área. No entanto, é relevante destacar que esta legislação, por si só, se mostra insuficiente para assegurar a proteção da privacidade dos dados.

Esta lei é importante quando vista sob a ótica da democracia. Um país democrático necessita que seus cidadãos tenham condições para decidirem sobre o futuro de seu país e o acesso à informação é condição necessária para tal (Ayuda, 2012). Além disso:

> A Lei de Acesso à Informação determina que o tratamento das informações pessoais detidas por entidades e instituições nela abrangidas seja realizado de modo transparente, respeitando o direito fundamental à proteção da intimidade, da vida privada, da honra e da imagem das pessoas, o que, nos fundamentos defendidos nesta pesquisa, corresponde à proteção do direito fundamental à privacidade (Boff; Fortes, 2016, p.17).

Apesar destes pontos positivos é necessário entender, como dito acima, que o foco em questão desta lei não é a proteção cibernética. Assim, não há robustez no que tange esse campo, de forma que não seja suficiente por si só.

Outra norma jurídica pré-Snowden é a lei 12.737/2012 que versa sobre a "Invasão de dispositivo informático". Seu Art 155-A é sancionado com pena de 3 meses a um ano, contra "Invadir dispositivo informático alheio (...) com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo" (BRASIL, 2012).

A lei está voltada para o ataque cibernético em si e, apesar de seus pontos positivos, possui algumas coisas não justificadas que dificultam sua aplicação, como asseverou Fortes (2016):

> Depreende-se do diploma legal, que tutela os crimes informáticos, a preocupação do legislador em conferir maior proteção na seara penal aos dados, estendendo a compreensão do crime de invasão de dispositivo informático à obtenção, à adulteração, ou à destruição de dados e informações do titular do dispositivo, sem seu consentimento expresso ou tácito. Contudo, o legislador imprimiu à Lei de Crimes Informáticos uma economia textual desnecessária, não expressando questões relacionadas aos conceitos e às definições fundamentais para a aplicação da norma (p.17. 2016).

Ademais, fato importante a ser mencionado é que a espionagem eletrônico-cibernética, conforme já explanado no capítulo 1, não tem como fator *sine qua non* a invasão de computadores ou telefones celulares em solo brasileiro. Além disso, a maioria dos grandes bancos de dados, como visto acima, não estão em território nacional. Essas leis são importantes para garantia da segurança frente ao ataque cibernético, caracterizado por invasões. Porém, tem resoluções focadas em roubo de dados de forma pessoal e direcionada, sem abranger a espionagem em massa. Destaca-se que, no que tange aos crimes cibernéticos, a lei possui apenas 2 artigos, o 154-A (citado acima) e o 154-B, que versa sobre as procedências e imputações penais do artigo anterior.

Nesse contexto, é relevante sublinhar que a amplitude dessa legislação se revela limitada no que diz respeito à prevenção da espionagem em larga escala, sobretudo quando levamos em consideração o meio eletromagnético, cuja obtenção de informação não precisa de nenhum tipo de invasão (como já demonstrado nos conceitos básicos de Inteligência de sinais).

Torna-se perceptível que as legislações existentes no Brasil, com foco no campo cibernético, vigente antes de 2013, carece de um arcabouço adequado para fazer frente às atividades de coleta de dados em massa, seja efetuada pelo governo nacional ou por estrangeiros.

4.2 Políticas públicas pós Snowden

Após as revelações de Snowden a primeira reação visível do governo brasileiro foi o acalorado discurso da ex-presidente Dilma citado acima. As repreensões da então presidente e suas promessas para um novo sistema de internet para o Brasil tiveram grande repercussão:

> Dilma também ordenou que seu governo tome medidas, incluindo a instalação de linhas de fibra óptica diretamente para a Europa e nações sul-americanas em um esforço para "separar" o Brasil da espinha dorsal da Internet centrada nos EUA, que especialistas dizem ter facilitado a espionagem da NSA (The guardian, 2013).

Além destas medidas, houve diversas outras "promessas" para preservar a privacidade do cidadão brasileiro, tais como, preservar a neutralidade de rede a qual garante que os provedores de internet cobrariam o mesmo valor para a taxa de dados, sem diferenciações (o que corroboraria para que o usuário pudesse utilizar os serviços on-line sem distinções

monetárias), criação de um e-mail estatal mais difícil de ser invadido e desenvolvimento de tecnologias que protejam os usuários da internet. (The guardian, 2013).

Algumas dessas propostas foram relativamente cumpridas e outras não, caberá abaixo uma análise das principais ações governamentais no que tange às políticas públicas brasileiras frente à ameaça cibernética. O objetivo desta análise é fornecer elementos que nos auxiliem a explicar como o Estado brasileiro tem buscado fortalecer sua segurança cibernética tanto no nível interno quanto em suas relações com outros Estados. Nesse sentido, não faz parte do escopo deste trabalho a análise das políticas públicas para o setor cibernético. Principalmente, porque esse tipo de avaliação requer metodologia própria o que foge aos objetivos desta pesquisa. Assim, efetuou-se uma exploratória das principais legislações do Brasil criadas para regular esse setor.

Com relação à regulação, como fator relevante levanta-se o Marco Civil da Internet (Lei n. 12.965/2014). Antes dele "o acesso aos dados e o registro da conduta de seus usuários eram plenamente destituídos de regulação específica, o que também permitiu que a internet se tornasse um ambiente hostil e de cometimento de abusos e violações de direitos" (Boff; Fortes, 2016, p.18). Assim, o Marco Civil emerge de importância.

Seu âmago versa sobre os "direitos e deveres para o uso da internet no Brasil" e delimita os limites para a atuação na internet do governo federal, estadual e municipal (Art.1). Tem como principais princípios (Art.3): A garantia da liberdade de expressão (I); proteção da privacidade (II); "proteção dos dados pessoais, na forma da lei"; (III); entre outros. Além disso, estabelece (Art.7) a "inviolabilidade da intimidade e da vida privada" (I); "a inviolabilidade e sigilo do fluxo de suas comunicações pela internet" (II) e armazenadas (III); e o não fornecimento a terceiros de seus dados pessoais (VII) (Brasil, 2014). Vemos aqui um arcabouço para defesa dos direitos humanos no que tange ao direito à privacidade que excede, em muito, os avanços antes de Snowden.

Com relação às comunicações, foi criado um e-mail governamental, o que fornece certa segurança, mas continua ligado à rede de internet comum. É necessário ressaltar que esse provedor sofreu alguns golpes, por exemplo, em 2016 houve uma invasão hacker que incluiu este domínio (Pôssa, 2016) e em 2022 hackers se utilizaram do domínio para se passar pelo governo e efetuar golpes cibernéticos (Gov.br, 2022).

Com relação à neutralidade de redes, esse termo é creditado a Tim Wu (2011), para ele todo o domínio da internet deve ser público, no sentido de tratar igualmente a taxa cobrada por dados de todos os servidores. Isso gerou conflito com muitos interesses, tanto na área econômica quanto tecnológica, e a dificuldade de implementação deste princípio no Brasil gerou problemas que reverberaram na privacidade e liberdade de expressão dos usuários da internet (Lima, 2021). Sendo um pouco mais explicativo, Valente (2017) afirma que no contexto brasileiro essa expressão intui que o "tráfego da internet deve ser tratado igualmente, sem discriminação, restrição ou interferência independentemente do emissor, recipiente, tipo ou conteúdo, de forma que a liberdade dos usuários de internet não seja restringida" (Brasil, 2014). Por exemplo, uma empresa de telefonia não pode cobrar mais pelos dados móveis utilizados para fazer uma chamada telefônica pelo WhatsApp. Esse princípio, que corrobora com a privacidade e direitos do usuário, foi plenamente estabelecido no Brasil com o Marco Civil da Internet (Brasil, 2014).

Finalmente em 2018 foi promulgada a lei de proteção de dados (Lei nº 13.709 de 14/08/2018). Esta lei:

> dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

Em seu segundo artigo é garantido a privacidade dos dados digitais (Art.2.I), a "preservação inviolável de mensagens pessoais e imagens" (IV), e a "defesa dos direitos humanos" (VII). A completude da lei está direcionada a cada indivíduo ou a operações de tratamento de dados de "pessoa jurídica de direito público ou privado", incluindo até mesmo em banco de dados internacional, contanto que a operação de tratamento seja em território nacional (Brasil, 2018). Esta lei faz clara distinção entre dados pessoais (de maneira geral) e dados sensíveis, além de versar a favor da total privacidade (Art.5), regula a coleta de dados feita pelo estado ou por instituições (Art.3) e proíbe a coleta para casos não previstos em lei e autorizados por autoridade competente (Art.4).

Esta regulação versa que a coleta ou tratamento de dados podem ser autorizadas através de 10 maneiras diferentes dentre elas: Pelo consentimento do possuinte (Art.7.I), para "cumprimento de obrigação legal" (II); pelo governo para fins específicos (III); para "realização de estudos por órgão de pesquisa" (IV); e para a salvaguarda da vida do possuinte (VII). Ademais, "O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular" (Art.8), isso significa que nas outras 9 possibilidades de coleta de dados, somente a primeira terá como fator necessário o conhecimento do usuário da internet. Embora o titular tenha "direito ao acesso facilitado às informações sobre o tratamento de seus dados" (Art.9), esse direito é restrito a apenas 7 tópicos (Art.9 I-VII). O artigo 9, evidentemente, não garante que o usuário tenha acesso ao tratamento de seus dados em toda e qualquer situação e o Art.8 garante esse acesso apenas ao inciso I do Artigo 7. Isso deixa o titular relativamente vulnerável a determinadas situações, principalmente no que tange a coleta governamental. Um exemplo a ser levantando é o caso americano, citado no capítulo II deste trabalho, onde foi mostrado que a petição judicial efetuada pelo governo americano às empresas de telefonia, em que o usuário não recebeu nenhum tipo de notificação da existência dessa coleta de dados, por se tratar de coletas que visavam uma investigação secreta. Para casos desse tipo, ou parecidos, que envolvam algum tipo de investigação, ou coisas desse gênero, não há salvaguarda legal que obrigue o governo a notificar o titular. Ao contrário, o Art.11 permite a coleta e análise de dados pessoais sem a participação do titular para "cumprimento de obrigação legal" (II.a), "tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos" (II.b) e a salvaguarda da vida de terceiros (II.e) (Brasil, 2018).

A questão da garantia de políticas públicas e a proteção da vida de terceiros abrem margem para coleta de dados pessoais que visam a tão citada e de difícil definição, "segurança nacional". Com esta afirmação, este artigo não se porta contra ou a favor desse tipo de atitude, mas apenas traz ciência de que sendo bem argumentado, independente de suas vontades, conhecimento ou consentimento, todos os seus dados pessoais podem ser coletados e analisados pelo governo.

Além disso, nada é dito nas referidas leis, no que tange ao campo eletromagnético e a coleta de informações propagadas através de um RDS (rádio definido por software). Leis sobre o campo cibernético que não envolvem o campo eletromagnético é fator de grande preocupação, visto a interoperabilidade entre esses meios mostradas acima, no capítulo I.

Outro fator relevante a ser mencionado é a dificuldade da elaboração de leis para o campo cibernético. Um estudo de 2015 apresentou um software de coleta de metadados em cartões de crédito capaz de identificar pessoas pelas compras realizadas. Uma forma de fazer identificação de maneira reversa (Montjoye, 2015). Ao analisar esse software, Boff afirma que:

> Metadados anônimos e até mesmo protegidos por normas de sigilo bancário, tal como prevê a lei brasileira, tornam-se dados pessoais vulneráveis, eis que passíveis de identificação da pessoa em questão, ainda que sujeitos às proteções legais, especialmente as relacionadas com a tutela constitucional e civilista da vida privada.

Abrem-se, com isso, diversas possibilidades de registro e tratamento dos dados, inclusive de maneira ilícita, por governos, empresas e indivíduos (Boff; Fortes, 2016).

Isso demonstra que a elaboração de leis com vistas à privacidade cibernética encontra entraves no rápido avanço da tecnologia. A legislação muitas vezes não consegue acompanhar esses avanços, criando lacunas na proteção de dados pessoais e na privacidade dos indivíduos. A formulação de leis e regulamentos que abordem questões de privacidade cibernética é fundamental para equilibrar o avanço tecnológico com a proteção dos direitos individuais. Adicionalmente, é preciso fortalecer o debate público sobre a conscientização de boas práticas de segurança cibernética.

Assim, apesar das imperfeições e lacunas existentes nessas leis, conforme demonstrado nos parágrafos precedentes, elas representaram um avanço significativo na proteção da privacidade de dados. Contudo, foi somente em 2021 que o senado federal aprovou a proposta de emenda à constituição (PEC) 17/2019 e incluiu a proteção de dados privados, de maneira pessoal, no campo cibernético como como direito fundamental na constituição, aprovado por 64 votos a zero. Nesta PEC está previsto que a União terá razão exclusiva para legislar sobre o tema. O diferencial desta para anterior é que esta coloca o direito individual como comando específico ao invés de tratar essa questão de maneira genérica. (Senado notícias, 2021).

Após as revelações de Snowden, ao tratar de privacidade cibernética, o Brasil, de fato, avançou, principalmente com o "marco civil da internet". Após 2013, as empresas privadas e governos estrangeiros ficam impedidos de coletar dados em massa em território nacional (sem o consentimento dos usuários). Contudo, é necessário refletir sobre a ciência da população com relação a esses riscos. Não é difícil supor que a imensa maioria dos brasileiros que utilizam os aplicativos das grandes *Big Techs* não tenham lido os termos de serviço de seus programas e seguem lotando essas plataformas de informações que, em certo sentido, podem ser consideradas sua própria vida.

Outra ação governamental é a preocupação do governo em alertar a população. O Senado Federal divulgou algumas publicações para alertar a população quanto ao perigo da coleta de dados em massa e demonstrar que os parlamentares estão preocupados em debater o assunto. A que melhor se destaca aos fins deste trabalho é a edição "espionagem cibernética" que afirma que "a interconexão abriu caminho para novos e alarmantes níveis de invasão de privacidade" (Em discussão, 2014). Esta cartilha demonstra que historicamente a privacidade possui valor social, como por exemplo as leis de direitos civis dos ingleses datadas do século 17 que proibiam o governo monárquico de entrar em locais privados, como residências, sem autorização de seus possuintes. Tais exemplos históricos devem instruir a população a não renunciar seus direitos e perceber que tratar de privacidade é uma questão de garantia da democracia (p. 14-15). A publicação traz algumas informações sobre a maneira como ocorrem a coleta de dados cibernéticos para que a população entenda os pontos vulneráveis e elenca alguns dos programas de coleta de dados americanos (p. 10-11).

Porém, apesar desses pontos positivos, o texto do Senado Federal parece demostrar uma situação brasileira mais otimista que a realidade. Segundo Rafael Mandarino (ex-Diretor do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional (GSI) o Brasil "está em um "bom nível" de entendimento e de preparo para a segurança e a defesa cibernéticas" (p. 17). Atitudes que visam não criticar a real situação do governo, aparentemente em prol de evitar degradar a imagem populacional, pode ser muito prejudicial e levar a população a acreditar que a segurança digital é uma realidade. O texto do senado dá a entender que a segurança existe, mas que os funcionários governamentais são o problema para o vazamento de dados. Segundo um relatório do TCU "73% das 337 instituições públicas federais pesquisadas não classificam a informação, 90% não fazem análise de riscos e 55% não possuem política de segurança da informação" (p. 17). Para o

Senado brasileiro metade dos órgãos da administração pública não está preocupada com a defesa cibernética e tramitam informações sem a devida segurança, mesmo havendo uma média de dois mil e cem ataques por hora nas redes de informação do governo, além de uma única rede registrar 4,4 milhões de incidentes de segurança (p. 18).

Segundo o Senado brasileiro e a ex-presidente Dilma o maior problema é a concentração de servidores de internet nos Estados Unidos e a dependência tecnológica deste meio americano (p. 19). Uma medida tomada pelo governo nesse sentido foi a criação de cabos submarinos que não passem por solo americano. Veja a figura 1 e perceba que existem 3 cabos que vão diretamente na direção da África e Europa. O primeiro chama-se EllaLink, construído em julho de 2021 e colocado em operação em 2023, que efetua ligação entre o Brasil, Portugal e Marrocos (Submarinecablemap, 2023). Este meio cibernético foi construído pela empresa portuguesa EllaLink em 2021, através da construtora de cabos francesa *Alcatel Submarine Networks* (ASN) e a italiana GTT. A construção não utilizou capital da Telebras e foi construída apenas com aporte estrangeiro (Bucco, 2019).

O segundo cabo submarino em questão é o *South Atlantic Inter Link* (SAIL), que liga o Brasil a Camarões, construído em 2020 pela Huawei Marine Networks, a já citada construtora chinesa. Esse meio foi construído com uma parceria entre a China Unicom e a CAMTEL (estatal de telecomunicações do Camarões). Novamente, ressalta-se que o Brasil não participou da construção (Huawei, 2018).

O terceiro em questão é o *South Atlantic Cable System* (SACS), construído em 2018 pela *Angola Cables* em parceria com a *NEC Corporation* uma empresa japonesa (de integração de sistemas de cabos de fibra óptica) e a *Orange Marine*, uma empresa francesa. Ambos sem capital brasileiro (TeleGeography, 2023).

Existe uma empresa privada que atua na construção de cabos submarinos chamada GlobeNet. Atualmente essa companhia é de capital brasileiro, mas está sediada na Flórida. Esta empresa foi vendida pela empresa Tele ao BTG Pactual em 2014, e em 2021 já havia se tornado uma das grandes empresas do ramo de cabos submarinos (Valenti, 2021). Esta empresa é proprietária do cabo GlobeNet (que liga Brasil, Venezuela, Colômbia e Estados Unidos) e lançou o cabo *Malbec* que conecta Rio de Janeiro e São Paulo a Buenos Aires e tem pretensão de conectá-lo aos Estados Unidos (TeleGeography, 2023).

Percebe-se que apesar de ser uma empresa de capital nacional, ela não participou (como já demonstrado) do lançamento dos meios que conectam o Brasil a países não americanos e seus cabos submarinos se restringem às américas. É notório que apesar de o governo brasileiro reconhecer a necessidade de reduzir sua dependência dos Estados Unidos em 2013, dez anos depois ele permanece totalmente dependente do solo americano e a imensa maioria de suas ligações cabeadas passam por lá (veja figura 2). A conexão com a Europa e a África é feita por empresas francesas e chinesas, países que participaram de escândalos de coleta de dados. Trocar a dependência americana por dependência chinesa deve ser questionada uma vez que não fortalece a autonomia estratégica do Brasil. Não há motivos para ter total confiança na privacidade dos dados nacionais se eles estiverem nas mãos de estrangeiros que possuem seus próprios interesses estratégicos e que já estiveram envolvidos em espionagem.

Evidentemente, o lançamento de cabos nacionais não garante completamente a segurança de dados, como muito bem salientou a comissão parlamentar de inquérito (CPI) da espionagem:

> A NSA, segundo consta, age por meio de grampeamento dos cabos submarinos (...), é necessário investir no lançamento de cabos óticos submarinos do Brasil para outras regiões com vistas a diminuir a dependência dos Estados Unidos para comunicação com outras partes do globo (...) conforme aponta a Estratégia Nacional de Defesa. Hoje, 90% do tráfego de informações que sai do Brasil passa pelo território norte-americano, ainda que se destine a outras localidades (Ferraço, 2014).

Repare que mesmo reconhecendo a espionagem americana por meio de grampos cabeados, a CPI recomendou a instalação de cabos nacionais, isso se dá porque a “coleta de dados é (...) árdua. Os cabos estão no fundo do mar, com suas grossas armaduras para proteger as frágeis fibras óticas do ambiente agressivo, e às vezes utilizam dispositivos alimentados em alta tensão (Ferraço, 2014).

A CPI da Espionagem atestou a veracidade das denúncias de que a Agência de Segurança Nacional dos Estados Unidos (NSA), pratica coleta de dados em massa no Brasil, inclusive da presidente da república, demonstrou que o Brasil está vulnerável à inteligência estratégica estrangeira devido à falta de uma política eficaz de defesa cibernética, além de não possuir recursos cabíveis para combater essa prática. A CPI, por fim, recomenda melhoria nas regulações e aumento dos investimentos em segurança digital (Ferraço, 2014).

Mesmo após o reconhecimento das vulnerabilidades feita pela comissão, foi exposto acima que as regulações criadas, apesar de serem um grande avanço, não são em si mesmas, suficientes para combater a espionagem, além disso, a dependência dos provedores americanos dadas pelos cabos submarinos permanece. Não foram encontradas grandes propagandas governamentais no que tange a conscientização populacional da inteligência estratégica estrangeira. É realmente muito difícil afirmar que o brasileiro, de maneira geral, tenha qualquer conscientização do perigo da coleta de dados, tanto para sua própria vida, quanto para o país como um todo, prova disso foi uma matéria publicada pela revista Exame em 2021. Segundo essa matéria, em uma pesquisa feita pelo instituto Ipsos, o Google é a empresa mais influente no Brasil, e o YouTube ficou em segundo lugar (Exame, 2021). O Brasil é o terceiro país do mundo que mais busca por moda e beleza no Google (Pavan, 2023), 93% dos brasileiros pesquisam no Google antes de efetuar uma compra, o que é um número impressionante se considerarmos a grande quantidade de pessoas abaixo da linha da pobreza no Brasil (Teodoro, 2021). Segundo a revista Forbes, o Brasil é o terceiro país que mais utiliza as redes sociais do mundo (Pacete, 2023). Em certo sentido, face ao exposto no capítulo dois, poderia se dizer, em tese, que o Brasil é um dos países que mais alimenta o banco dados das grandes redes sociais e consequentemente um dos maiores produtores de informações pessoais do mundo.

Dez anos depois da divulgação dos documentos da NSA por Snowden, ao invés de reduzir e salvaguardar os cidadãos dos perigos da coleta de dados, o Brasil se tornou um grande consumidor de redes sociais, e como muito bem diz um famosíssimo jargão: Quando o serviço é de graça, o produto é você. Cabe-se ressaltar, todavia que, muito além de simples privacidade, o assunto diz respeito a quantidade de informações que, vistas em conjunto podem ser de grande valia estratégica para nações estrangeiras (Conforme explanado no capítulo 2). Como o Sistema Internacional, conforme a teoria realista, é anárquico, cabe-se refletir sobre os riscos e desvantagens que um país pode ter quando seus cidadãos, voluntariamente, entregam todas as suas informações pessoais a nações estrangeiras. Ademais quando as informações governamentais podem estar comprometidas.

CONCLUSÃO

O Capítulo 1 lançou as bases fundamentais para compreensão do assunto e demonstrou que o espaço eletrônico-cibernético é extremamente vulnerável. Tratando-se do espectro eletromagnético, possuir a chave de criptografia das chamadas de telefone traz extrema facilitação para que a espionagem seja realizada. Foi demonstrado que o campo cibernético é um novo domínio de insegurança e vulnerabilidade para o Estado e para as populações.

No capítulo 2 foi elencado os principais programas de espionagem eletrônico-cibernética dos Estados Unidos e observado que as chaves de criptografia do maior produtor de cartão SIM do mundo foram roubadas, o que, conforme dito no capítulo 1 deu livre acesso a quase todas chamadas. Além disso, observamos a busca pelos computadores quantum e a coleta em massa de SMS. Por fim, vimos os programas que coletam dados das redes sociais, de aplicativos de internet, e diretamente dos cabos submarinos. Como se não bastasse existe a questão do programa PRISM que armazena e associa as informações coletadas nos demais programas e cria um banco de dados pesquisável. Assim, a abrangência dos programas da NSA incluiu, de maneira organizada, quase todas as chamadas de telefone, SMS, e praticamente tudo que passava pelos principais cabos submarinos. Foi possível perceber que o Brasil possui um alto grau de vulnerabilidade devido a sua dependência de cabos submarinos estrangeiros.

No capítulo 3 foi demonstrado que a espionagem não terminou, apesar das diversas tentativas internacionais. A observação de ambos os capítulos em conjunto demonstra que a situação do Brasil é muito complicada. A proximidade da embaixada norte-americano dos principais prédios governamentais brasileiros, os cabos submarinos em sua maioria chegando aos Estados Unidos e a dependência tecnológica nos deixou em uma situação que nem mesmo o presidente da república conseguiu escapar com facilidade.

No capítulo 4 que tange a situação brasileira, as novas políticas públicas tiveram como fator principal a criação do Marco Civil da Internet. Este foi um grande avanço no que tange à proteção dos indivíduos, porém, apesar de ser uma base para a proteção cibernética, não é suficiente para garantir a privacidade frente às ameaças citadas. Além disso, é necessário perceber que as regulações, conforme mostradas, enfrentam a dificuldade da volatilidade tecnológica, cujo avanço se dá muito rapidamente. É necessário que o Estado esteja atento à infindável criação ou atualização de normas no campo cibernético, para abarcar as mais diversas tecnologias emergentes. Ainda assim precisamos perceber, como é notório a todos, que os crimes cibernéticos com novas tecnologias que burlam a lei, são anteriores a regulação que os proíbe, ou seja, primeiro o problema é identificado e depois combatido. Disto surge a percepção da necessidade de um sistema nacional de proteção digital dotado de maior robustez possível.

De maneira geral, o presente trabalho demonstrou que as ações do Estado brasileiro, realizadas após a descoberta dos documentos vazados por Snowden, apesar de importantíssimas e necessárias, não foram suficientes para acabar ou reduzir consideravelmente a coleta de dados em massa e a utilização dos aplicativos das grandes *Big Techs*. Aparentemente, a única opção viável para o Brasil é o investimento em um sistema de comunicação nacional, próprio para que os agentes governamentais possam se comunicar de forma mais segura em um meio tecnologicamente robusto. Seria de capital importância que o cidadão venha a optar voluntariamente pela sua utilização. Investimentos em ciência e tecnologia tornam-se imprescindíveis para tal. Além disso, não é necessário isolar os cidadãos brasileiros do mundo, como fazem governos autoritários e ditatoriais, devemos levar em consideração uma maior consciência populacional frente à espionagem, com isso refere-se a propaganda em massa sobre segurança de dados. Proibir acesso aos dados do globo pode

tomar um tom ditatorial, e não está no escopo deste trabalho mensurar as consequências internacionais causadas por uma ruptura completa com os dados globais. Uma boa opção, e muito menos radical, visa conscientizar a população, para que, livremente, os indivíduos escolham o sigilo de dados e possam aproveitar da tecnologia sem expor suas vidas em redes sociais ou conversas de aplicativos.

Outro ponto relevante nesse sentido é que, como demonstrado acima, a opinião pública acarretou a mudança dos grandes bancos de dados de armazenamento em nuvem. O governo precisa perceber que um investimento em operação de informação voltado ao combate da coleta de dados é verdadeiramente eficaz. Se o cidadão não se sente seguro com a utilização de determinado aplicativo e opta por utilizar um aplicativo do concorrente, ou do governo, o custo financeiro da coleta indiscriminada aumentará sobremaneira. Isso é suficiente para afirmar que, quando a espionagem é praticada contra a população, um movimento populacional pode combatê-la, mas para tal, é necessário o conhecimento dos fatos.

A vulnerabilidade do espaço eletrônico-cibernético é uma questão difícil de resolver. Quando se trata de ondas eletromagnéticas, ao nos depararmos com os programas citados, podemos concluir que não há proteção disponível que possa ser suficientemente confiável ao ponto de trafegar dados sensíveis. Principalmente ao levarmos em consideração que países como os Estados Unidos parecem continuar com a utilização dos programas citados (apesar de algumas restrições). Isso nos leva a refletir sobre a necessidade de um sistema cabeado, como fibra ótica, menos dependente de ondas eletromagnéticas (onde a dependência de tecnologia é muito grande e a vulnerabilidade é inevitável, como visto nos conceitos básicos apresentados no capítulo 1). Com relação a chamada governamental para outros países, os novos cabos submarinos (que vão em direção a África e a Europa) foram construídos por estrangeiros e a confiança total nesses meios pode se confundir com uma percepção equivocada, e isso pode aumentar a vulnerabilidade do país. Nesta linha, a empresa GlobeNet poderia ser muito útil, porém é necessário analisar os interesses desta empresa uma vez que ela está sediada no país que possui os maiores escândalos de coleta de dados. É realmente muito difícil fugir da conclusão de que uma empresa nacional de construção de cabos submarinos é necessária.

Não há como homiziar-se completamente do perigo da espionagem, principalmente se levarmos em consideração que a coleta de dados em massa é um grande recurso para a tomada de decisão estatal e que, como visto no capítulo 3, não temos sanções internacionais, até o momento, aplicadas de maneira forte o suficiente para deter essa prática. Porém, apesar das dificuldades, é possível restringir a espionagem, e esse tipo de atitude deve ser de capital importância para qualquer governo pertencente ao mundo globalizado e digitalizado do século XXI, principalmente para o Brasil, país dotado de grandes riquezas.

Ao longo deste trabalho ressaltamos como a inteligência estratégica estrangeira encontra no Brasil um terreno fértil e, tratando-se do maior país da América do Sul, é fundamental a busca pelo fortalecimento defensivo nesse campo tão importante. Este trabalho identificou que outras pesquisas podem ser realizadas sobre a relação entre segurança cibernética e produção de inteligência estratégica. As potenciais pesquisas futuras poderiam envolver estudos aprofundados sobre a eficácia da resposta internacional para garantia dos direitos humanos. Além disso, poderia ser feito um estudo profundo voltado para inteligência estratégica americana e seus impactos na política de defesa brasileira.

REFERÊNCIAS

ADAMY, David L. **EW 101:** A First Course in Electronic Warfare. 2. ed. Boston: Artech House, 2001.

ADAMY, David L. **EW 102:** A Second Course in Electronic Warfare. Boston: Artech House, 2004.

ADAMY, David L.. **EW 103:** A Third Course in Electronic Warfare: Tactical Battlefield. communications electronic warfare. 2 ed. Boston: Artech House, 2009.

ADAMY, David L. **Electronic Warfare Pocket Guide**. SciTech Publishing. Carolina do Norte, 2011.

ADAM, T. Elsworth. **Electronic Warfare:** Defense, Security and Strategy. Nova Science Nova York, 2010.

ANGWIN, JULIA, et al. AT&T Helped U.S. Spy on Internet on a Vast Scale. **The New York Times**, 2015. Disponível em: https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html. Acesso em: 07 ago. 2023.

BAUMAN, David j. Cellular Packet Communications. Tecnopolíticas e vigilância. vol. 18. N° 2, 2015.

BAUMAN, Zygmunt (et al). Após Snowden: Repensando o Impacto da Vigilância. **Revista Eco Pós**, vol. 18, nº 2, 2015. Disponível em: https://revistaecopos.eco.ufrj.br/eco_pos/article/view/2660. Acesso em: 17 out. 2023.

BOWCOTT, Owen. Intelligence services 'creating vast databases' of intercepted emails. The Guardian, Londre, 2014. Disponível em: https://www.theguardian.com/uk-news/2014/jul/18/intelligence-services-email-database-internet-tribunal. Acesso em: 17 ago. 2023.

BRASIL. Cabos submarinos. ANATEL. Disponível em: https://www.gov.br/anatel/pt-br/dados/infraestrutura/cabos-submarinos. Acesso em 20 jul. 2023.

BRASIL.**Lei nº 12.527**, de 18 de novembro de 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 06 set. 2023.

BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 06 set. 2023.

BRASIL. **Lei n° 12.965**, de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 06 set. 2023.

BRASIL. Alerta de golpe por e-mail. **Gov.br**, 2022. Disponível em: https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/12/alerta-de-golpe-por-e-mail. Acesso em: 15 set. 2023.
BROOKE, Heather. What's really changed 10 years after the Snowden revelations? The Guardian, 2023. Disponível em: https://www.theguardian.com/us-news/2023/jun/07/edward-snowden-10-years-surveillance-revelations Acesso em: 7 ago. 2023.

BROOKE, Heather. States haven't stopped spying on their citizens, post-Snowden – they've just got sneakier. The Guardian, 2023. Disponível em: https://www.theguardian.com/commentisfree/2023/jun/06/edward-snowden-state-surveillance-uk-online-safety-bill. Acesso em: 16 set. 2023.

BUUCO, Rafael. Sem dinheiro da Telebras, começa a construção do cabo submarino Brasil-Europa. Tele.sintese, 2019. Disponível em: https://www.telesintese.com.br/sem-dinheiro-da-telebras-comeca-a-construcao-do-cabo-submarino-brasil-europa/. Acesso em: 12 out. 2023.

CONSILIUM EU. Proteção de dados na EU. Disponível em: https://www.consilium.europa.eu/pt/policies/data-protection/#rights. Acesso em: 19 ago. 2023.

COLARIK, Andrew; JANCZEWSKI, Lech (eds.). **Cyber warfare and cyber terrorism**. Information Science Reference: Hershey, Pensilvânia, 2008.

CRONIN, Blaise; CRAWFORD, Holly. Information Warfare: Its Application in Military and Civilian Contexts. **The Information Society:** An International Journal. Volume 15, 1999. Disponível em: https://www.tandfonline.com/doi/abs/10.1080/019722499128420. Acesso em: 17 ago. 2023

CZOSSECK, Chirstian (Edt), GEERS, Kenneth (Edt). **The Virtual Battlefield:** Perspectives on Cyber Warfare. IOS Press BV: Amsterdam, 2009.

EM DISCUSSÃO: Espionagem cibernética. Brasília: Secretaria Agência e Jornal do Senado, ano 5, nº 21, jul. 2014. Disponível em: https://www2.senado.leg.br/bdsf/item/id/503306. Acesso em: 01 out. 2023.

EUR-LEX. **Summaries of EU Legislation:** General data protection regulation (GDPR). European Union law, 2022. Disponível em: https://eur-lex.europa.eu/EN/legal-content/summary/general-data-protection-regulation-gdpr.html#:~:text=Regulation%20(EU)%202016%2F679%20of%20the%20European%20Parliament%20and,(OJ%20L%20119%2C%204.5 Acesso em: 19 ago. 2022.

FERRAÇO, Ricardo. **Relatório final da CPI da espionagem**. Brasília: Senado Federal, 2014. Disponível em: https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco. Acesso em: 13 out. 2023.

FRATER, Michael R. **Electronic Warfare for the Digitized Battlefield**. Artech Print on Demand, 2001.

FIREEYE. Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. Mandiant, 2022. Disponível em: https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor. Acesso: 25 Jul. 2023.

GENOVA, James. **Electronic Warfare Signal Processing**. Artech House: Massachusetts, 2018.

GHOSH, Nirmal *et al*. NSA spied on Indian embassy and UN mission, Edward Snowden files reveal. **The Guardian**, 2014. Disponível em: https://www.theguardian.com/world/2013/sep/25/nsa-surveillance-indian-embassy-un-mission Acesso em: 07 ago. 2023.

GOODMAN, David J. Cellular Packet Communications. **Transactions on communications**, vol. 38, n° 8, 1990.

GOUVÊA, Conrado P. L. **Introdução à Computação Quântica.** Instituto de Computação, Universidade Estadual de Campinas: SP, 2023. Disponível em: https://www.ic.unicamp.br/~ducatte/mo401/1s2008/T2/079724-t2.pdf. Acesso em 05 ago 2023.

GOOGLE. **Política de privacidade**. Disponível em: https://policies.google.com/privacy?hl=pt-BR Acesso em: 20 jul. 2023.

GOOGLE. **Termos de serviço**. Disponível em: https://policies.google.com/terms?hl=pt-BR Acesso em 20 jul. 2023.

GREENWALD, Glenn *et al*. NSA collects millions of text messages daily in 'untargeted' global sweep. **The Guardian**, 2014. Disponível em: https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep Acesso em: 5 ago. 2023.

GREENWALD, Glenn. NSA collecting phone records of millions of Verizon customers daily. **The Guardian**, 2013. Disponível em: https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep Acesso em: 7 ago. 2023.

GREENWALD, Glenn; Macaskill, Ewen. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian**, 2013. Disponível em: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data Acesso em 17 ago. 2023.

GREENWALD, Glenn. Us threatened germany over snowden, vice chancellor says. **The Intercept**, 2015. Disponível em: https://theintercept.com/2015/03/19/us-threatened-germany-snowden-vice-chancellor-says/ Acesso em: 8 ago. 2023.

HAUTALA, Laura. **NSA surveillance programs live on, in case you hadn't noticed**. CNET, 2018. Disponível em: https://www.cnet.com/tech/services-and-software/nsa-surveillance-programs-prism-upstream-live-on-snowden/ Acesso em: 18 ago. 2023

HUAWEI. Cabo submarino de alta velocidade conecta América Latina e África. **Huawei noticias**, 2018. Disponível em: https://www.huawei.com/br/news/br/2018/setembro/cabo-submarino. Acesso em: 12 out. 2023.

INFOCURIA. Acórdão do tribunal de justiça (grande secção) - português. **InfoCuria**, 2020. Disponível em: https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=10257253. Acesso em: 14 de setembro de 2023.

IRION, Kristina. Cloud services made in Europe after Snowden and Schrems. **Internet policy review**, 2015. Disponível em: https://policyreview.info/articles/news/cloud-services-made-europe-after-snowden-and-schrems/377 Acesso em: 30 de Agosto de 2023.

JUDICIARY COMMITTEE. USA Freedom Act. Disponível em: https://judiciary.house.gov/usa-freedom-act Acesso em: 7 ago. 2023.

KAN, Shirley. China's Anti-Satellite Weapon Test. **CRS Repost for congress**, 2007. Disponível em: https://sgp.fas.org/crs/row/RS22652.pdf. Acesso em 12 ago. 2023.

KRISTIANSSON, Jacob. Vigilância Digital em nome da Segurança Nacional. 2023. Trabalho de conclusão de curso (bacharel em ciência política). Universidade de Lund, Lund, Suécia. Disponível em: https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9105587&fileOId=9106782 Acesso em: 18 ago. 2023.

LAUDAU, Susan. Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations. **IEEE Security & Privacy**. Vol.11, 2013. Disponível em: https://www.computer.org/csdl/magazine/sp/2013/04/msp2013040054/13rRUwIF6ck Acesso em: 19 ago. 2023.

LEMOS, Ronaldo. 10 perguntas para Ronaldo Lemos, especialista em direito digital. **Isto é Dinheiro**, 2012. Disponível em: https://istoedinheiro.com.br/10-perguntas-para-ronaldo-lemos-especialista-em-direito-digital/. Acesso em: 05 set. 2023.

LIMA, Cintia R. Neutralidade da rede e proteção do consumidor no contexto pandêmico. **ConJur**, 2021. Disponível em: https://www.conjur.com.br/2021-jun-16/garantias-consumo-neutralidade-rede-protecao-consumidor-contexto-pandemico. Acesso em: 01 set. 2023.

MA, David. C. Deterministic-Based Performance Modeling of a Cluster of Nodes Handling Subscriber Profile Query and Update in CDMA Mobile Switching Center. **Bell Labs technical journal**, Vol.12 (1), 2007, p.247-261. Disponível em: https://www-periodicos-capes-gov-br.ezl.periodicos.capes.gov.br/index.php/buscador-primo.html Acesso em: 21 jul. 2023.

MACASKILL, Ewen *et al*. **GCHQ taps fibre-optic cables for secret access to world's communications**. Disponível em: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa Acesso em: 17 ago. 2023.

MATHEWS, Peter. SIGINT: **The secret History of signals intelligence in world wars**. The History Press: Gloucestershire, 2013.

MOORE, Daniel. **Offensive Cyber Operations:** Understanding Intangible Warfare. Hurst & company: LONDON, 2022.

MONTJOYE, De Yon. et al. Unique in the shopping mall: On the reidentifiability of credit card metadata. **Science,** vol. 347, n°221, p. 536–539, 29 jan. 2015. Disponível em: https://www.researchgate.net/publication/271591449_Unique_in_the_shopping_mall_On_the_reidentifiability_of_credit_card_metadata. Acesso em: 06 set. 2023.

MARQUIS-BOIRE, Morgan; GREENWALD, Glenn. XKEYSCORE NSA's Google for the World's Private Communications. **The Intercept**, 2015. Disponível em: https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/ Acesso em: 29 Ago. 2023.

NAÇÕES UNIDAS. Assembleia Geral da ONU aprova resolução de Brasil e Alemanha sobre direito à privacidade. **Nações Unidas**, 2013. Disponível em: https://brasil.un.org/pt-br/64661-assembleia-geral-da-onu-aprova-resolu%C3%A7%C3%A3o-de-brasil-e-alemanha-sobre-direito-%C3%A0-privacidade. Acesso em 07 out. 2023.

OLIVEIRA, Nathan. A geopolítica da vigilância da Agência Nacional de Segurança dos Estados Unidos (NSA): A espionagem da América Latina como recurso de poder. **Diário das nações.** Disponível em: https://diariodasnacoes.wordpress.com/2020/12/18/a-geopolitica-da-vigilancia-da-agencia-nacional-de-seguranca-dos-estados-unidos-nsa/ Accesso em: 19 ago. 2023.

PACETE, Gustavo. L. Brasil é o terceiro maior consumidor de redes sociais em todo o mundo. **Forbes**, 2023. Disponível em: https://forbes.com.br/forbes-tech/2023/03/brasil-e-o-terceiro-pais-que-mais-consome-redes-sociais-em-todo-o-mundo/?amp Acesso em: 15 out. 2023.

PAVAN, Bruno. Brasil é o terceiro país que mais busca por moda e beleza na Google, diz pesquisa. **Isto é Dinheiro**, 2023. Disponível em: https://istoedinheiro.com.br/brasil-e-o-terceiro-pais-que-mais-busca-por-moda-e-beleza-na-google-diz-pesquisa/ Acesso em: 15 out. 2023.

POISEL, Richard. Introduction to communication electronic warfare systems. Norwood: Artech House: Massachusetts, 2002.

PÔSSA, Nanna. Hackeres invadem sites governamentais do Rio em protesto contra Olimpíada. **Rádio agência**, 2016. Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/geral/audio/2016-08/hackeres-invadem-sites-governamentais-do-rio-em-protesto. Acesso em: 15 set. 2023.

REFORM GOVERNMENT SURVEILLANCE. **EU Adequacy Decision Provides Certainty and Privacy Protection.** REFORM GOVERNMENT SURVEILLANCE, 2023. Disponível em: https://www.reformgovernmentsurveillance.com/post/eu-adequacy-decision-provides-certainty-and-privacy-protection Acesso em: 14 set. 2023.

RICH, Steven; GELLMAN, Barton. NSA seeks to build quantum computer that could crack most types of encryption. **The Washington Post**, 2 jan. 2014. Disponível em: https://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html Acesso em: 5 ago. 2023.

ROSSITER, Ash. High-Energy Laser Weapons: Overpromising Readiness. **The US Army War College Quarterly**: Parameters, v..48, n°4. Disponível em: < https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3010&context=paramete Acesso em 20 Jul. 2023.

SCAHILL, Jeremy; BEGLEY, Josh. The great sim heist: How Spies Stole the Keys to the Encryption Castle. **The Intercept**, 2015. Disponível em: https://theintercept.com/2015/02/19/great-sim-heist/ Acesso em: 8 ago. 2023

SENADO NOTÍCIAS. **Senado inclui proteção de dados pessoais como direito fundamental na Constituição**. Agência do senado: Brasília, 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/10/20/senado-inclui-protecao-de-dados-pessoais-como-direito-fundamental-na-constituicao acesso em: 19 Set. 2023.

SILVA, Italia L. C. S. **Do 1g ao 5g:** evolução das redes de telefonia móvel. UFRB: Bahia, 2016. Disponível em: https://www2.ufrb.edu.br/bcet/components/com_chronoforms5/chronoforms/uploads/tcc/20190327163532_2015.2_-_TCC_Itala_Liz_-_Do_1g_Ao_5g_Evolucao_Das_Redes_de_Telefonia_Movel.pdf Acesso em: 20 jul. 2023.

SILVA, Mario J.V.T. Thienen. **Investigando a telefonia celular:** ensinando-aprendendo com a interatividade em uma abordagem temática no ensino de Física. TESE (mestre em educação) linha de investigação Ensino de Ciências Naturais. Universidade Federal de Santa Catarina, 2003. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/86103/194754.pdf?sequence=1 Acesso em: 21 jul. 2023.

SECURE TECHNOLOGY ALLIANCE. **Claro Brazil selects Gemalto for mobile network optimization.** Disponível em: https://www.securetechalliance.org/claro-brazil-selects-gemalto-for-mobile-network-optimization/. Acesso em: 04 de Ago. 2023.

SNOWDEN, Edward. Eterna vigilância: como montei e desvendei o maior sistema de espionagem do mundo. Tradução de Sandra Martha Dolinsky. São Paulo: Planeta do Brasil, 2019. 288p.

SOUSA, Leandro. Vivo: Solução com Gemalto. **Baguete**, 2013. Disponível em: https://www.baguete.com.br/noticias/28/11/2013/vivo-solucao-nfc-com-gemalto. Acesso em 13 jul. 2023.

TELEGEOGRAPHY. **Submarine Cable Map**. Disponível em: https://www.submarinecablemap.com/submarine-cable/firmina Acesso em: 20 jul. 2023.

TELETIME. Oi e Gemalto juntas na oferta de conteúdos do Pan Rio 2007. **Teletime**, 25 jun. 2007. Disponível em: https://teletime.com.br/25/06/2007/oi-e-gemalto-juntas-na-oferta-de-conteudos-do-pan-rio-2007/. Acesso em: 08 Abr. 2023.

TEODORO, Marina. **93% dos brasileiros pesquisam no Google antes de comprar**. E-Commerce Brasil, 2021. Disponível em: https://www.ecommercebrasil.com.br/noticias/pesquisa-google-antes-comprar. Acesso em: 15 out. 2023.

THE GUARDIAN. NSA boundless informant: vast data-mining trawls online help-track targets. **The Guardian**, Londres, 2013. Disponível em: https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining Acesso em: 7 ago. 2023.

THE GUARDIAN. James Clapper pressed for number of citizens US collects data on. **The Guardian**, Londres, 2016. Disponível em: https://www.theguardian.com/world/2016/apr/22/james-clapper-nsa-spying-us-data-collection-senate-hearing Acesso em: 7 ago. 2023.

THE GUARDIAN. Brazil to legislate on online civil rights following Snowden revelations. **The Guardian**, Londres, 2013. Disponível em: https://www.theguardian.com/world/2013/nov/01/brazil-legislate-online-civil-rights-snowden Acesso em: 06 set. 2023.

TOZETTO, Claudia. **Após espionagem dos EUA, Brasil tenta acelerar construção de cabos submarinos**. Disponível em: https://nic.br/noticia/na-midia/apos-espionagem-dos-eua-brasil-tenta-acelerar-construcao-de-cabos-submarinos/ Acesso em: 20 jul. 2023.

UNITED NATIONS. **Report of the Special Rapporteur on the Promotio.** United nations digital library, 2018. Disponível em: https://digitallibrary.un.org/record/1631686. Acesso em: 07 out. 2023.

UNITED NATIONS. **The right to privacy in the digital age.** United nations digital library, 2014. Disponível em: https://digitallibrary.un.org/record/788140. Acesso em: 07 out. 2023.

UNITED NATIONS. **The right to privacy in the digital age.** United nations digital library, 2020. Disponível em: https://digitallibrary.un.org/record/3896430. Acesso em: 07 out. 2023.

VALENTE, Jonas. Entenda o que é neutralidade de rede e como é o seu funcionamento no Brasil. **Agência Brasil**, 2017. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2017-12/entenda-o-que-e-neutralidade-de-rede-e-como-e-o-seu-funcionamento-no-brasil. Acesso em 14 set. 2023.

WILEY, Richard G. **ELINT: the interception and analysis of radar signals**. Artech House radar library. Norwood: Artech house: Massachusetts, 2006.

WIKILEAKS. **NSA Targets World Leaders for US Geopolitical Interests**. WikiLeaks, 2016. Disponível em: https://wikileaks.org/nsa-201602/ Acesso em: 08 ago. 2023.

WOLFE, Jan; PIERSON, Brendan. **Explainer-U.S. government hack:** espionage or act of war? Reuters, 2020. Disponível em: https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor Acesso em: 25 jul 2023.

WRIGHT, David; KREISSL, Reinhard. **European responses to the Snowden revelations**: A discussion paper. Increasing Resilience in Surveillance Societies: Londres, 2013. Disponível em: https://cyberwar.nl/d/fromEUFP7/IRISS/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf Acesso em: 8 ago. 2023.

ZETTER, Kim. **Snowden: Spy Agencies 'Screwed All of Us' in Hacking Crypto Keys**. Wired, 2015. Disponível em: https://www.wired.com/2015/02/snowden-spy-agencies-screwed-us-hacking-crypto-keys Acesso em: 5 ago 2023.