Laura Mabel Lacaze

VIGILÂNCIA MASSIVA DE COMUNICAÇÕES: uma (ciber)Inquisição. Análise do discurso estadunidense no período 2001 - 2016

Dissertação submetida ao Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina para obtenção do Grau de Mestre em Relações Internacionais.
Orientadora: Prof[a]. Dr[a]. Clarissa Franzoi Dri

Florianópolis

2017

Laura Mabel Lacaze

VIGILÂNCIA MASSIVA DE COMUNICAÇÕES: uma (ciber)Inquisição. Uma análise do discurso estadunidense no período 2001 - 2016

Esta Dissertação foi julgada adequada para obtenção do Título de Mestre em Relações Internacionais e aprovada em sua forma final pelo Programa de Pós-Graduação em Relações Internacionais da Universidade Federal de Santa Catarina.

Florianópolis, 16 de março de 2017

.

_____
Prof.ª Dr.ª Clarissa Franzoi Dri
Coordenadora do Curso

Banca Examinadora:

_____
Prof.ª Dr.ª Clarissa Franzoi Dri
Orientadora
Universidade Federal de Santa Catarina

_____
Prof. Dr. Eugenio Raúl Zaffaroni
Membro titular
(videoconferência)
Universidade de Buenos Aires

_____
Profª. Drª. Karine de Souza Silva
Membro titular
Universidade Federal de Santa Catarina

_____
Prof. Dr. Rogério Christofoletti
Membro titular
Universidade Federal de Santa Catarina

AGRADECIMENTOS

O conteúdo dessa seção deu voltas na minha cabeça quase que desde o início da pesquisa. Essa dissertação é resultado de um longo processo no qual estiveram envolvidas muitas pessoas e embora simples palavras não sejam suficientes para expressar a minha gratidão gostaria sim mencionar alguma delas.

Em primeiro lugar gostaria agradecer a generosidade do povo brasileiro que nos recebeu com muito carinho, que me outorgou o privilegio de estudar na universidade pública e gratuita e que, ainda, ofereceu-me a oportunidade de dedicar-me à pesquisa beneficiando-me com uma bolsa de estudos. Preciso aqui mencionar em particular à Universidade Federal de Santa Catarina e aos professores e alunos do Programa de Pós-Graduação em Relações Internacionais que tem me acolhido durante esses dois anos e tem me norteado nas minhas inquietações. Agradeço à minha orientadora Clarissa Franzoi Dri por ter aceitado esse desafio e, enormemente, as leituras aprofundadas de Gabriel Mendez e Analice Palombini que com esforço e dedicação contribuíram a melhorar a presente dissertação.

Também quero agradecer à nossa grande família gaúcha, aqueles que em tanto aportaram para nos ajudar a cumprir o nosso sonho de vir para o Brasil. Começando por Márcio Belloc e Sandra Fagundes e seguindo por toda a família Wolski de Oliveira que nos ofereceu um lar quando mais o precisávamos.

Aos meus amigos, especialmente ao *xat*, por se manter perto na distância e à minha família, principalmente aos meus pais Graciela e Roberto, quem nem sempre felizes com as minhas decisões, brindaram-me seu amor e seu apoio incondicional.

Impossível não expressar gratidão aos líderes latino-americanos dos 2000 que, nas diversas latitudes e com as suas particularidades, vieram propor e cumprir sonhos. Sonhos de dignidade, sonhos de verdade e sonhos de justiça. Eles resgataram, para a minha geração, a política como ferramenta de transformação e a solidariedade como ideal de construção comunitária. Também com todos aqueles que tiveram a decisão e

a coragem de expor as características reais deste punitivismo planetário arriscando, no caminho, as suas próprias vidas.

Finalmente, meu agradecimento para o Santiago por combater as minhas certezas, por me mostrar uma e outra vez que outro sentido é possível e por me ajudar a fazer uma realidade diferente. Sem dúvidas nada disto, especialmente a presente dissertação, teria sido imaginável sem ele.

“Todos nós vivemos sob uma lei marcial no que diz respeito às nossas comunicações”
Julian Assange (ASSANGE et al., 2013, p. 41–53).

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Lacaze, Laura Mabel
VIGILÂNCIA MASSIVA DE COMUNICAÇÕES : uma (ciber)Inquisição. Uma análise do discurso estadunidense no período 2001 - 2016 / Laura Mabel Lacaze ; orientadora, Clarissa Frazoi Dri - SC, 2017.
214 p.

Tese (doutorado) - Universidade Federal de Santa Catarina, Centro Sócio-Econômico, Programa de Pós Graduação em Relações Internacionais, Florianópolis, 2017.

Inclui referências.

1. Relações Internacionais. 2. Vigilância massiva de comunicações. 3. Securitização. 4. Criminologia crítica. 5. Segurança internacional. I. Frazoi Dri, Clarissa. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Relações Internacionais. III. Título.

RESUMO

O vazamento de um conjunto de documentos secretos por parte do ex-agente de inteligência estadunidense Edward Snowden possibilitou comprovar a existência de uma complexa estrutura de monitoramento encabeçada pelos Estados Unidos da América. Desenvolvida, fundamentalmente, a partir dos atentados do 11 de setembro de 2001 configura um esquema de vigilância da atividade digital de características massivas e que abrange uma porção substancial da população mundial, violando tanto a normativa internacional em matéria de direitos humanos quanto o princípio de soberania territorial. No discurso oficial estadunidense tal prática é apresentada como uma ferramenta essencial na manutenção da segurança internacional, seja na prevenção de atos terroristas, seja na neutralização de um conjunto mais ou menos preciso de ameaças diretamente ligadas ao uso de Tecnologias de Informação e Comunicações (TICs). A presente pesquisa visa problematizar esse discurso entendendo que se ordena segundo uma estrutura que nem esta determinada pelas particularidades das TICs (como intuitivamente caberia pensar), nem é especifica das narrativas em matéria de segurança internacional (como sugere o *marco analítico da securitização* dentro do campo das relações internacionais). Pelo contrario, afirma-se, que no que nele se reitera é a estrutura daquilo que no âmbito da criminologia crítica denomina-se *discurso do poder punitivo.* Segundo o trabalho de Zaffaroni, esta formação discursiva tem sua primeira versão condensada nos tempos da Inquisição Medieval e se articula em torno a uma série de noções que, resumidamente, consistem na necessidade de intervir antecipadamente para neutralizar uma ameaça que configura um risco superlativo, na asseveração de que a ameaça configura um estado emergencial que habilita a adoção de medidas de caráter extraordinário. Em definitiva, trata-se de um discurso que se estrutura em torno à afirmação de uma autoridade central como agente legítimo da tomada de decisões a qual ganha um controle ampliado da população através de mecanismos de vigilância. Em conseqüência, na presente dissertação tentou-se colocar em perspectiva histórica o discurso oficial estadunidense através de uma análise baseada em um conjunto de 152 documentos (conformado por: textos normativos,

por documentos doutrinários e por manifestações públicas) considerados representativos da conceituação oficial estadunidense a respeito do monitoramento das comunicações em um período que se estende entre finais de 2001 e meados de 2016. A intenção dessa análise foi a de identificar as particularidades com as quais esse discurso se apresenta no cenário atual enfatizando a coerência que, em termos de matriz argumentativa e das estratégias associadas, mantém respeito do discurso inquisitorial. Tal como no passado, trás um objetivo declarado de neutralizar um fenômeno que configura uma emergência conceitualmente focalizada em um grupo de supostos *periculosos*, hoje se avança em dispositivos orientados ao controle do conjunto populacional. É neste sentido que argumenta-se, salvando as diferenças, que a vigilância massiva e global de comunicações orientada pelo princípio de “saber tudo, coletar tudo e analisar tudo” configura uma (ciber)inquisição que se encaminha a um fichamento individual com base na atividade digital exercido a escala global e centralizado nas agências de segurança dos Estados Unidos as América.

Palavras-chave: Vigilância massiva de comunicações. Securitização. Criminologia crítica. Segurança internacional.

RESUMEN

La publicación de un conjunto de documentos secretos por parte del ex agente de inteligencia estadounidense Edward Snowden posibilitó comprobar la existencia de una compleja red de monitoramento encabezada por los Estados Unidos de América. Esta se desarrolló fundamentalmente a partir de los atentados del 11 de septiembre de 2001 y configura un esquema de vigilancia sobre la actividad digital de características masivas y que alcanza a una proporción sustancia de la población mundial violando tanto la normativa internacional en materia de derechos humanos como el principio de soberanía territorial.

En el discurso oficial estadounidense, tal práctica es presentada como una herramienta esencial para garantizar la seguridad internacional, sea a partir de la prevención de ataques terroristas o en la neutralización de un conjunto más o menos concreto de amenazas directamente identificadas como vinculadas con el uso de las Tecnologías de Información y Comunicaciones (TICs). La presente investigación procura problematizar ese discurso entendiendo que este se ordena siguienndo una estructura que no está determinada ni por las particularidades de las TICs (como podría pensarse de manera intuitiva) ni por las especificidades de las narrativas sobre seguridad internacional (como sugeriría el marco analítico de la securitización dentro del campo de las relaciones internacionales). Contrariamente se argumenta que lo que en él se reitera es la estructura de lo que en el ámbito de la criminología crítica se denomina *discurso del poder punitivo*. De acuerdo al trabajo de Zaffaroni, esta formación discursiva tuvo su primera versión condensada en los tiempos de la Inquisición Medieval y se articula en torno a una serie de nociones que, en resumen, consisten en la necesidad de intervenir anticipadamente para neutralizar una amenaza que configura un riesgo superlativo y en la afirmación de que tal amenaza configura un estado de emergencia que habilita a la adopción de medidas de carácter extraordinario. En definitiva, se trata de un discurso que se estructura en torno a la afirmación de una autoridad central como agente legítimo de la toma de decisiones la que, entre otros poderes, amplía su poder de control sobre la población a partir de la adopción de mecanismos de vigilancia.

En consecuencia, en la presente disertación se pretendió poner en perspectiva historia los discursos actuales acerca de la vigilancia masiva de comunicaciones para lo cual se realizó un análisis sobre un conjunto de 152 documentos (conformado por textos normativos, por documentos doctrinarios y por manifestaciones públicas) considerados representativos de la conceptualización estadounidense sobre la temática entre finales del año 2001 y mediados del 2016. El objetivo perseguido fue el de identificar las particularidades con las cuales ese discurso se presenta en la actualidad enfatizando la coherencia que mantiene respecto del discurso insquisitorial tanto en términos de la matriz argumentativa como de las estrategias asociadas. Tal como en el pasado, por tras de un objetivo declarado de neutralizar un fenómeno que configura una emergencia conceptualmente focalizada en un grupo de supuestos *peligrosos* se avanza en dispositivos orientados al control de la población en su conjunto. Es en este sentido que se argumenta, salvando las diferencias, que la vigilancia masiva y global de comunicaciones que se orienta por el principio de “saber todo, colectar todo y analizar todo” configura una (ciber)inquisición que se encamina a un fichaje individual basado en la actividad digital ejercido a escala global y centralizado en las agencias de seguridad de los Estados Unidos de América.

Palabras-clave: Vigilancia masiva de comunicaciones. Securitización. Criminología crítica. Seguridad internacional.

ABSTRACT

The leak of a set of secret documents by former US intelligence agent Edward Snowden made it possible to prove the existence of a complex monitoring structure headed by the United States of America. Developed mainly from the attacks of September 11, 2001, it constitutes a scheme of surveillance of digital activity with massive characteristics and that covers a substantial portion of the world population, violating both international human rights law and the principle of sovereignty territorial. In the official US discourse, such a practice is presented as an essential tool in the maintenance of international security, either in the prevention of terrorist acts or in the neutralization of a more or less precise set of threats directly linked to the use of Information and Communication Technologies (ICTs) . The present research aims to problematize this discourse by understanding that it is ordered according to a structure that neither is determined by the peculiarities of the TICs (as intuitively one would think), nor is it specific of the narratives in matters of international security (as suggested by the analytical framework of securitization within the field Of international relations). On the contrary, it is affirmed that what is reiterated in it is the structure of what in the scope of critical criminology is called the punitive power discourse. According to the work of Zaffaroni, this discursive formation has its first condensed version in the days of the Medieval Inquisition and is articulated around a series of notions that, in brief, consist in the necessity of intervening in advance to neutralize a threat that constitutes a superlative risk, in the Assertion that the threat constitutes an emergency state that enables the adoption of extraordinary measures. In short, it is a discourse that is structured around the affirmation of a central authority as a legitimate agent of decision-making which gains an expanded control of the population through surveillance mechanisms. As a result, in this dissertation we tried to place the official American discourse in a historical perspective through an analysis based on a set of 152 documents (conformed by: normative texts, doctrinal documents and public manifestations) considered representative of the official US conceptualization Monitoring of communications in a period extending between the end of 2001 and mid-2016. The intention of this analysis was to identify the particularities with which this discourse presents itself

in the current scenario emphasizing the coherence that, in terms of argumentative matrix And associated strategies, maintains respect for the inquisitorial discourse. As in the past, there is a stated goal of neutralizing a phenomenon that constitutes an emergency that is conceptually focused on a group of presumed perilous ones, nowadays one advances in devices oriented to the control of the population as a whole. In this sense, it is argued, saving the differences, that the massive and global surveillance of communications guided by the principle of "knowing everything, collecting everything and analyzing everything" constitutes a (cyber) inquisition that is directed to an individual file based on the Digital activity exercised on a global scale and centralized in the security agencies of the United States of America.

Keywords: Mass surveillance of communications. Securitization. Critical criminology. International security.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ACLU	União Americana pelas Liberdades Civis (American Civil Liberties Union)
BAH	Booz Allen Hamilton
CIA	Agência Central de Inteligência (Central Intelligence Agency)
COPRI	Instituto de investigações sobre a paz de Copenhague (Copenhagen Peace Research Institute)
CS	Conselho de Segurança da Organização das Nações Unidas
CSS	Serviço Central de Segurança (Central Security Service)
EUA	Estados Unidos da América
FBI	Agência Federal de Investigações (Federal Boureau of Investigations)
FISA	Lei de Vigilância da Inteligência Estrangeira (Foreign Intelligence Surveillance Act)
GCHQ	Central de Comunicações do Governo (Government Communications Headquarters)
HLT	Tecnologia da Linguagem Humana (Human language technology)
IP	Protocolo de Internet (Internet Protocol)
ISPs	Provedores de serviços de Internet (Internet Service Providers)
IXP	Pontos de intercâmbio de tráfego (Internet Exchange Points)
NSA	Agência de Segurança Nacional (National Security Agency)
ODNI	Escritório do Diretor de Inteligência Nacional (Office of the Director of National Intelligence)
ONU	Organização das Nações Unidas
OTAN	Organização do Tratado do Atlântico Norte
PDF	Formato de Documento Portátil (Portable Document Format)
PGP	Pretty Good Privacy
RI	Relações Internacionais
SSO	Divisão de Fontes Especiais (Special Sources Operations)

SIGINT	Inteligência de Sinais (Signals Intelligence)
SWIFT	Sociedade de Telecomunicações Financeiras Globais (Society for Worldwide Interbank Financial Telecommunication)

SUMÁRIO

1 INTRODUÇÃO

A difusão de um conjunto de documentos secretos do governo estadunidense, vazados pelo ex-agente de inteligência estadunidense Edward Snowden,[1] desencadeou um período de elevadas tensões na esfera diplomática. Estas tiveram, provavelmente, seu ponto de maior intensidade na obstrução do plano de voo do Presidente Morales do Estado Plurinacional da Bolívia, seguida da pretensão de vistoriar a aeronave por parte das autoridades dos Estados Unidos[2] (BOLÍVIA, 2013).

[1] Embora contasse com somente 29 anos de idade no momento de disponibilizar o conjunto de documentos que desvelaram a complexa rede de vigilância sobre as comunicações digitais, Edward Snowden já tinha percorrido uma longa carreira dentro dos serviços de segurança estadunidenses. No ano 2004, tentou formar-se como soldado das forças especiais, objetivo que se viu impossibilitado de atingir, presuntivamente, por um acidente no qual teria quebrado as duas pernas. Posteriormente, trabalhou como segurança no Centro de Estudos Avançados da Linguagem, da Universidade de Maryland (centro filiado ao Departamento de Defesa dos Estados Unidos). Em 2006 foi contratado pela Agência Central de Inteligência (CIA, sigla em inglês) para se encarregar da seguridade das redes da agência e, um ano depois, foi enviado em missão ao consulado estadunidense em Genebra. Segundo suas próprias declarações, a experiência na sede diplomática na Suíça, centro de escuta e espionagem operado pela CIA e pela Agência de Segurança Nacional (NSA, na sigla em inglês), marcaram-no profundamente. Sobre isto, declarou: "o que vi em Genebra realmente me desapontou sobre a forma como funciona o governo e seu papel no mundo" (SNOWDEN, 2013 apud GREENWALD; MACASKILL; et al., 2013, tradução livre). Snowden deixou a CIA e foi contratado pela Dell, empresa provedora da NSA e instalada no Japão. Posteriormente passou a integrar o plantel de outra empreiteira da agência: a firma Booz Allen Hamilton (BAH). Nesta, de "administrador de sistemas informáticos", Snowden passou a ser considerado um "estrategista cibernético" e "especialista em segurança informática". No mês de março de 2013, integra-se à equipe da BAH no Havaí – contexto que lhe possibilitou o acesso massivo a documentos secretos da agência, cujo vazamento planejou ao longo de vários meses (LEFÉBURE, 2014, p. 27–37). Maiores informações sobre a história de Edward Snowden e suas passagens pelas diversas agências e empreiteiras da comunidade de inteligência estadunidense podem ser consultadas, dentre outros, no livro *Os arquivos Snowden: A historia secreta do homem mais procurado do mundo* (HARDING, 2014) e no novo filme *Snowden* (STONE, 2016).

[2] Em julho de 2013, durante o percurso do voo de retorno de Evo Morales a Bolívia, após a participação em um evento de caráter oficial na Rússia, os governos de Portugal, França, Itália e Espanha revogaram a permissão de ingresso em seu espaço aéreo e uso de seus aeroportos (que previamente haviam concedido). Como resultado, o avião presidencial foi forçado a realizar um pouso imprevisto na Áustria, local no qual permaneceu parado por 13 horas. Durante esse período, o Governo boliviano denunciou pressões por parte dos Estados Unidos para inspecionar o avião, à procura de Snowden. As autoridades estadunidenses suspeitaram que o ex-agente

A relevância que esse vazamento assumiu na agenda política mundial correspondeu ao teor das práticas por ele registradas. Em particular, os documentos têm provado a existência tanto de uma complexa rede de espionagem seletiva sobre líderes políticos e alvos econômicos a nível global, quanto de um sistema de vigilância das atividades de pessoas e de instituições de características massivas e em escala planetária.

Em relação à primeira dimensão, nos diversos arquivos detalham-se as particularidades de um conjunto de programas orientados a espionar as atividades de Chefes de Estado da República Federal da Alemanha, da República Federativa do Brasil, da França e da República do México, dentre outros, como também do Secretário-Geral das Nações Unidas e as ações desenvolvidas em diversas repartições diplomáticas[3,4] (BALL, 2013; GREENWALD, 2016, p. 146–152).

A respeito da segunda, os documentos desvelaram que uma parte substancial da população mundial é sujeita a um esquema de monitoramento sobre sua atividade digital. Esta prática, referida no marco da presente dissertação pela noção de *sistema de vigilância massiva e global de comunicações,* compreende a execução rotineira de um conjunto de programas que contribuem à coleta, à análise, ao armazenamento e ao compartilhamento de informações digitais de forma massiva e em escala planetária. Tal sistema tem se estruturado, fundamentalmente nos últimos quinze anos e possibilita aos Estados Unidos da América (EUA) e a um conjunto seleto de

---

de inteligência viajasse na aeronave presidencial e, por este motivo, reclamavam inspecioná-la, configurando uma ação que, tal como expressara o vice-presidente boliviano Garcia Linera, constituiu uma "violação absoluta da Convenção de Viena que estabelece que os voos dos presidentes do mundo não podem ser obstruídos e gozam de imunidade" (BOLÍVIA, 2013, tradução livre).

[3] Uma série especial de documentos sobre este assunto foi publicada pelo site Wikileaks em julho de 2015, desvelando a estrutura de espionagem sobre funcionários do máximo nível e empresários do Brasil (ASSANGE; VIANA, 2015; WIKILEAKS, 2015a), da França (WIKILEAKS, 2015b), da Alemanha (WIKILEAKS, 2015c), do Japão (WIKILEAKS, 2015d), da União Europeia, da Itália e das Nações Unidas (WIKILEAKS, 2016).

[4] Destaca-se, neste sentido, a carta de agradecimento que o *secretário assistente de Estado* Thomas Shannon escreveu a Keith Alexander, na época diretor da NSA, para expressar sua "gratidão e [seus] parabéns pelo extraordinário apoio de inteligência de sinais" no marco da Quinta Cúpula das Américas. Assim, Shannon expressava que "[o]s mais de cem relatórios recebidos da NSA nos proporcionaram uma profunda compreensão dos planos e intenções dos outros participantes da Cúpula" (GREENWALD, 2016, p. 147).

estados nacionais, dentre os quais se destacam Grã-Bretanha, Canadá, Austrália e Nova Zelândia,[5] acesso a dados ligados às atividades de bilhões de pessoas e de instituições a nível global (GREENWALD, 2014).

Ambas as práticas suscitaram amplas condenações por parte de diversos atores do sistema internacional. No que se refere a pronunciamentos no âmbito diplomático, a República Federativa do Brasil foi ativa protagonista, fato influenciado a partir da dimensão particular que o esquema de espionagem tinha assumido no país.[6] Dentre outras reações,[7] a mandatária brasileira pronunciou-se abertamente a respeito por ocasião do evento de abertura da 68ª Assembleia Geral das Nações Unidas. Destacou a gravidade das ações reveladas, qualificando-as como contrárias ao direito internacional e aos "princípios que devem reger as relações entre os Estados" (ROUSSEFF, 2013). Adicionalmente, impulsionou a apresentação, em conjunto com a República Federal da Alemanha, de um projeto de Resolução[8] perante a Assembleia Geral da Organização das Nações Unidas (ONU), denunciando a prática de vigilância massiva como violadora dos direitos humanos (ONU, 2013a).

---

[5] Trata-se dos membros da denominada aliança dos *cinco olhos* (Five eyes) no marco da qual as diversas agências compartilham os dados coletados seguindo uma cooperação definida nos documentos como "abrangente" (NSA, 2014b). Uma descrição mais aprofundada sobre este assunto é realizada no segundo capítulo da presente dissertação.

[6] Os documentos manifestam que tanto a Presidenta da República Dilma Rousseff quanto seus principais assessores, constituíam alvos de um "esforço especial" de vigilância orientado a: "melhorar a compreensão dos métodos de comunicação e seletores associados" (GREENWALD, 2013, p. 148); somado a isto, também desvendaram a existência de um esquema de espionagem sobre as redes privadas da empresa Petrobras e do Ministério de Minas e Energia (LEFÉBURE, 2014).

[7] Poucas semanas após a publicação de informações quanto à estrutura do esquema de espionagem do qual diversas esferas do Estado foram alvos, a Presidente Rousseff decidiu cancelar a visita oficial programada aos Estados Unidos para o mês de outubro daquele mesmo ano (BRASIL, 2013). Adicionalmente, estimulou-se a organização no país da conferência *NETmundial* e a sanção do Marco Civil da Internet (Id., 2014), o qual visa regulamentar a atividade dentro do marco jurídico doméstico. Uma análise aprofundada a respeito do contexto de emergência dessa Lei e das suas principais características em relação à proteção da privacidade digital pode ser encontrada em Christofoletti (2015).

[8] Trata-se do Projeto de Resolução A/C.3/68/L.45, que contou com o apoio de Áustria, Estado Plurinacional da Bolívia, Equador, França, Indonésia, Liechtenstein, Peru, República Popular Democrática da Coréia, Suíça e República Oriental do Uruguai. Esta resolução foi aprovada em dezembro de 2013 e configura um dos múltiplos pronunciamentos que têm acontecido por parte de órgãos multinacionais a este respeito (ONU, 2013b).

Precisamente, as implicações destas revelações em matéria de normas internacionais foram um eixo singular do debate. Em linhas gerais, as manifestações salientaram que a lógica massiva que caracteriza o sistema resulta contrária aos tratados internacionais em matéria de direitos humanos, ao mesmo tempo em que a abrangência planetária lesa o princípio de soberania territorial (ONU, 2013b, 2014, PARLAMENTO EUROPEU, 2014a, b).

Analisadas desde a perspectiva dos seus objetivos declarados, estas duas práticas de monitoramento (a de espionagem seletiva e a da vigilância massiva) podem ser diferenciadas. De fato, tal discriminação foi formulada pelo Presidente Barack Obama por ocasião do anúncio de revisão dos programas de coleta de informações. Naquele pronunciamento, que constitui uma das primeiras respostas políticas articuladas após o vazamento, o então Presidente estadunidense traçou uma distinção entre aqueles programas especificamente direcionados a esquadrinhar as atividades de alvos políticos e econômicos e aqueles orientados a exercer uma vigilância de comunicações de características massivas. Ao passo que, a respeito do primeiro tipo, asseverou que se orientava a coletar informações a respeito das *intenções de outros governos,*[9] em relação ao segundo, argumentou que constitui um insumo fundamental para a manutenção da segurança doméstica e internacional (OBAMA, 2014, p. 6).

A apresentação da vigilância massiva como uma ferramenta fundamental na garantia da segurança remonta ao

[9] Em igual sentido, uma das comunicações internas da Agência Nacional de Segurança (NSA) estadunidense celebrava o êxito deste programa para auxiliar "a modelar a política externa dos Estados Unidos" (NSA, 2010c). Trata-se de uma edição da publicação interna da NSA SIDToday, na qual se destaca que, no marco da reunião do Conselho de Segurança (CS) da ONU que analisava a imposição de sanções sobre o Irã, a agência teve um papel fundamental "em manter a embaixadora dos Estados Unidos na ONU informada sobre como os outros membros do CS iriam votar". Neste sentido, na publicação são citadas declarações da embaixadora que afirmam que a agência "me ajudou a saber quando os outros Permreps [Representantes Permanentes] estavam dizendo a verdade (…) revelou seu verdadeiro posicionamento em relação às sanções (…) nos beneficiou nas negociações (…) e forneceu informações sobre os 'limites de negociação' de diversos países" (GREENWALD, 2016, p. 152).

momento mesmo de sanção da Lei Patriota[10] (EUA, 2001b). Tal como expressado no seu texto, esta norma teve como objetivo declarado o de oferecer "procedimentos aprimorados de vigilância"[11] para "prevenir e punir atos terroristas nos Estados Unidos e ao redor do mundo"[12] (EUA, 2001b, p. 2, tradução livre). Sancionada apenas seis semanas após os atentados de 11 de setembro de 2001, essa norma constituiu um dos elementos fundadores da estrutura do sistema de vigilância de comunicações estruturado pelos Estados Unidos, ao oferecer o marco legal, dentro do ordenamento jurídico desse país, para seu desenvolvimento posterior (FINLEY; ESPOSITO, 2014; LEFÉBURE, 2014). Isto porque, dentre outras questões, ampliou significativamente os poderes investigativos dos diversos órgãos de inteligência, levou a uma fusão nos esforços das agências de segurança e defesa (CAVELTY, 2007a, p. 105) e incrementou exponencialmente os recursos públicos destinados à área de segurança e defesa.

Invocando a necessidade de ferramentas para garantir a segurança doméstica e internacional, foi através da Lei Patriota, suas complementares e emendas,[13] que se consagraram alguns dos princípios que iriam modelar o sistema de monitoramento. Trata-se dos mesmos princípios que, anos depois, seriam apontados como violadores das normas internacionais em matéria de direitos humanos.

Com efeito, como salientado pelo *Relator Especial sobre a promoção e proteção dos direitos humanos e as liberdades fundamentais na luta contra o terrorismo das Nações Unidas*, "a dura realidade é que o uso das tecnologias de vigilância à grande escala realmente suprime completamente o direito à privacidade das comunicações via Internet"[14] (EMMERSON, 2014, p. 5, tradução livre). O Relator salientou que, tal como desenvolvida pelos Estados Unidos, a vigilância de comunicações vulnera os

[10] No marco da presente pesquisa, empregar-se-á o termo Lei Patriota em referência a: USA PATRIOT ACT: "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001' (EUA, 2001b)'.

[11] "Enhanced surveillance procedures".

[12] "to deter and punish terrorists acts in the United States and around the world".

[13] Destacam-se especialmente a Lei de Proteção de América (EUA, 2007) e Lei de Emendas da Lei FISA de 2008 (Id., 2008c).

[14] No original: "la dura realidad es que el uso de la tecnología de vigilancia a gran escala realmente suprime por completo el derecho a la privacidad de las comunicaciones en Internet."

princípios que o direito internacional exige para justificar qualquer ingerência no direito à privacidade como consagrado no Pacto Internacional sobre Direitos Civis e Políticos (ONU, 1966). Isto porque, argumenta, violam-se os princípios de necessidade e de proporcionalidade na ingerência nas comunicações privadas. Assim como também o de qualidade da Lei dado que já que permite a coexistência de estatutos de proteção assimétrica que garantem um tratamento diferenciado para nacionais e estrangeiros, e de salvaguardas previstos no Artigo 17 do Pacto.

Em outras palavras, o que se manifesta como contrário à normativa internacional em matéria de direitos humanos é aquilo que constitui a lógica central do esquema de vigilância global de comunicações articulada pelos Estados Unidos: o princípio da massividade. E é precisamente esta orientação, a qual tem se reiterado até o presente, que é identificada a nível oficial pelos EUA, e através dos pronunciamentos dos seus principais líderes políticos, como fundamental na garantia da segurança doméstica e na provisão de segurança em nível internacional.[15]

Em certo sentido, este constitui o ponto de início da pesquisa da qual emergiu a presente dissertação. Dada a complexidade do assunto abordado e a consequente multiplicidade de dimensões e de potenciais perspectivas de análise, o primeiro desafio esteve na definição de o percurso a seguir na pesquisa. Embora nem o façam de maneira linear nem expressem uma cronologia exata, as seções a continuação expressam parcialmente essa evolução e refletem de maneira geral as diversas decisões de enfoque e recorte adotadas ao longo da mesma.

A exploração inicial teve seu núcleo específico na indagação a respeito do processo perante o qual esta prática foi apresentada e legitimada como uma ferramenta na manutenção da segurança internacional. Seguindo as considerações daquilo

[15] Um dos últimos casos envolve a Agência Federal de Investigações Estadunidense (FBI, sigla em inglês), que, a princípios de 2016, solicitou à Justiça do país que forçasse a companhia Apple a desenvolver um software capaz de iludir os protocolos de segurança que preservam os dispositivos iPhone. Esta petição, avaliada pelo juiz e apelada pela companhia, vincula-se à investigação do denominado Massacre de San Bernardino, ocorrido em dezembro de 2015 e qualificado de atentado terrorista pela administração Obama. A posição oficial do executivo estadunidense, tal como expressada pelo Diretor do FBI, é precisamente que, "após o que terroristas fizeram a americanos inocentes", o desenvolvimento da investigação não pode ser interrompido por considerações ligadas à privacidade (FBI, 2016; LACAZE, 2016b).

que, no campo das Relações Internacionais, entende-se como *processo de securitização* (BUZAN et al., 1998) partiu-se do entendimento de que no âmbito da segurança internacional é recorrente a articulação de narrativas ligadas à ideia da urgência (principalmente da neutralização das ações terroristas) e práticas manifestamente violadora das normas internacionais (a vigilância massiva e global de comunicações).

Precisamente, como desenvolvido no primeiro capítulo, considera-se que o aporte principal do enfoque da securitização para o campo tem a ver com estudar a dinâmica da segurança internacional como emergente de um processo de natureza política. A ideia central por trás deste enfoque é que a configuração de determinadas problemáticas como assuntos ligados à segurança internacional, longe de ser o resultado de uma simples avaliação de caráter objetivo, constitui um processo orientado à legitimação de práticas concretas que resultam na adoção de medidas extraordinárias. Isto é, na justificação da quebra de normas e de procedimentos geralmente aceitos no plano internacional.

Assim, a análise discursiva é colocada pelos autores no centro da cena toda que identificam que o núcleo dos estudos no campo da Segurança Internacional está ligada aquilo que denominam a "política da ameaça existencial" (BUZAN et al., 1998, p. 27). Isto é, a articulação de narrativas em torno à configuração de um estado emergencial, ligado a um fenômeno que se apresenta como uma ameaça para a sobrevivência e a adoção de medidas de caráter extraordinário. Como se argumenta no mesmo primeiro capítulo o marco analítico da securitização, embora útil na identificação de algumas das regularidades presentes nos discursos a serem analisados, apresenta duas limitações para a presente pesquisa. De um lado em seu recorte analítico esse enfoque não coloca essas regularidades em perspectiva histórica, de outro não estabelece vinculações entre as particularidades da estrutura discursiva e as práticas concretas as quais se refere.

É neste ponto que se considerou útil complementar a analise seguindo aportes de outras áreas do conhecimento, principalmente do campo da criminologia critica, linha na qual referentes teóricos do âmbito da Segurança Internacional já tem incursionado (BIGO; TSOUKALA, 2008). Basicamente, o argumento central desenvolvido nessa seção final do primeiro

capítulo consiste em que aquelas características definidas pelos autores do marco analítico da securitização como específicas da *narrativa securitizadora* expressam, de maneira parcial, o que dentro de uma perspectiva criminológica crítica se identifica como próprio do *discurso do poder punitivo*. Essa estrutura remonta-se aos tempos do Império Romano e tem sua primeira versão condensada no *Malleus Maleficarum*, ou *O Martelo das feiticeiras* (KRAMER; SPRENGER, 2002), manual em torno do qual se organizou a função inquisitorial no século XV. Com base no estudo realizado por Zaffaroni[16] (2011a) daquela obra detalha-se, na segunda seção desse primeiro capítulo, o conjunto de reiterações identificadas como estruturais do discurso punitivo. Na exposição destas reiterações procurou-se enfatizar, não somente os pontos de conexão entre os elementos estruturais do discurso do poder punitivo e aquelas regularidades trabalhadas pelos teóricos da Securitização, mas também as relações entre esses componentes do discurso e as características do dispositivo de monitoramento em questão. Como abordado mais aprofundadamente no capítulo correspondente na tradição inaugurada por Foucault que serve de inspiração à criminologia crítica, argumenta-se que a lógica em torno da qual se organizam os discursos mantém estreita ligação com as práticas concretas às quais tais discursos se remetem. Assim, a diferença do enfoque securitizador, no qual o discurso é estudado exclusivamente como instância que segue sua própria dinâmica independente das particularidades das práticas que visa legitimar, este outro enfoque requer uma abordagem que integra ambas as esferas, sendo que a análise se orienta a enfatizar as estratégias às quais o discurso se vincula.

Essa, precisamente, é a orientação que se seguiu na elaboração dos Capítulos 2 e 3 da presente dissertação. No primeiro, detalham-se as características centrais do sistema de vigilância massiva e global de comunicações. Dado que constitui um assunto temporalmente recente e relativamente pouco abordado na produção acadêmica, a descrição se baseia

[16] Trata-se de Eugenio Raúl Zaffaroni, tratadista sobre Direito Penal de amplo reconhecimento na América Latina; ministro da Corte Suprema de Justiça Argentina entre os anos 2003 e 2014; desde o ano 2015, juiz da Corte Interamericana de Direitos Humanos; vice-presidente da Associação Internacional de Direito Penal. Merecedor, dentre outros, do prêmio Estocolmo de Criminologia no ano 2009; especificamente no Brasil, é coautor do manual de Direito Penal Brasileiro.

fundamentalmente nos documentos que conformam o denominado *acervo Snowden* e em algumas fontes secundárias de natureza jornalística. A descrição se orienta a abordar de maneira introdutória os arranjos institucionais e econômicos que servem de sua base de sustentação material, assim como a expor a lógica segundo a qual se organiza. Esta última, ilustrada por seus próprios protagonistas, pode ser resumida pelo princípio de "saber tudo, coletar tudo, analisar tudo". Em outras palavras, longe de se restringir a um conjunto restrito de potenciais *periculosos* ela se orienta a monitorar a atividade do universo populacional.

Finalmente, no Capítulo 3, detalham-se os resultados da análise sobre os discursos selecionados. A seção começa detalhando os procedimentos seguidos para a conformação da amostra, constituída por um conjunto total de 152 documentos que compreendem textos legislativos, documentos doutrinários e manifestações públicas dos máximos líderes do sistema político estadunidense. Nessa primeira seção também se detalham as orientações que se seguiram no momento de analisar os textos. A respeito disto, uma primeira aclaração para o leitor é que a leitura desses documentos se orientou a identificar o conteúdo específico que o discurso punitivo assume em relação à vigilância massiva de comunicações. Neste sentido, o estudo dos documentos da amostra não se orientou a procurar diferenças entre aquilo que foi declarado de maneira oficial e aquilo que foi comprovado através do acervo Snowden. Muito pelo contrário, o estudo tentou enfatizar aquelas instâncias nas quais se expressa, de maneira mais contundente, a coerência entre ambos.

Em consequência, no final desse terceiro capítulo detalham-se aqueles elementos que caracterizam o discurso oficial estadunidense a respeito da vigilância massiva de comunicações e as vinculações que, em termos funcionais, esses elementos mantêm com aqueles característicos do discurso inquisitorial tal como trabalhados no primeiro capítulo. Em resumo a ideia central é que se repete uma estrutura idêntica caracterizada pela identificação de um fenômeno como uma ameaça máxima que requer uma intervenção urgente e de caráter preventivo; pela existência de um agente central que se arroga a legitimidade de intervir e de escolher discricionariamente as alternativas de suas ações; pela

asseveração de que resulta imprescindível o emprego de meios extraordinários e de que em definitiva, tem de se articular dispositivos orientados ao monitoramento da população que possibilitem detectar um inimigo difuso e de ação coordenada. Em definitiva, é esta ideia que inspira o nome da presente dissertação. A noção da (ciber)inquisição tenta enfatizar que, embora as manifestas diferenças, longe de configurar uma abordagem *nova* orientada segundo as especificidades do conflito contemporâneo, a conceituação oficial estadunidense a respeito da vigilância massiva de comunicações não faz muito alem de reiterar aquilo que cinco séculos atrás, argumentava-se em relação à inquisição medieval.

2 NARRATIVA DA SECURITIZAÇÃO E DISCURSO DO PODER PUNITIVO

Tal como abordado na introdução, os documentos secretos vazados por Snowden possibilitaram comprovar a existência de um sistema de vigilância massiva de comunicações, assim como definir as suas características e o seu alcance.

Destacou-se, dentre outras questões, o fato de que se trata de uma prática desenvolvida e exercida de maneira rotineira por um conjunto de Estados Nacionais, principalmente os Estados Unidos da América, e que afeta os dados e as comunicações de pessoas e de instituições a nível global. Salientou-se, também, que se trata de uma prática que supõe violações massivas de normas e princípios internacionais. Finalmente, ressaltou-se que, tal como expressado pelos principais representantes do sistema político estadunidense, a racionalidade por trás de tal sistema é que ele constitui um insumo fundamental na luta contra fenômenos tais como o terrorismo e o crime organizado transnacional, que se apresentam como ameaças de caráter existencial.

O presente capítulo tem o propósito de desenvolver os aspectos fundamentais do marco interpretativo que auxiliará a análise a ser desenvolvida no terceiro capítulo. Para tal fim, foi articulado em duas seções. A primeira inicia com uma breve introdução dos estudos de Segurança Internacional dentro do campo das Relações Internacionais. Trata-se, em especifico, de uma breve descrição orientada a contextualizar a emergência do conceito de securitização. O foco é colocado na denominada Escola de Copenhague, que se tem destacado por argumentar que o núcleo dos estudos em matéria de Segurança Internacional está na denominada *política da ameaça existencial*.

Através do desenvolvimento do chamado *marco analítico da securitização*, os autores enquadrados nesta escola se diferenciaram por argumentar que a identificação de ameaças constitui um ato político pelo qual os diversos atores intervenientes têm de ser responsabilizados e que responde à intencionalidade de articular argumentos que sirvam à legitimação da quebra de normas ou, em outras palavras, à

justificação de práticas geralmente não aceitas. Esta primeira parte culmina com uma breve caracterização das limitações de dito esquema interpretativo em relação aos objetivos analíticos da presente pesquisa, em particular vinculados à performatividade como elemento chave para pensar o poder em relação ao discurso.

A segunda seção começa desenvolvendo os conceitos de *análise discursiva do poder* e do *discurso do poder punitivo* tal como elaborados por Foucault. A abordagem destes aspectos possibilita avançar no final, na subseção na qual, seguindo o trabalho de Zaffaroni, foca-se o aspecto da continuidade na evolução histórica do discurso punitivo. Em específico este autor elabora uma detalhada descrição das características estruturais deste discurso, com base na análise do Malleus Maleficarum, o compêndio que orientou o exercício da função inquisitorial no século XV.

Os trabalhos de vinculação de diversas perspectivas teóricas constituem sempre empreendimentos dificultosos. Frequentemente, e tal o caso desta pesquisa, as conceituações desenvolvidas pelos autores são resultados de processos históricos e políticos marcadamente diferentes, seguidos de interpretações divergentes sobre a própria *entidade* da produção acadêmica. Uma primeira ressalva, neste sentido, é que a intenção de construir o diálogo não deriva de uma pretensão de ocultar, de ignorar ou de obscurecer essas divergências, mas persegue o objetivo de salientar aqueles pontos comuns que podem fortalecer um olhar mais crítico e uma análise de maior profundidade sobre os discursos em matéria de segurança internacional.

Antecipando para o leitor, o argumento central do presente capítulo é o seguinte: aquilo que os autores da Escola de Copenhague (e outros junto com eles) denominaram *narrativa da securitização* expressa aquilo que Zaffaroni, seguindo a tradição da criminologia crítica, chama de *discurso do poder punitivo*. Portanto, não se trata de uma construção narrativa de características *novas*, própria do século XX ou do século XXI; tampouco constitui um fenômeno próprio da ordem da segurança internacional. Pelo contrário, tal como nos demonstra Zaffaroni, trata-se de uma prática que, surgida no marco do Império Romano, inspirou todos os processos inquisitoriais da

humanidade e tem-se incorporado à lógica segundo a qual se regula o conflito social de forma contínua a partir do século XV.

Em consequência, a segunda seção culmina com o detalhamento das características do discurso do poder punitivo, enfatizando, sempre que possível, os pontos de ligação entre estas e as identificadas pelos autores da Escola de Copenhague como próprias da *narrativa da securitização.* Ditas características discursivas, ou regularidades, são, finalmente, empregadas como categorias analíticas dos pronunciamentos sobre vigilância massiva de comunicações no segundo capítulo da presente dissertação.

2.1 O MARCO ANALÍTICO DA SECURITIZAÇÃO: A POLÍTICA DA AMEAÇA EXISTENCIAL COMO NÚCLEO DOS ESTUDOS DE SEGURANÇA INTERNACIONAL

> Nossa afirmação é que é possível estudar a prática ligada a este conceito de segurança nas relações internacionais (que é distinto de outros conceitos de segurança) e encontrar um padrão característico com uma lógica interna. Se colocarmos a sobrevivência de unidades e princípios coletivos - a política da ameaça existencial - como o núcleo definidor dos estudos de segurança, temos a base para aplicar a análise de segurança a uma variedade de setores sem perder a qualidade essencial do conceito[17] (BUZAN et al., 1998, p. 27, tradução livre).

O grande fio condutor que orienta a tradição que comumente se denomina de estudos sobre Segurança internacional é o de reclamar, para o âmbito civil, o debate referente às reflexões sobre assuntos relativos à paz e à segurança, mas também à guerra e à estratégia no nível

[17] No original: "Our claim is that it is possible to dig into the practice connected to this concept of security in international relations (which is distinct from other concepts of security) and find a characteristic pattern with an inner logic. If we place the survival of collective units and principles—the politics of existential threat—as the defining core of security studies, we have the basis for applying security analysis to a variety of sectors without losing the essential quality of the concept".

internacional (SAINT-PIERRE, 2011). Em torno deste princípio, que lhes confere uma relevância política fundamental, agrupam-se diferentes leituras da realidade que orientam a reflexão dos diversos referentes que, desde a historiografia, são reconhecidos como conformadores desta área do conhecimento.

Não se pretende, nestas linhas, reproduzir um debate sobre a evolução deste campo do conhecimento, o qual carece por completo de consensos (BUZAN; HANSEN, 2009), tal como acontece nas diversas áreas da produção acadêmica. O que se tentará fazer, ao invés, é salientar algumas questões introdutórias que servem para contextualizar a emergência do marco analítico da securitização.

Na sua reconstrução da evolução histórica do campo, Walt (1991, p. 213–214) argumenta que os primeiros estudos expressivos na área em questão foram elaborados no período do entre guerras, em um contexto no qual a contribuição civil na área era frequentemente desalentada e, em consequência, os trabalhos eram afetados pela falta de informação disponível. O autor relata que a produção teórica se incrementou significativamente após a Segunda Guerra Mundial, mas a consolidação definitiva do campo aconteceu após a derrota estadunidense no Vietnã.[18] Neste ponto, argumenta que se produziu uma integração entre duas linhas de reflexão relativamente diferenciadas. Estas podem ser sintetizadas como sendo uma diretamente envolvida com os *estudos para a paz* (principalmente ligada a acadêmicos da Europa) e outra voltada especificamente à reflexão sobre estratégia nacional (representativa do desenvolvimento do campo nos Estados Unidos).

Nucleados no Instituto de investigações sobre a paz de Copenhague (COPRI, na sigla em inglês), o trabalho dos autores do livro *Segurança: um novo marco de análise*[19] (BUZAN et al., 1998), obra chave no desenvolvimento do conceito de securitização, insere-se dentro dessa primeira tradição. A

[18] Em uma linha semelhante, Saint-Pierre (2015, p. 9) argumenta que os acontecimentos de 11 de setembro de 2001 tiveram, por sua vez, um impacto positivo para as Relações Internacionais (RI) no fortalecimento da área dos estudos de Segurança. Isto porque estes eventos deram "uma nova vitalidade às pesquisas e análises a uma área que, embora tivesse dado origem à disciplina das RI, estava um pouco esquecida e até estigmatizada na academia".

[19] No original: Security: a new framework for analysis.

publicação do livro se enquadra no contexto do fim da denominada *Guerra Fria* que, no campo, expressou-se em um amplo debate em torno das mudanças e das continuidades na dinâmica dos conflitos e sobre a própria centralidade do Estado no sistema internacional.

É em referência a esse estado do debate que, na introdução do seu livro, Buzan, Wæver e Wilde (1998, p. 3–5) argumentaram que os estudos de segurança internacional estruturavam-se em torno a duas visões. À primeira, denominaram de *tradicionalista*, por condensar conceituações ligadas a manter o foco no Estado e na agressão externa como eixos estruturantes do campo, sendo, nas palavras dos autores, uma *visão velha de cunho militar e estadocêntrica.* A segunda foi chamada de *ampliadora* – categoria que, segundo o critério dos autores, condensou as posições ligadas ao fato que a dinâmica da segurança teria assumido um caráter multidimensional produto das mudanças acontecidas no cenário internacional.[20,21]

O argumento central por trás da caracterização feita pelos autores é que, até a introdução do marco analítico da securitização, o debate acadêmico dominante na área discorria entre posições favoráveis e contrárias à ampliação do espectro de fenômenos e de atores inclusos no domínio do campo da segurança internacional, sob uma conceituação centrada na análise de um conjunto de fenômenos e transformações de caráter *objetivo*.

Além das considerações a respeito da originalidade destes argumentos, o fato é que a emergência do marco analítico da securitização pode ser entendida como representativa de uma corrente de estudos que surgiram neste contexto e que identificaram seu foco analítico no estudo mesmo do processo perante o qual diversos temas são incorporados ao debate sobre segurança. Rejeitando a perspectiva perante a qual a política de segurança se apresenta como reação simples a ameaças (sejam estas objetivamente estabelecidas e, portanto, completamente independentes do sujeito ou subjetivamente percebidas), estes

[20] Saint-Pierre (2011, p. 410) argumenta que, de fato, a cristalização da ideia das *novas ameaças* (correlato do conceito de segurança multidimensional) desenvolveu-se no contexto do Conselho de Segurança das Nações Unidas, no marco da chamada Comissão Palme, no ano 1983.

[21] Uma reconstrução dos debates no campo da Segurança Internacional na época pode ser consultada em Huysmans (2009).

enfoques iniciam um debate acadêmico que argumenta que a conformação dessa agenda, a transformação de temas diversos em assuntos de segurança, constitui o resultado de um processo de natureza política.

Como salienta Huysmans (2009, p. 4), na época, as posições que destacavam a impossibilidade de considerar as ditas *ameaças* apenas como um dado objetivo que emerge do cenário internacional se orientaram, fundamentalmente, por tentar salientar sua característica de fato política, assim como por colocar no centro da análise o papel que as próprias agências de segurança têm na sua constituição como fenômenos da agenda da segurança internacional.

Precisamente, o ponto fundamental do marco analítico da securitização, tal como formulado no âmbito da Escola de Copenhagen, é que a configuração dos temas que são identificados como assuntos relativos à segurança está condicionada pelas ações daqueles com maior capacidade de influência[22] na cena internacional. Neste sentido, os autores salientam que a *securitização* de um assunto, isto é, o processo perante o qual fenômenos específicos são apresentados como ameaças existenciais que requerem medidas de tipo extraordinário, constitui um fenômeno político com consequências concretas toda vez que resultam em que o ator *aja* de forma diferenciada (BUZAN et al., 1998, p. 30). Em palavras dos autores:

> Nosso enfoque tem o mérito fundamental de conceituar a segurança como um rotulado pelo qual atores podem ser responsabilizados, mais do que como um enquadramento objetivo de ameaças. Então, embora a multidimensionalidade do enfoque

[22] Tal como manifestado, a pesquisa dos autores é conduzida por duas inquietações: a primeira tem a ver com as implicações políticas da tendência de ampliação das categorias de fenômenos abordados desde a óptica da segurança internacional, que constitui o foco da presente seção. A segunda questão, que fica fora do escopo da presente dissertação, tem a ver com a existência de dinâmicas de segurança geograficamente diferenciadas. Sobre este último ponto, os autores desenvolvem a teoria dos complexos de segurança definidos como zonas geograficamente coerentes que se definem por padrões de interdependência na dimensão da segurança e que têm, provavelmente, seu tratamento mais acabado no livro Regions and powers (BUZAN; WÆVER, 2003).

> habilite a proliferação da securitização, seu construtivismo oferece os meios para questionar e politizar cada instância específica[23] (BUZAN et al., 1998, p. 212, tradução livre).

É por isto que a publicação do livro está decididamente orientada pelo argumento de que é preciso operar uma transformação do enfoque mesmo com o qual os assuntos de segurança estavam sendo refletidos no âmbito acadêmico. Para os autores, argumentar que a segurança constitui um fenômeno socialmente construído (ao invés de objetivo) implicou questionar o próprio escopo de problemas abordados pelos teóricos do campo.

Na visão dos autores, rejeitar o argumento em torno à existência de uma configuração *real* (objetiva e externa) das ameaças significou também rechaçar a orientação dos estudos de segurança centrados na consideração do procedimento de sua identificação, na análise de suas características e na avaliação da pertinência da sua administração por parte dos decisores de políticas. Não existindo referenciais objetivos para enquadrar a questão, a eleição deve ser justificada, argumentam, pela conveniência e pelas suas consequências políticas (BUZAN et al., 1998, p. 203–211).

Em concreto, os teóricos da Escola de Copenhague propõem pensar a agenda da segurança internacional como emergente de um processo de construção social, de tipo intersubjetivo, caracterizado pelo apelo a um tipo particular de formulação narrativa. Em consequência, argumentam que o foco dos estudos de segurança internacional teria que se constituir em torno daquilo que denominam a *retórica da ameaça.* Esta é chamada, ao longo da obra, de forma alternativa como: *estrutura retórica da securitização, gramática da segurança*, *construção do enredo*, *política da ameaça existencial* e *política do pânico*, dentre outras formulações.

---

[23] No original: “Our approach has the basic merit of conceptualizing security as a labeling for which actors can be held responsible rather than an objective feature of threats. Thus, although the multisectoralism of the approach enables a proliferation of securitization its constructivism delivers the means for questioning and politicizing each specific instance”.

Na visão desses autores, o processo de securitização tem de ser analisado como um processo integral, com intervenção de uma série de elementos cujo estudo se orienta a expor suas características com o objetivo político de propender à mudança do estado atual das coisas (BUZAN; WÆVER, 2003, p. 204). Para interpretar dito processo, os autores adotam a conceituação de Austin[24] sobre os *enunciados performativos* e a aplicam ao campo da segurança internacional. Assim, é com base nesta conceituação que os autores elaboram um dos seus argumentos centrais: que o caráter socialmente construído do fenômeno da segurança internacional é resultado da característica performativa dos enunciados sobre o tema.

Austin desenvolve o conceito de *enunciados performativos* principalmente no seminário de 1955, intitulado "Como fazer coisas com palavras"[25] (AUSTIN, 2009). Neste, define tais enunciados como um tipo específico de *discurso* ou *declaração*[26] cuja característica principal é a de que a própria emissão da declaração constitui uma ação. Argumenta que sua identificação tem de se realizar através do contexto no qual se insere sua formulação, não existindo, portanto, critérios gramaticais que o caracterizem.

Nesta mesma linha, Austin salienta que, enquanto enunciados, eles não devem ser considerados segundo o critério proposicional que classifica entre verdadeiro e falso; sua avaliação deve ser no sentido deles serem *exitosos* ou *não exitosos.* Sempre segundo Austin, as condições para o *funcionamento* de um enunciado performativo são de duas ordens: a primeira vinculada à observância de um procedimento convencional específico, e a segunda, ligada ao contexto no qual se inscrevem os atores envolvidos. Em outras palavras, é possível *fazer coisas com palavras* sempre que o enunciado seja proferido de uma forma específica, em um contexto determinado e pelas pessoas adequadas.

Aplicando os conceitos de Austin à problemática da segurança, Buzan, Wæver e Wilde conceituam a *securitização* como o resultado de um processo que envolve um rito centrado

[24] Trata-se de John Langshaw Austin, linguista de origem britânica que, após atuar no serviço de inteligência desse país, tornou-se professor da disciplina de Filosofia Moral na Universidade de Oxford.
[25] No original: "How to do things with words".
[26] No original: utterance.

em um discurso específico, que é enunciado por um ator em particular e orientado a provocar a aceitação de práticas concretas por parte de uma audiência determinada. Respeitando a formulação de Austin, os autores da Escola de Copenhague argumentam que o *ato de fala da segurança* não se define pela inclusão da palavra *segurança* nos enunciados. Pelo contrário, apontam que ele se define por uma lógica composta por:

a. *Um discurso centrado na emergência de uma ameaça existencial, que invoca a necessidade de intervir conforme um padrão de regras diferenciadas*: Segundo os autores, o discurso securitizador constitui uma narrativa centrada na identificação de um fenômeno que ameaça a sobrevivência. Argumentam que um tema será conceituado como um assunto de segurança após ser apresentado exitosamente como uma ameaça existencial a um objeto referente determinado. Neste sentido, o discurso securitizador é entendido pelos autores como uma lógica narrativa aplicável a um amplo conjunto de fenômenos e de objetos referentes. Em outras palavras, é entendido como uma estrutura orientada à produção de uma leitura sobre o fenômeno cujas particularidades, cujo conteúdo, mudará em relação às características específicas do dito objeto referente. Segundo os autores, tal estrutura narrativa observa as seguintes características:

   a.1. Aponta-se a existência de um fenômeno que constitui um risco superlativo. A narrativa se orienta a *hierarquizar*[27] o assunto em relação ao conjunto de fenômenos diversos potencialmente perigosos, com o objetivo de afirmar sua absoluta prioridade enquanto ameaça. Com base nas análises textuais de Wæver, afirmam que um fenômeno é designado como um assunto de segurança internacional porque foi possível apresentá-lo como de maior importância

[27] Nos últimos anos, os autores cunharam o termo *macrossecuritização* para se referir a um grau adicional de hierarquização de um assunto sobre os fenômenos restantes. Embora a mudança terminológica, considera-se que esse novo conceito não altera o essencial da lógica do processo para os fins da presente análise toda vez que, como argumentam os própios autores: s. "As macrossecutizações são definidas pelas mesmas regras que aplicam as restantes: a identificação de uma ameaça existencial sobre um objeto referente e o apelo à adoção de medidas extraordinárias" (BUZAN; WÆVER, 2009, p. 257).

que outros, estabelecendo, assim, seu caráter absolutamente prioritário (BUZAN et al., 1998, p. 24).

a.2. Enquanto ameaça para a sobrevivência, pondera-se que dita intervenção tem de se efetuar de maneira urgente e ser orientada à neutralização. Os autores identificam como próprio desta narrativa securitizadora o apelo a uma dramatização dos eventos, com o objetivo de sustentar o argumento a respeito da urgência na adoção de ações de resposta. A retórica aponta a configuração de um estado emergencial através de formulações do tipo: "porque se o problema não for administrado agora, será tarde demais e não existiremos para remediar nossa falha"[28] (BUZAN et al., 1998, p. 26, tradução livre).

a.3. Argumenta-se que esse fenômeno configura um risco potencial que afeta um ideal. Neste sentido, como salienta Wæver, apela-se de forma recorrente à equiparação entre o conceito de seguridade e a ideia de um estado *livre de ameaças*[29] (WÆVER, 1995, p. 51). De fato, os autores mencionam uma série de valores tipicamente apresentados como em situação de risco pelos diversos atores no âmbito da segurança internacional. Tais valores, a saber, soberania, riqueza, identidade e sustentabilidade, dentre outros, constituem um dos elementos característicos da subdivisão do mundo da segurança em subsetores específicos.

b. *Enunciado por um ator securitizador e orientado a uma audiência:*

b.1. O ator em questão reclama para si o direito de intervir: Os autores reconhecem como outra característica central do processo securitizador que a autoridade em questão invoque para si o direito de intervir (BUZAN et al., 1998, p. 26), manifestando que esta ação se realiza *em nome e em referência a uma coletividade* (BUZAN; WÆVER, 2009, p. 255).

b.2. Afirma que o êxito da intervenção só pode se garantir através da adoção de medidas de caráter extraordinário. Tal como salienta Wæver (1988, p. 4), tendo-se estabelecido a justificativa para a ação, as suas características específicas

[28] No original: "because if the problem is not handled now it will be too late, and we will not exist to remedy our failure".
[29] No original: "freedom from threats".

> desta serão definidas em última instância pela autoridade em questão. Em outras palavras, para os autores, constitui um elemento característico da securitização de um assunto a habilitação de práticas de definição eminentemente discricionária, tais como "a determinação de prioridades políticas e a justificação do uso da força, a intensificação dos poderes executivos, a invocação do direito ao segredo e outras medidas extraordinárias"[30] (BUZAN et al., 1998, p. 208, tradução livre).

Cabe salientar que, dentro deste enfoque, a articulação e a formulação do discurso não constituem um ato, mas um *intento securitizador*. Seguindo a conceituação de Austin, os autores da Escola de Copenhague argumentam que o êxito no processo de securitização, o efetivo cumprimento da performatividade do enunciado, depende da capacidade do ator (securitizador) em conseguir que esse discurso seja aceito pela audiência relevante. Ainda, conceituam essa aceitação como resultado de uma *negociação*, na qual, ao mesmo tempo em que a audiência aceita a narrativa de que a ameaça não pode ser combatida seguindo as regras convencionais, também aceita a quebra de ditas normas tendo o medo como motivação fundamental[31] (BUZAN; WÆVER, 2003, p. 26).

Assim, longe de se construir sob bases objetivas, a conformação da agenda de segurança internacional, seguindo este enfoque, funda-se na formulação (exitosa) de enunciados de caráter performativo. É essa característica performativa, própria dos enunciados relativos à segurança, o que lhes outorga consequências concretas em termos de poder, a saber, a legitimação de determinadas práticas de intervenção específicas por parte de atores concretos que, de outra forma, não seriam toleradas. É precisamente este o entendimento por trás da proposta dos autores de considerar a política da ameaça

---

[30] No original: "setting political priorities and justifying the use of force, the intensification of executive powers, the claim to rights of secrecy, and other extreme measures".

[31] No original: "The security act is negotiated between securitizer and audience (…) Typically, the agent will override such rules, because depicting a threat the securitizing agent often says someone cannot be dealt with in the normal way (…) the fear that the other party will not let us survive as a subject is the foundational motivation for the act".

existencial como núcleo definidor dos estudos no âmbito da segurança internacional (BUZAN et AL, 1998, p. 27).

Seguindo a conceituação de Austin, a importância política do discurso, suas consequências concretas em termos de poder, vincula-se ao êxito na performatividade. É por isto que, uma vez detalhadas as características fundamentais da narrativa securitizadora, especialmente com base nas análises textuais de Wæver,[32] a tradição analítica desenvolvida dentro deste enfoque se centra nos elementos que perfazem o processo de *negociação* ou, em termos mais gerais, o seu mecanismo de aceitação.[33]

Decorrente da análise baseada no conceito de performatividade, o discurso emerge como ferramenta de poder, na medida em que, através dele, é possível construir entendimentos que levem à justificação de determinados eventos. Toda vez que *quem fale seja quem pode falar* e que o faça conforme ao rito, a característica de performatividade dos enunciados habilitaria a possibilidade de, perante a narrativa em torno à retórica da ameaça existencial, enquadrar um assunto específico como uma problemática de segurança internacional e legitimar práticas de intervenção de caráter extraordinário.

Autores como McDonald argumentam que, precisamente, este é um elemento chave para compreender o êxito de tal perspectiva dentro dos estudos de segurança. O autor argumenta que a ênfase nas condições de êxito acabou resultando em que o marco da securitização se tornasse uma elevada capacidade explicativa, para a qual o foco da análise está na "forma do ato, na posição do falante e na ressonância histórica das *ameaças* específicas" (MCDONALD, 2008, p. 570, tradução livre, ênfase no original).

A reflexão, então, é focada nos elementos e nos mecanismos através dos quais o sentido do discurso muda em relação à situação do enunciador – trata-se de uma espécie de

[32] No original: "form of the act, position of speaker and historical resonance of particular 'threats'".

[33] De fato, outras correntes, como a *teoria dos marcos de ameaça*, têm trabalhado desenvolvendo marcos interpretativos que estudam de forma muito mais detalhada essas condições do contexto. Como se depreende da revisão elaborada por Cavelty (2007a, p. 24–38), ditos desenvolvimentos teóricos se pautam por preencher os pontos identificados como lacunas dentro do esquema analítico da securitização, mas não alteram sua lógica central, que consiste em identificar, como aspecto fundamental em relação ao estudo do discurso, o caráter performativo dos enunciados.

análise *pragmática* do discurso, nos termos de Foucault (2009, p. 82). Em contrapartida, a lógica que orienta a narrativa, as particularidades que apresenta essa estrutura, a configuração dos enunciados e as relações entre eles, assim como as suas ligações com as características desses meios extraordinários, são situadas longe do foco analítico.

Neste sentido, os teóricos da Escola de Copenhague articulam um enfoque que considera efetivamente o papel do discurso no âmbito da segurança internacional, mas cuja incorporação se dá exclusivamente como fator de construção de legitimidade. Toda vez que a relevância política do discurso depende, segundo essa perspectiva, da capacidade de executar *ações com palavras* constitui uma ferramenta de poder toda vez que através do discurso se constrói aceitação voluntária de práticas concretas, sendo, porém, tal discurso, pensado em definitivo como uma dimensão separada dessas mesmas práticas.[34]

É precisamente neste ponto que a presente dissertação segue uma orientação alternativa. Em termos gerais, e seguindo a Foucault, o discurso é pensado como parte de uma prática, de um dispositivo, e não como mero mecanismo da sua legitimação. O estudo exige, portanto, ligar de forma indissolúvel a lógica que orienta o discurso às práticas concretas às quais se refere. Como adiantado na introdução, a presente pesquisa se orienta não somente a listar um conjunto de regularidades presentes nos discursos a respeito do monitoramento massivo de comunicações, mas a vinculá-los logicamente com a própria prática da vigilância.

Como se desenvolve nas seções seguintes da presente pesquisa, isto remete a dois objetivos: o primeiro é o de mostrar que aqueles elementos que os autores da Escola de Copenhague caracterizaram de narrativa *securitizadora*

[34] Essa identificação do estudo do discurso com o "meramente simbólico" se estende a outros autores referentes de enfoques muito mais críticos no âmbito da segurança internacional. Em particular, Huysmans (2009) aponta que a maioria dos estudos discursivos no âmbito da segurança são restritos à considerações a respeito daquelas "estruturas culturais profundas" que predispõem as pessoas a se vincular com outras seguindo um conjunto de padrões predefinidos tais como: bom ou mal, amigos ou inimigos. Em outras palavras, para o autor, estas análises focam exclusivamente no "poder estrutural da linguagem e da representação simbólica" negligenciando as diferencias existentes em termos das capacidades que os diversos atores tem em matéria de "securitização de um fenômeno".

constituem as regularidades próprias do discurso do poder punitivo. Afirma-se, portanto, que esta estrutura argumentativa nem é própria da lógica da segurança internacional, a diferenciar, como fazem os autores da Escola de Copenhague, do contexto de segurança doméstica (BUZAN et al., 1998, p. 21), nem constitui uma novidade argumentativa emergente no contexto da pós Guerra Fria. Pelo contrário, afirma-se que esta expressa a lógica segundo a qual se estruturam as respostas ao conflito social e que, inclusive, remonta a períodos históricos que antecedem o surgimento do Estado Moderno. O segundo é o de interpretar os discursos a respeito da vigilância massiva sob o prisma do desenvolvimento concreto da própria prática, salientando que, embora a emergência de novos padrões tecnológicos possibilite na atualidade o desenvolvimento de novas ferramentas de monitoramento, a lógica que a orienta é idêntica àquela sob a qual se estruturou a prática inquisitorial cinco séculos atrás.

Considera-se que este constitui o principal aporte dos desenvolvimentos no campo da denominada *criminologia crítica*, inspirados na análise dos dispositivos de saber-poder de cunho foucaultiano, para os estudos no âmbito da segurança internacional.[35] Como se detalha a seguir, no discurso do poder punitivo, a questão da ameaça, embora desde uma perspectiva diferente, também está situada no centro do debate. Expressa-se agora sob a forma do risco ou da periculosidade, mas continua orientando a narrativa em idêntica direção: a racionalização de práticas seguindo o princípio da neutralização ou prevenção.

A seção seguinte começa então com a apresentação de algum dos elementos chaves na conceituação da prática discursiva para Foucault. Em seguida, é abordada a questão do discurso do poder punitivo, que desemboca na descrição das

[35] Autores como Huysmans (2009) e Campbell (BIALASIEWICZ et al., 2007; CAMPBELL, 1992) têm localizado o discurso no centro da cena e, particularmente, dos efeitos que o ordenamento da linguagem tem sobre ação e a reflexão. O primeiro argumenta em relação à necessidade de considerar o *poder da representação*, enquanto o segundo adverte que *o mundo não pode ser pensado por fora da linguagem.* Em particular, uma coletânea publicada no ano 2008 intitulada *Terror, Insecurity and Liberty Illiberal practices of liberal regimes after 9/11* se orienta neste sentido analítico e tem como objetivo central integrar a produção dos *campos* das Relações Internacionais, da Ciência Política, da Sociologia e da Criminologia (TSOUKALA; BIGO, 2008). Vários destes conceitos são retomados na seção seguinte.

suas características centrais seguindo a análise de Zaffaroni sobre o discurso inquisitorial, com a qual se encerra o presente capítulo.

2.2. A AMEAÇA NO DISCURSO DO PODER PUNITIVO

> Onde está, então, a importância política do poder punitivo? O elemento chave foi identificado por Michel Foucault anos atrás: o poder punitivo não se exerce sobre os que estão presos, mas sobre os que estamos soltos porque é *poder de vigilância*[36] (ZAFFARONI, 2011a, p. 506, tradução livre, ênfase no original)

Como salientado, a presente seção está orientada a detalhar e explicar as características estruturais do discurso do poder punitivo. Características que, por sua vez, são empregadas como categorias analíticas para o estudo dos pronunciamentos em matéria do sistema de vigilância massiva de comunicações no segundo capítulo da presente dissertação.

Para tal fim o trabalho se organizou em duas subseções. A primeira aborda, de maneira meramente introdutória, aqueles conceitos que se revestem de maior relevância para compreender a análise do discurso sob a perspectiva de uma *crítica política do saber*. Fundamentalmente, detalha-se aquilo que, no marco da presente análise, entende-se por *discurso.* Seguindo o caminho traçado por Foucault, abordam-se as noções de dispositivo saber-poder e de formação discursiva como base para introduzir o conceito de discurso do poder punitivo, central na perspectiva criminológica crítica. Entende-se por *criminologia crítica* a tradição que incorpora a análise do exercício do poder repressivo no campo dos estudos criminológicos. Também chamada de *criminologia da reação social*, remonta à década de 1960 e tem em Alessandro Baratta uma das suas figuras de referência. Seu trabalho, voltado a

[36] No original: "¿Dónde está, pues, la importancia política del poder punitivo? La clave la dio hace años Michel Foucault: el poder punitivo no se ejerce sobre los que están presos, sino sobre los que estamos sueltos pues es poder de vigilancia."

mostrar que o poder punitivo é estruturalmente seletivo, que funda sua seleção na base de estereótipos e que persegue pessoas ao invés de simplesmente punir ações, é considerado uma instância de transformação no campo criminológico. Neste sentido, como argumenta Andrade[37] (2013), abre-se uma nova criminologia, a qual passa a estudar o funcionamento efetivo do aparelho punitivo, as condições de criminalização.

Na segunda subseção, finalmente, chega-se à descrição analítica do discurso demonológico ou inquisitorial como expressão do discurso do poder punitivo. Com inspiração no aporte de Zaffaroni, nesta se apresentam as características de tal formação discursiva, as quais conformam as categorias de análise empregadas no capítulo seguinte.

2.2.1 A crítica política do saber e o discurso do poder punitivo

> No meu ver, o problema que está em jogo é o seguinte: no fundo, não são precisamente os dispositivos de poder [...] o ponto a partir do qual devemos poder assinalar a formação das práticas discursivas? Como podem esse ordenamento do poder, essas táticas e estratégias do poder, dar origem a afirmações, negações, experiências e teorias, em suma, a todo um jogo da verdade?[38] (FOUCAULT, 2005, p. 30, tradução livre).

> Como o punitivo é a chave do poder planetário, o que se diz a seu respeito não é resultado de uma busca ingênua de conhecimentos, de curiosidade científica

[37] Trata-se da Professora Vera Pereira Regina de Andrade, Professora titular da Universidade Federal de Santa Catarina, atuando nos cursos de graduação e pós-graduação de direito, responsável pela área de criminologia e direitos humanos.

[38] No original: "A mi juicio, el problema que está en juego es lo siguiente: en el fondo, ¿No son justamente los dispositivos de poder, con lo que la palabra *poder* aún tiene de enigmático y será preciso explorar, el punto a partir del cual debemos poder asignar la formación de las prácticas discursivas? ¿Cómo pueden ese ordenamiento del poder, estas tácticas y estrategias del poder, dar origen a afirmaciones, negaciones experiencias, teorías, en suma, a todo un juego de la verdad?"

> desinteressada em âmbitos acadêmicos, mas sim que se defronta com o cerne da expansão colonial. Por isso, tudo o que se diz em criminologia é político, porque sempre será funcional ou disfuncional ao poder, o que não muda, ainda que quem o afirma o ignore ou o negue (ZAFFARONI, 2013a, p. 48).

O discurso não constitui uma simples *somatória de palavras*; trata-se, pelo contrário, de uma forma concreta de organização da linguagem orientada à produção e à fixação de um sentido específico. As palavras são organizadas segundo uma lógica particular, ordenação que condiciona a forma na qual é percebida a realidade e, também, quais são os espaços possíveis a ocupar e quem irá ocupá-los (GÓMEZ, 2012).

Isto não equivale a dizer que *tudo é linguagem,* mas a afirmar que o ordenamento da linguagem tem efeitos concretos sobre a ação e a reflexão. Esta orientação já foi trabalhada por autores como Huysmans (2009) e Campbell (CAMPBELL et al., 2007; CAMPBELL, 1992), que salientaram a necessidade de considerar a dimensão da representação de sentido nos estudos no campo da Segurança Internacional, particularmente, o segundo adverte que *o mundo não pode ser pensado por fora da linguagem.*

Com efeito, é através da linguagem, mas sempre organizada em torno a um discurso, que se outorga um sentido a *esse mundo*. A enunciação de um conjunto aleatório de ideias não produz uma leitura da realidade concreta. Pelo contrário, o que possibilita a produção de um sentido específico é a articulação de enunciados cuja inclusão na narrativa guarda coerência em termos da lógica argumentativa.

Uma das particularidades do enfoque analítico desenvolvido por Foucault é a de identificar a existência de diversos *discursos*, vinculando-os com uma lógica particular ou princípio de racionalização. Longe de expressar apenas uma disputa no campo das ideias,[39] o ponto central para o autor é que

[39] Nesta linha, o autor argumenta: "O problema é ao mesmo tempo distinguir os acontecimentos, diferenciar as redes e os níveis a que pertencem e reconstituir os fios que os ligam e que fazem com que se engendrem, uns a partir dos outros. Daí a recusa das análises que se referem ao campo simbólico ou ao campo das estruturas

esses princípios têm de ser estudados enquanto emergentes das configurações de poder subjacentes e como âmbito da sua reprodução.

É neste marco que Foucault se propõe fazer uma *crítica política do saber*, focada nas condições e nos efeitos com os quais se exerce uma veridicção. A lógica discursiva, argumenta, está ligada às características das práticas concretas sobre as quais se fala (FOUCAULT, 2008, p. 53). E, assim sendo, a unidade de análise não está concentrada nem na prática nem no discurso de forma isolada, mas na articulação entre ambas.

Sem pretender fazer uma exposição detalhada sobre a complexa obra do autor, cabe salientar que a ideia central, no que tange à presente dissertação, é que neste acoplamento com práticas concretas é que o discurso tem efeitos reais.[40] Resumida no conceito de dispositivo de saber-poder, tal noção concebe que é a unidade conformada entre uma prática concreta e um tipo específico de racionalização *que possibilita afirmar como verdadeiras uma série de coisas*[41] (FOUCAULT, 2008, p. 37).

Portanto, desde esta perspectiva, a importância política do discurso não radica, como sugerem os teóricos da securitização, no fato de que um ator determinado, em um contexto específico, possa executar uma ação através da

---

significantes, e o recurso às análises que se fazem em termos de genealogia das relações de força, de desenvolvimentos estratégicos e de táticas. Creio que aquilo que se deve ter como referência não é o grande modelo da língua e dos signos, mas sim da guerra e da batalha. A historicidade que nos domina e nos determina é belicosa e não linguística. Relação de poder, não relação de sentido. A história não tem "sentido", o que não quer dizer que seja absurda ou incoerente. Ao contrário, é inteligível e deve poder ser analisada em seus menores detalhes, mas segundo a inteligibilidade das lutas, das estratégias, das táticas. Nem a dialética (como lógica de contradição), nem a semiótica (como estrutura da comunicação) não poderiam dar conta do que é a inteligibilidade intrínseca dos confrontos. A "dialética" é uma maneira de evitar a realidade aleatória e aberta desta inteligibilidade reduzindo−a ao esqueleto hegeliano; e a "semiologia" e uma maneira de evitar seu caráter violento, sangrento e mortal, reduzindo−a à forma apaziguada e platônica da linguagem e do diálogo" (FOUCAULT, 1979, p. 4).

[40] Nesta linha, o próprio Foucault (2005, p. 29) realiza uma avaliação crítica do seu foco em estudos anteriores, como aquele que orientou seu seminário *A história da loucura* de 1961. Esse trabalho de pesquisa, argumenta o autor, esteve voltado à análise das representações, das imagens construídas ao longo da história sobre o fenômeno da loucura, pensando identificar nelas o lugar onde têm origem as práticas.

[41] Neste sentido, para o autor, "... precisamente esse é o ponto em que a análise histórica pode ter um alcance político. Não é uma história do verdadeiro, não é uma história do falso: a história da veridicção é que tem importância politicamente" (FOUCAULT, 2008, p. 50–51).

enunciação de um conjunto de palavras que observam um rito predeterminado. Pelo contrário, tal importância vincula-se ao fato de que é através do discurso que se outorga um entendimento específico sobre um conjunto de práticas que têm consequências concretas em termos de poder. A lógica discursiva, por sua vez, manifesta-se em forma de reiterações que configuram a sua unidade conceitual. É através destas regularidades que se pode identificar diversos pronunciamentos, enunciados por diferentes atores em momentos históricos distintos, como parte de uma única formação discursiva (FOUCAULT, 1987, p. 55).

Como referido, um dos argumentos do presente capítulo desta pesquisa consiste naquilo que os autores da Escola de Copenhague denominaram narrativa da securitização: é expressão das regularidades próprias do que, dentro da tradição da criminologia crítica, chamou-se de discurso do poder punitivo.

Antecipando brevemente aquilo que será objeto específico da próxima subseção, pode-se afirmar que, em paralelo ao conceito de ameaça identificado como núcleo central da retórica securitizadora (BUZAN et al., 1998, p. 34), o discurso do poder punitivo tem um dos seus eixos fundamentais em uma ideia muito próxima que é a de periculosidade.

Resumidamente pode-se afirmar que, na caracterização de Foucault, o dispositivo punitivo[42] conforma-se pela articulação de práticas de punição e vigilância com um princípio de racionalização centrado na prevenção de fenômenos a respeito dos quais uma autoridade se identifica como afetada. O exercício de poder punitivo segue, assim, uma lógica essencialmente disciplinar, que recai sobre a virtualidade do comportamento "ainda antes que o gesto seja uma realidade" (FOUCAULT, 2004, p. 73). Assim sendo, o seu aspecto diferencial é o de orientar intervenções de caráter repressivo, a ocorrer de forma prévia ao acontecimento pontual daqueles eventos ou fenômenos que se identificam como desejáveis de ser neutralizados. Isto é, a reprimir a ação daqueles atores considerados potencialmente perigosos.

[42] Esta questão é o núcleo central da obra Vigiar e Punir (1983), mas permeia quase a totalidade da obra de Foucault, como os seminários O poder psiquiátrico (2005) e O nascimento da biopolítica (2008), ministrados no Collège de France entre os anos 1972-1973 e 1977-1978, respectivamente. Em particular, em O poder psiquiátrico o autor contrasta as características que definem o que ele denomina de *poder disciplinar* em relação àquilo que chama de *poder soberano* (2005, p. 57–80).

Embora o estudo de Foucault sobre o particular focalizou principalmente os finais do século XIX, Zaffaroni avançou na linha da análise e da arqueologia do discurso do poder punitivo. Assim, acabou concluindo que, tal como ele se apresenta nos nossos dias, articula-se em torno a uma matriz argumental que tem sua primeira formulação sintetizada no *Malleus Maleficarum*, ou o *Martelo das feiticeiras* (KRAMER; SPRENGER, 2002). O argumento do autor é que o conteúdo do *Malleus*, que constitui o referencial da função inquisitorial, expressa as regularidades repetidas ao longo de todo o discurso punitivo posterior que, com poucas alterações, permanece vigente no presente. Ilustra essa continuidade na reflexão sobre o conflito social com uma ideia tão potente quanto perturbadora: "A Idade Média não terminou"[43] (ZAFFARONI, 2013b, p. 29, tradução nossa).

Assim, desde o discurso do poder punitivo, retoma-se então a questão da ameaça sob a fórmula da periculosidade – elemento chave para os teóricos da securitização e, também, para a conceituação de cunho foucaultiana, como reflexo da lógica preventiva. Em outras palavras, a ideia de que essa periculosidade pode ser eliminada ou contida perante uma ação punitiva (isto é, repressiva) não constitui uma retórica própria dos discursos sobre conflitos no nível internacional de finais do século XX.[44] Corresponde, em todo caso, à reiteração sobre formas de governamentalidade usadas em diversas oportunidades ao longo da história, em torno às quais se articula a prática penal ocidental há uns cinco séculos.

O objetivo central da seção final do presente capítulo é, precisamente, o de salientar estes aspectos que manifestam a continuidade histórica no discurso do poder punitivo. Seguindo o trabalho de Zaffaroni, faz-se uma descrição analítica das regularidades que lhe são centrais sobre a base da sua formulação no discurso demonológico, as quais são empregadas no segundo capítulo como categorias de análise dos discursos sobre vigilância massiva de comunicações.

---

[43] "La Edad Media no ha terminado".

[44] Embora exista essa diferenciação, os autores admitem a existência de conexões entre ambos e especificam que as principais divergências se vinculam aos referentes e às audiências. Argumentam, ainda, que "não excluem a possibilidade de encontrar de forma crescente este tipo de segurança nos contextos domésticos" (BUZAN et al., 1998, p. 46, tradução livre). Finalmente, cabe salientar que Bigo e Tsoukala (2008) debatem essa diferenciação conceitual.

2.2.2 A Idade Média não terminou: o discurso inquisitorial como expressão do discurso do poder punitivo

> a questão criminal é central nessa corrente que não para, como algo do presente, que é pura projeção do passado. Se não compreendemos que a Idade Média não terminou, não podemos entrever para onde vamos, ou pior, para onde podemos ir (o que me eximo de dizer, até mesmo por motivos de boa educação).
> Como a Idade Média não terminou, nada do passado está morto nem enterrado, mas apenas oculto, e não por acaso. Não é um passado que volta, mas sim que nunca se foi, porque ali está o poder punitivo, sua função verticalizante, suas tendências expansivas, seus resultados letais.
> [...]
> Porém, o que quero dizer com que a Idade Média não terminou? Por um lado, que somos hoje um produto daquele poder punitivo que renasceu na Idade Média e permitiu aos colonizadores europeus ocupar a América, a África e a Oceania, escravizar, dizimar e até extinguir os povos nativos, transportar milhões de africanos, avançar sobre o mundo com massacres e depredação colonialista e neocolonialista No entanto, por outro lado, quero dizer que os discursos legitimadores do poder punitivo da Idade Média estão plenamente vigentes, até o ponto de que a criminologia nasceu como saber autônomo no final do período medieval e fixou uma estrutura que permanece quase inalterada e reaparece cada vez que o poder punitivo quer se libertar de todo e qualquer limite e desembocar em um massacre. (ZAFFARONI, 2011b, p. 35–36).

No marco de um cenário marcado pela progressiva debilitação da autoridade papal, cuja legitimidade via-se minada pela ascensão dos poderes laicos, pelas práticas de corrupção no interior da estrutura eclesiástica e pelo crescimento dos

movimentos reformistas, o Papa Inocêncio VIII emitiu, no ano 1484, a bula[45] *Summis desiderantes affectibus.* Esta teve o efeito de intensificar a perseguição contra as "bruxas" na Europa central, ao proclamar que estas constituíam uma ameaça de caráter iminente e fortalecer a autoridade dos inquisidores para intervir, convocando Kramer e Sprenger a escrever aquilo que acabaria por se transformar no Malleus Maleficarum (INOCÊNCIO VIII, 2002).

Publicado em 1486, essa obra constitui, nas palavras de Zaffaroni (2011a, p. 29), o primeiro tratado que integrou de forma sistêmica o saber sobre a origem do mal (saber criminológico), sobre as manifestações do mal (saber penal) e sobre as práticas para descobri-lo concretamente (saber criminalístico). Neste sentido, a obra compilou o *saber* existente sobre a matéria até então, articulando-o para a produção de um sentido específico, e se tornou o Manual que orienta a prática inquisitorial na Europa central entre o século XV e XVIII.[46] De fato, salienta o autor, o livro foi editado vinte e nove vezes entre 1487 e 1669, sendo o segundo livro com maior número de edições, perdendo somente para a Bíblia.

Zaffaroni enumera um conjunto de características estruturais do relato articulado no Malleus Maleficarum que

[45] No direito canônico uma bula constitui um tipo de documento pontifício, isto é um decreto emitido pelo Papa que requere "respeito e acatamento" sem que exista possibilidade de interpor recurso nem apelação (IGREJA CATÓLICA, 1995, p. 59).

[46] Zaffaroni (2016, p. 10–20) diferencia cinco manifestações do modelo inquisitorial ao longo da história. 1) o procedimento inquisitorial romano, tal como constituído no direito romano, recuperado e incorporado no século XII no norte da Itália. 2) a inquisição medieval, que se desenvolve no marco da crescente disputa em torno à posição política do Papa na cena europeia e, em consequência, volta-se ao combate aos *heréticos* (textualmente, àqueles que sustentam uma posição diferente à doutrina oficial da Igreja). Carente de uma autoridade central, combinava as figuras, sempre conflitantes entre si, dos bispos locais, dos inquisidores e das autoridades laicas. 3) A Inquisição espanhola, que se enquadrou na disputa entre a monarquia absolutista que focou-se principalmente na burguesia convertida (judeus convertidos, cristãos novos ou marranos). Estendeu-se desde o século XV e, após vários intentos, só conseguiu ser formalmente abolida em 1834, durante a regência de María Cristina. Constituiu um instrumento político subordinado à monarquia (que tinha o poder de nomear e remover os inquisidores), completamente alheio ao domínio político de Roma, com o qual conflitava habitualmente. 4) A Inquisição Romana que instaurou-se no ano 1542, também no marco da crescente contestação quanto à hegemonia continental papal (personificada pelos chamados *reformados*), mas, diferentemente da medieval, operou em um esquema altamente centralizado, sob o então Papa Paolo III. 5) Finalmente a inquisição laica ou estatal dirigida pelos príncipes tal como aconteceu na França e na Alemanha .

expressam as regularidades do discurso do poder punitivo. Com o objetivo de simplificar a exposição, e buscando enfatizar o sentido que tenta se construir ao longo do livro, a listagem original do autor, composta por 27 itens (ZAFFARONI, 2013b, p. 30–36), foi reagrupada ao redor das 5 funções que organizam um relato, a saber: o quê, quem, por quê, quando e como.

Cabe salientar, novamente, que os diversos *elementos* ou *regularidades* identificados a seguir se encontram interligados através de uma lógica unificadora,
voltada à produção de um sentido específico. Assim, a subdivisão apresentada constitui uma escolha arbitrária, parcialmente inspirada nas categorias usadas por Zaffaroni, mas que nunca deve entender-se como taxativa, guardando cada um deles relação com as restantes.

i. O quê? – Em primeira instância, o que se enuncia é uma ação de caráter preventivo. Em particular o Malleus é apresentado como um Tratado que serve de guia para o exercício da função inquisitorial medieval. Tal como salientado na Carta Oficial da sua aprovação pela Universidade de Colônia, o livro contém "variadas e ponderadas orientações para o extermínio de bruxas", de cuja ação se desejava prevenir e salvaguardar todos os homens bons (DE MONTE et al., 2002, p. 520).
   Como foi expresso na seção precedente, a lógica preventiva é um dos elementos centrais que caracterizam o discurso punitivo e constitui, também, um elemento central na conceituação sobre o discurso securitizador. É precisamente este o sentido que tem o conceito de neutralizar aquele fenômeno que comporta um risco existencial (BUZAN et al., 1998, p. 26).[47]

ii. Quem? – Uma característica absolutamente saliente do discurso punitivo é a afirmação de uma autoridade central como sujeito legítimo da tomada de decisões. No Malleus, faz-se uma cuidadosa narrativa ligada ao estabelecimento da autoridade de intervenção e suas características, o que, basicamente, assume duas ordens: a primeira ligada à justificação do direito da autoridade em questão a intervir e a

[47] Este ponto se desenvolve no ponto a.1 da seção precedente.

segunda vinculada às suas capacidades superlativas para encarar a tarefa.

ii.a. A afirmação da autoridade e o *confisco do conflito:* A narrativa do poder punitivo se funda no que Zaffaroni denomina de *confisco do conflito* (2006, p. 22) ou *confisco da vítima*[48] (2013a, p. 19), isto é, o processo perante o qual a autoridade (política ou religiosa) se proclama como principal danificado pelo fenômeno em questão e se arroga a legitimidade para agir em resposta.

O Malleus é muito preciso neste ponto e estabelece, de acordo com as características da conjuntura política da Inquisição Medieval,[49] que a intervenção contra a bruxaria tinha de ser encarada por uma ação conjunta entre a autoridade eclesiástica (composta principalmente por Bispos e Inquisidores) e a civil (representada pelas Cortes seculares, entendidas como oficiais dos *governadores e senhores temporais*). Isto porque, na argumentação elaborada no Malleus, a bruxaria constituía um crime *misto na sua natureza,* já que simultaneamente era um crime contra a fé ou *heresia* – e, portanto, contra Deus, em cuja representação intervinha a autoridade eclesiástica (que está em graça diante de Deus) – e um dano temporal, sobre o qual o direito de intervenção era reconhecido para os tribunais civis[50] (KRAMER; SPRENGER, 2002, p. 377–395). De forma análoga ao que os autores da Escola de Copenhague identificaram como característico dos atores securitizadores, isto é, a reiteração de enquadrar sua atuação *em nome e em referência a uma coletividade*

[48] Com o termo *confiscação da vítima*, o autor refere-se ao processo histórico perante o qual o poder político institui-se como lesionado dos diversos tipos de conflito social. Neste sentido, Zaffaroni vai descrever a existência de dois modelos de administração de conflitos: o reparador e o punitivo. O primeiro, amplamente difundido na história da humanidade e empregado, por exemplo, pelos povos originários da América, baseia-se na procura de alternativas por meio das quais aquele que resultou danificado possa receber algum tipo de reparação por parte do agressor. O segundo, centra-se na substituição do danificado pelo poder político (Estado, senhor feudal, etc.) como vítima principal do processo. Assim, a decisão sobre o conflito é centralizada, o que acaba resultando na verticalização mesma da sociedade Id., 2013.

[49] Ver nota 46.

[50] Adicionalmente, reconhecem os autores do Malleus, essa formulação apresentava grandes vantagens para o sucesso da inquisição, uma vez que a cooperação das cortes civis possibilitaria aliviar a tarefa dos Inquisidores sempre que o trabalho se mostrasse muito árduo (KRAMER; SPRENGER, 2002, p. 377–395).

(BUZAN; WÆVER, 2009, p. 255), no Malleus se argumenta que se intervém “contra o crime da bruxaria, em nome da fé” para proteger ao povo cristão (KRAMER; SPRENGER, 2002, p. 396-397).

Através desta formulação sobre o direito a intervir – desta confiscação, nas palavras de Zaffaroni –, é que os principais danificados deixaram de ser as supostas vítimas diretas da ação da bruxaria e, no seu lugar, assumiram Deus pela *heresia* e o Senhor pelos danos temporais. O que se define, então, é quem está autorizado ou a quem é delegado o poder de designar em que consistem as ameaças e em quem estão personificadas e sob a base de qual racionalidade essa prática se institui.

É por isto que neste debate intervieram outros autores, como Jean Bodin, atualmente reconhecido dentro da chamada *filosofia* do Estado, pelos seus aportes ao desenvolvimento do conceito de soberania. Para Bodin, a bruxaria configurava um delito contra o Estado toda vez que o pacto satânico feria a religião, da qual o rei era garante e, assim, constituía um crime extraordinário de *lesa majestade”* (ZAFFARONI, 2016, p. 102–104). Inserido em um contexto inquisitorial diferente do Medieval ao qual pertence o Malleus, Bodin polemizou acaloradamente com Wier, o primeiro autor que tentou *patologizar* a atividade da bruxaria, isto é, subtrair as bruxas do controle das agências punitivas e localizá-las sobre controle do poder médico. Precisamente, essa publicação mereceu a resposta de Bodin quem em 1580 publicou *Da Demonomania das Feiticeiras,*[51] no qual dedicou um capítulo especial à *Refutação das opiniões de Jean Wier*. Neste sentido, o que à presente dissertação interessa destacar é que a natureza da disputa entre Wier e Bodin é diferente da que empreendem os autores do Malleus contra essas últimas. Na disputa que Bodin protagoniza, o que verdadeiramente

[51] No original: De la démonomanie des sorciers. Maiores referências sobre este livro de Bodin em língua portuguesa e sobre a ligação entre a teoria demonológica e a teoria e o percurso do denominado Estado moderno podem ser encontradas em Da Rosa (2013).

está em jogo é a autoridade, a jurisdição, isto é, quais agências concentrarão o poder de agir frente à ameaça.[52] Daí o caráter verticalizador deste discurso, já que possibilita à autoridade em questão e suas agências dispor de amplas prerrogativas discricionárias. Isto, novamente, resulta análogo àquilo que os autores da Escola de Copenhagen identificam como característico das consequências políticas do discurso securitizador[53] (BUZAN et al., 1998, p. 208).

ii.b. A argumentação sobre as capacidades superlativas da autoridade para encarar a intervenção: Também se apresentam argumentos orientados a ponderar a superior capacidade da autoridade central (e das suas agências) para encarar a ação em questão.

É nesta linha que no Malleus se afirma que os Inquisidores possuem *uma percepção privilegiada*. Embora não participassem do fenômeno em questão, Bispos, Inquisidores e outros teóricos como os autores do Malleus argumentavam ter um detalhado conhecimento sobre os procedimentos e atividades em geral de bruxas e demônios. Um aspecto central neste ponto é que, embora as bruxas e os demônios operassem através de encantamentos, na obra se especifica que aqueles encarregados da administração de justiça (civil ou eclesiástica) não eram afetados por nenhum tipo de feitiços destinados a enganar os sentidos (KRAMER; SPRENGER, 2002, p. 197–198).

Sendo o discurso orientado no sentido da prevenção, é preciso argumentar que as agências possuem algum tipo de capacidade diferencial para perceber aqueles sinais que antecedem ao ato ou se constituem em características próprias daqueles pertencentes ao grupo *inimigo*. Esta ideia, condensada por Zaffaroni na noção de *percepção*

[52] É por isto que Zaffaroni argumenta que esta constitui a primeira disputa entre o poder punitivo e o médico, documentada historicamente, antecedendo em três séculos àquela retratada por Foucault no seu artigo *A evolução da noção de "indivíduo perigoso" na psiquiatria legal do século XIX* (2004). Neste artigo, o autor argumenta a emergência da noção de risco como articuladora do saber, que a prática penal transforma completamente, já que substitui a pergunta sobre o ato (ligada ao princípio de responsabilidade) pela pergunta sobre o indivíduo (ligada ao princípio de risco ou ameaça) (2008, p. 53).

[53] Para maiores detalhes ver ponto i.d da seção precedente.

privilegiada,[54] é central, então, no que faz a legitimidade dos agentes e das agências no desenvolvimento das práticas voltadas à prevenção. Isto foi identificado com clareza por Foucault no caso dos médicos e sua capacidade exclusiva de perceber a monomania (2004, p. 10).

Nesta mesma linha, Bigo (2008, p. 25) salienta que é sobre esta ideia do conhecimento adicional, da sua capacidade diferencial para a compreensão das complexidades do cenário atual, que os burocratas das agências de segurança se autoafirmam como autoridades legítimas para intervir. O autor argumenta que, na disputa em torno à legitimidade no campo da segurança internacional, as burocracias das diversas agências sustentam sua posição superlativa sobre a base da crença de que as pessoas envolvidas no campo possuem, enquanto especialistas, um conhecimento superior dos segredos que somente os profissionais podem saber. Por sua vez, essa crença, afirma o autor, é reforçada pelas próprias rotinas de compartilhamento de informação entre agências e os enfoques sobre ameaças e inimigos evocados de forma cotidiana.

iii. Por quê? – A intervenção é apresentada como uma necessidade derivada da necessidade de neutralizar um risco iminente. Para isto, dois elementos centrais podem se reconhecer no discurso: a narrativa voltada à caracterização de dita ameaça e a legitimação dessa mesma narrativa.

iii.a. A ameaça é máxima: Seguindo a retórica do discurso religioso em torno do qual se articula o Malleus Maleficarum,

[54] Embora pelo enfoque cinematográfico, a ideia da percepção privilegiada e sua vinculação com o ideal da prevenção se ilustra, com singular clareza, no filme Sentença prévia (SPIELBERG, 2002), no original: Minority Report. Este apresenta a visão de uma sociedade futurista na qual o fenômeno dos homicídios teria sido em boa parte neutralizado mediante o funcionamento de um particular dispositivo punitivo baseado na condenação prévia – basicamente, o aprisionamento do suposto potencial homicida antes do assassinato ter sido cometido. No filme, o procedimento para obtenção daquele saber que habilita as agências de segurança e justiça executar a condenação prévia deriva de três seres super-humanos com capacidade de prever o futuro. Algo assim como uma forma máxima de indivíduos com percepção privilegiada. Cabe salientar que nem no filme esse sistema pode ser perfeito, sendo passível de engano e levando a uma série de condenações falhas, sobre as quais discorre a trama.

a bruxaria, o alvo principal da Inquisição medieval,[55] é indicada como um fenômeno de gravidade maiúscula. De fato, no livro se apresenta como a "mais maligna e a pior de todas", dentre as diversas formas de heresia[56] (KRAMER; SPRENGER, 2002, p. 77).

Como explica Zaffaroni, a exaltação desta dimensão é essencial, porque desta deriva a percepção construída em relação ao perigo e, assim, o poder que será conferido ao repressor para extingui-lo. Neste sentido, segundo a bula do Papa Inocêncio VIII, as bruxas

> [têm] assassinado crianças ainda no útero da mãe, além de novilhos, e têm arruinado os produtos da terra, as uvas das vinhas, os frutos das árvores, e mais ainda: têm destruído homens, mulheres, bestas de carga, rebanhos, animais de outras espécies, parreirais, pomares, prados, pastos, trigo e muitos outros cereais; estas pessoas miseráveis ainda afligem homens e mulheres, animais de carga, rebanhos inteiros e muitos outros com dores terríveis e lastimáveis e com doenças atrozes, quer internas, quer externas; e [impedem] os homens de realizarem o ato sexual e as mulheres de conceberem, [...] porém, acima de tudo isso, renunciam de forma blasfema à Fé que lhes pertence pelo Sacramento do Batismo, e por instigação do Inimigo da Humanidade não se escusam de cometer e de perpetrar as mais sórdidas abominações e os excessos mais asquerosos para o mortal perigo de suas próprias almas, pelo que ultrajam a Majestade Divina e são causa de escândalo e de perigo para muitos (INOCÊNCIO VIII, 2002, p. 43).

[55] Como referido anteriormente, Zaffaroni diferencia cinco manifestações históricas do modelo inquisitorial. Para maior detalhe, ver nota 46.

[56] Esta caracterização se justifica no texto, no sentido de que, sendo um pacto aberto com o demônio, resulta em um esforço máximo por profanar e danificar a Deus e suas criaturas (KRAMER; SPRENGER, 2002, p. 77). Sob essa lógica, os autores do Malleus argumentam que a bruxaria constitui um pecado que resulta, inclusive, de maior gravidade que o *pecado original*.

Aqui se evidencia um claro paralelo com o conceito de *hierarquização*, com o qual, no enfoque da securitização, designa-se a tendência de construir narrativas que tendem a priorizar o fenômeno em questão dentro do contexto de possíveis ameaças (BUZAN et al., 1998, p. 24). Como salientado nos casos anteriores, esta característica, entendida pelos autores da Escola de Copenhague como própria do discurso securitizador,[57] constitui um elemento característico do discurso do poder punitivo e está claramente presente já na sua formulação demonológica no século XV.

iii.b. Configura-se uma narrativa na qual se exaltam os valores positivos associados ao identificado como em situação de risco. No discurso punitivo, a imagem que se contrapõe àquele fenômeno identificado como ameaça é arquetípica do bom. Segundo os autores do Malleus, a prática da bruxaria comportava um risco nada menos que para a salvação da alma e não só daqueles que a praticam, mas de todos (KRAMER; SPRENGER, 2002, p. 77). Em idêntico sentido, na já referida Bula papal, argumentava-se que a falta de punição de tais *abominações e atrocidades* supunha um grave perigo para as almas de muitos e ameaça de danação eterna (INOCÊNCIO VIII, 2002, p. 44).

O discurso do poder punitivo, conforme Zaffaroni, articula-se em torno a uma narrativa moralizante que contrapõe o bem e o mal. O sentido do bem fica atrelado à imagem daquilo que é caracterizado como em situação de risco e, por extensão, à autoridade que se coloca em posição de seu defensor. Pelo contrário, o mal constitui a ameaça e é encarnado pelos grupos perigosos, tal como se desenvolve mais especificamente à continuação.

Como afirma Foucault (2004, p. 57–80), o discurso é direcionado a construir a imagem de um estado terminal ou superior que orienta a intervenção.

Por sua parte, esta regularidade também é identificada pelos teóricos da securitização, os quais a condensam na imagem de "estado livre de ameaças" que serve como orientação da narrativa securitizadora (WÆVER, 1995, p. 51).

[57] Isto foi abordado no ponto a da seção precedente.

iii.c.O conteúdo específico atribuído ao perigo vincula-se com os preconceitos da época. Uma conclusão bastante óbvia da leitura do Malleus é que os argumentos em torno à caracterização da bruxaria, e mais especificamente do papel das mulheres nesta prática, consolidaram-se como discurso dominante sustentados nos preconceitos da época.

Neste sentido, o argumento central a respeito de por quê, segundo a visão dos inquisidores, as mulheres constituíam o grupo que mais pactuava com Satã consistiu em que estas eram mais supersticiosas e mais crédulas, como resultado de uma mente mais débil e, assim, que resultava mais fácil menoscabar sua fé[58] (KRAMER; SPRENGER, 2002, p. 119–120).

Essa ideia é reforçada ao longo da obra, ao asseverar que as mulheres "são mais impressionáveis e mais propensas a receberem a influência do espírito descorporificado", "não se abstêm de contar às suas amigas tudo o que aprendem", "são mais débeis em mente e corpo", "no que tange ao intelecto, ou ao entendimento das coisas espirituais, parecem ser de uma natureza diversa da do homem" e, em definitivo, porque tendo havido "... uma falha na formação da primeira mulher, por ter sido ela criada a partir de uma costela recurva […] é contrária à retidão do homem" (KRAMER; SPRENGER, 2002, p. 115–116).[59]

Zaffaroni argumenta que o conteúdo do relato incluso no Malleus afirmava-se sobre os preconceitos da época em relação a atividades e, em particular, a grupos sociais que não se adaptavam às pautas daquilo tido como aceitável. Neste sentido, é destacável o foco nas parteiras e não é de surpreender, dentro do texto do Malleus, que as mulheres boas são as *virgens e outras santas* (KRAMER; SPRENGER, 2002, p. 49).

---

[58] Este ponto é reforçado pelos autores com uma suposta etimologia da palavra *fêmea* como sendo derivada de *minus fe,* formulação desacreditada por Zaffaroni, o qual argumenta que a palavra provém do sânscrito e significa *amamentar* (2013a, p. 28).

[59] Em idêntico sentido expressam ser possível comprovar que, em termos históricos, "quase todos os reinos do mundo tem sido derrubados por mulheres", o que exemplificam com os casos de Tróia e Helena, Roma e Cleópatra dentre outros e, assim, "portanto não é esquisito que o mundo sofra agora por casa das mulheres" (KRAMER; SPRENGER, 2002, p. 119).

iii.d.A veracidade da narrativa em torno à ameaça é inquestionável: ao mesmo tempo em que se caracteriza a ameaça, também se defende a veracidade do relato. Para isto:

iii.d.1.Inverte-se a valoração dos fatos: Na leitura do Malleus, resulta expressivo que a lógica do argumento é articulada para pautar a interpretação dos fatos proposta independentemente de qual seja a *realidade observada.* Como comenta Zaffaroni (2013a, p. 36), caso a mulher não confessasse durante a tortura, sua atitude era lida como sinal de que era apoiada por Satã. No entanto, se ela se enforcava, era porque o diabo a condenava pelo crime. Expressar arrependimento tampouco era garantia de salvação, já que, nesse caso, considerava-se que era simuladora.

Ainda mais, uma mesma ação devia ser interpretada de forma diferente segundo quem a realizasse. Por exemplo, aponta-se que a *observação do tempo e das estações*, quando realizada por um homem, deve ser considerada como um exercício vão *e ocioso* ou voltado à aquisição de conhecimentos que levem a provocar uma mudança benéfica no seu corpo. Pelo contrário, se for realizado por uma mulher, devia entender-se que se tratava de adivinhação e, assim, de bruxaria (KRAMER; SPRENGER, 2002, p. 76).

iii.d.2.Tenta-se neutralizar qualquer fonte de autoridade que estabeleça uma interpretação contrária à manifestada. Resulta ilustrativo que as primeiras seções do Malleus estejam destinadas à deslegitimação das posições tanto daqueles que afirmavam que as bruxas não tinham existência real quanto daqueles que, ainda acreditando nas bruxas, argumentavam que suas práticas não tinham efeitos reais e permanentes. Com o objetivo de construir legitimidade em relação ao seu argumento, Kramer e Sprenger começam justamente rebatendo os argumentos existentes até a época, que incluíam fontes de relevância doutrinária tais como cânones prévios.[60]

[60] Cabe salientar especialmente neste sentido ao Canon episcopi, o qual tem um lugar saliente no Malleus por estar diretamente envolvido com a questão da própria existência da bruxaria e dos efeitos concretos e duradouros que tais práticas tinham.

> Em definitivo, concluem que aqueles que argumentassem sobre a inexistência das bruxas tinham de ser considerados como *suspeitos de sustentar opiniões heréticas* (KRAMER; SPRENGER, 2002, p. 59–63).

iv. Quando? – Outra regularidade do discurso do poder punitivo consiste em argumentar em relação à necessidade de uma intervenção de caráter urgente sob a base de um fenômeno cuja ocorrência apresenta uma frequência alarmante. Assim, constatam-se as seguintes reiterações discursivas:

iv.a. Argumenta-se que a intervenção tem que ser realizada com urgência. Outra das noções manifestas no Malleus tem a ver com a alarmante proliferação da heresia em geral e da bruxaria, em específico, tudo o que cominava a necessidade de encarar uma intervenção peremptória.

Neste sentido, dentre outras formulações, os inquisidores afirmavam que a ação das bruxas havia multiplicado nos anos recentes; que a sua prática havia aumentado notavelmente; e que a quantidade de bruxas havia aumentado como consequência da rivalidade entre pessoas casadas e solteiras. Em igual sentido, na já referida Bula, afirmou-se que a ação inquisitorial era indispensável porque *muitas pessoas de ambos os sexos tinham se abandonado aos demônios e aos seus encantamentos* (INOCÊNCIO VIII, 2002, p. 43).

Como argumenta Zaffaroni, a função específica desta noção em torno à urgência ou à iminência do risco é a de salientar que o contexto em questão configura uma situação emergencial. É por isto que o medo aparece sempre como fundamento último da ação.

Isto novamente marca um ponto de contato com aquilo que os autores da Escola de Copenhague salientam como característico da narrativa da securitização. Estes identificam uma recorrente tendência de dramatização na caracterização do fenômeno e, nisto, um elemento chave para estabelecer o caráter urgente da intervenção (BUZAN et al., 1998, p. 29).[61]

iv.b. Afirma-se a veracidade da situação emergencial. Em paralelo à importância de legitimar o discurso sobre a

[61] Esse assunto foi abordado especialmente no ponto a.2 da seção precedente.

ameaça (isto é, da urgência da intervenção), encontra-se a necessidade de legitimar a urgência da mesma. Enquanto discurso orientado à legitimação de práticas ilimitadas, um elemento recorrente é a condenação daqueles que questionam o argumento da emergência. Também é recorrente a condenação daquelas expressões que manifestem dúvidas ou que, em forma mais taxativa, contrariem o diagnóstico relativo à frequência do fenômeno. Questionar a emergência é, portanto, também questionar a ação urgente. Nesta linha, na mencionada bula, o Papa Inocêncio VIII (2002, p. 44) dedica especial referência àqueles que "não se acanham em afirmar, na mais despudorada desfaçatez, que tais monstruosidades não são praticadas naquelas regiões e que, consequentemente, os supracitados Inquisidores não têm o direito legal de exercerem os poderes da Inquisição".

v.Como? – De forma regular se assevera que a neutralização da ameaça requer uma ação de tipo extraordinária. Fundada sobre uma série de caracterizações específicas sobre a natureza do conflito e sobre o inimigo, o que se argumenta, em definitivo, é que unicamente uma ação que articule meios excepcionais tem a possibilidade de ser exitosa. Para isto, invoca-se a figura de uma guerra que configura um estado de exceção, contra um inimigo cuja imagem se desvaloriza e que é caracterizada com uma organização simultaneamente difusa e articulada.

v.a.Emprega-se uma retórica belicista: Uma das características do Malleus é o apelo a uma linguagem totalmente bélica. Citando a São Tomás, os autores do referido manual afirmam que "o que há é uma guerra declarada entre os homens e os demônios" (KRAMER; SPRENGER, 2002, p. 363).

Esse conflito, aliás, apresenta certas características diferenciais em função da caracterização que se faz da pessoa do inimigo e sua estratégia:

v.b.O inimigo é difuso, mas sua ação é coordenada. As múltiplas manifestações do fenômeno em questão são apresentadas como sendo resultado da ação de um inimigo cuja identificação concreta implica dificuldades e cuja atuação é coordenada. Em relação aos demônios, no

Malleus assevera-se que se apresentavam em forma humana através de encantamentos ao tempo que, a respeito das bruxas, diz-se que cometiam “seus crimes em segredo” (KRAMER; SPRENGER, 2002, p. 396). Por sua vez, argumenta-se que ambos operam de maneira coordenada toda vez que, segundo os Inquisidores, constituía *uma verdade católica* que, no que faz à geração de dano, “as bruxas e o demônio trabalham juntos”[62] pois, “como se encontram em guerra como a raça humana, combatem-na de forma ordenada; julgam assim prejudicar mais os homens e, como efeito, o conseguem” (KRAMER; SPRENGER, 2002, p. 92).

Em uma terminologia mais contemporânea, pode-se dizer que, quanto às suas características táticas, o inimigo narrado no Malleus se articula como um tipo de *exército irregular.* O paralelo entre ambos os conceitos é traçado pelo próprio Zaffaroni, que vincula esta formulação com aquela que, no século XX, emprega Carl Schmitt (1998).[63] Sem desejar entrar nas várias dimensões que o debate em torno ao conceito de *exército irregular* apresenta no campo da Segurança Internacional,[64] o ponto central a respeito é que, já desde a época inquisitorial, a ação do inimigo apresentou-se sempre como diferenciada, oculta e organizada.

A leitura proposta é que as supostas múltiplas manifestações do fenômeno apresentado como emergencial

[62] Sobre este particular, os autores colocam especial ênfase em refutar as visões que afirmavam que as bruxas constituíam unicamente um instrumento do diabo, posição que implicaria que não seriam responsáveis.

[63] Sobre este ponto, Zaffaroni argumenta que: “Ainda que não o afirme, é claro que esta é a tese central da definição do político de Carl Schmitt e a constatação de que se tenta uma trágica planetarização da chamada doutrina da segurança nacional dos anos 1970 sul-americanos. Esse caminho teórico é um dos que, desde a periferia, devemos reelaborar e aprofundar, porque nos toca muito diretamente; além do mais, é a partir daí que podemos detectar mais facilmente o papel central e protagonista do poder punitivo” (ZAFFARONI, 2013a, p. 168).

[64] Saint-Pierre fez uma profusa análise sobre este conceito e suas implicâncias político-legais. Em particular, destacou que, na história recente, a fórmula *forma armada não regular* pode ser definida desde um ponto de vista técnico, em contraposição àquilo que é reconhecido como exército regular pela Haia (2000, p. 183–185). Neste sentido, considerando o fato de que, logicamente, as denominações *regular* e *irregular* são historicamente determinadas, consideramos o paralelo conceitual útil em termos do sentido interpretativo que tentam construir em torno às características do fenômeno em questão.

resultam da ação de grupos que seguem uma lógica única. Portanto, devem ser combatidos com uma ação única e total.

O sentido por trás da ideia da irregularidade é assim duplo, como salienta Saint-Pierre (2000, p. 185–194): por um lado, faz questão da pretensão de anonimato do combatente (que se oculta entre a população civil ou inocente) e da versatilidade de seu movimento (sua mobilidade tática) e, por outro, diz respeito ao que não se submete às normas que regulam os conflitos. Existe assim uma ostensiva proximidade entre a conceituação que se tem em relação à ação enquadrada de um grupo de criminalidade organizado e a de um exército irregular. Isto porque ambas apresentariam traços comuns nas técnicas empregadas (no sentido dos *modus operandi*, na expressão do autor), mas diferenciam-se expressamente no que faz as suas intencionalidades.[65] Neste sentido, Kramer e Sprenger (2002, p. 74) afirmam que suas práticas deviam ser consideradas "o acme da iniquidade criminal".

v.c.Desvaloriza-se a imagem do inimigo como justificativa para lhe propiciar um trato diferenciado. Na narrativa se repetem formulações que apontam a diferenciar o inimigo e conotá-lo negativamente. Aqueles grupos caracterizados como fonte da ameaça encarnam, no discurso do poder punitivo, o lugar do mal. Sendo a estreita vinculação, entre ambas as noções, ilustrada na etimologia da palavra Satã, que em hebraico significa inimigo (ZAFFARONI, 2013a, p. 27).

Este aspecto cumpre uma função essencial na legitimação de práticas extraordinárias. Ainda mais, como destacaram os autores do tratado inquisitorial, a característica diferencial da bruxaria é que esta consistia de forma direta em praticar o mal. Nas suas palavras: "seu nome latino, *maleficium,* significa exatamente praticar o mal e blasfemar contra a fé verdadeira" (KRAMER; SPRENGER, 2002, p. 77, ênfase no original).

[65] Aqui o autor debate o conceito de guerrilha, sua característica não regular e as particularidades de seu status legal, identificando que é, precisamente, o compromisso político aquilo que diferencia de forma definitiva a organização guerrilheira das organizações criminais, abrindo um "abismo conceitual intransponível" entre ambos (SAINT-PIERRE, 2000, p. 188–190).

Embora o conteúdo específico fosse mudando ao longo da história, o discurso do poder punitivo se caracteriza por atribuir ao outro a intencionalidade explícita de fazer dano. Como salienta Zaffaroni (2006, p. 11), se lhe nega a condição de pessoa e somente é considerado como ente perigoso ou daninho.

O que se julga então não são os fatos, mas a vontade que teria orientado as ações. É por isto que Zaffaroni argumenta que este instrumento tenha servido ao objetivo de eliminação dos indesejáveis, daqueles tidos como elementos humanos degenerados.

Como foi salientado nos pontos precedentes, o fenômeno em questão é apresentado como a manifestação do mal, sendo que as características do inimigo se sustentam sobre os preconceitos da época. Ainda, argumenta-se que sua tática é difusa e coordenada. Neste contexto, sua neutralização só pode ser alcançada mediante ações de caráter emergencial, isto é, diferentemente das formas de intervenção *regulares*.[66] Argumenta-se, assim, que as causas deviam ser "conduzidas da maneira mais simples e mais sumária, sem os argumentos e as contenções dos advogados de defesa". Ainda mais, estabelecem que

> o Juiz encarregado de tais causas não necessitará, para proceder ao julgamento, de nenhuma ordem judicial por escrito [...] e deverá dar prosseguimento ao julgamento da forma mais sumária possível, desautorizando quaisquer exceções, apelos ou obstruções, quaisquer contenções impertinentes de defensores ou advogados (KRAMER; SPRENGER, 2002, p. 406).

[66] O procedimento de tortura, institucionalizado desde a antiga Roma, constitui um recurso por demais válido no desenvolvimento da tarefa dos inquisidores. A quase totalidade da terceira seção do livro discorre sobre as alternativas do procedimento judicial, a extensão da prática da tortura, as técnicas habilitadas para deprimir a capacidade dos acusados permanecerem em silêncio durante os interrogatórios (KRAMER e SPRENGER, 2002, p. 428–430), dentre outras. Neste sentido, manuais de procedimentos de interrogação contemporâneos, como o aplicado na base estadunidense em Guantánamo, guardam uma lamentável semelhança com esta terceira seção do Malleus Maleficarum. No ano 2012, o site Wikileaks difundiu uma série de documentos nos quais se detalham as políticas aplicáveis aos réus em custódia militar, especialmente na base estadunidense da Baía de Guantánamo. Para maiores informações consultar: https://wikileaks.org/detaineepolicies/document/

Isto novamente remete ao que foi identificado pelos autores do marco analítico da securitização como relativo à *natureza especial* da segurança, que justificaria medidas extraordinárias, ações por fora dos parâmetros considerados como regulares dentro do processo político (WÆVER, 1988, p. 4; BUZAN et al., 1998, p. 208).[67]

v.d. Apresenta-se a estratégia do inimigo como orientada à exploração de vulnerabilidades. Finalmente, outra regularidade presente no discurso do poder punitivo é a de afirmar que a ação do inimigo se serve das *fraquezas* ou *debilidades* da sociedade em geral para fazer o mal. Montado sobre os preceitos morais próprios do discurso cristão, no qual se insere o Malleus, seus autores apontam principalmente à *libertinagem da carne* como fonte de vulnerabilidade enquanto favorecedora da ação do Satã. Neste sentido argumentam que: "[t]rês vícios gerais parecem ter um domínio especial sobre os males das mulheres: a infidelidade, a ambição e a luxúria" (KRAMER; SPRENGER, 2002, p. 121) ou que "as mulheres vilãs fazem os homens abandonar as esposas belas" (KRAMER; SPRENGER, 2002, p. 127).

Assim, a mesma seletividade estrutural que outorga ao poder punitivo a capacidade de escolher arbitrariamente seu inimigo, aplica-se à caracterização daquelas condutas que serão consideradas como *desordenadas.*

As regularidades agrupadas no item iv.b apontam, precisamente, à racionalidade política do dispositivo punitivo, já que reúne as dimensões ligadas aos mecanismos de intervenção. O ideal da prevenção como fim declarado da ação implica, consequentemente, mecanismos de detecção antecipada que possibilitem encontrar o inimigo antes que ele atue.

Enquanto a racionalidade sob a qual se articula o discurso no marco deste dispositivo é a de impedir que um fato aconteça, uma série de noções emergem como logicamente ligadas. Os exemplos mais claros são os conceitos de risco, de perigo, que intervém para nomear aquilo que se tenta neutralizar,

[67] Este aspecto é abordado especialmente no ponto i.d da seção precedente.

mas também toda uma série de outros conceitos (e práticas) orientados à identificação prévia ao acontecimento. No dispositivo enquadrado em torno à ideia da prevenção, precisamente, o acontecimento do fenômeno não é um parâmetro para a ação. Sendo a racionalidade a de intervir com antecedência, manifesta-se como necessário desenvolver uma série de mecanismos de detecção prévia. Isto é, de monitoramento, de determinação dos indicadores de risco, etc.

A retórica belicista e a desvalorização do inimigo assumem a função principal de enfatizar a necessidade e pertinência do uso de mecanismos de exceção que, em teoria, seriam de aplicação circunscrita à população alvo (isto é, ao inimigo). Ao mesmo tempo, a narrativa que caracteriza o inimigo como difuso e voltado à exploração de vulnerabilidades aponta a necessidade de estender os mecanismos sobre o conjunto populacional. O exercício de poder punitivo é sempre, então, caracterizado por uma vigilância contínua, sustentada sobre um sistema de registro permanente, constante e centralizado, que configura um centro e uma periferia de controlados e controladores.

Cabe salientar neste ponto que, segundo a definição inclusa no Malleus, o processo de inquisição não se funda na existência de informações ou acusações sobre a atuação de pessoas concretas; basta "apenas uma denúncia geral de que há bruxas em determinado lugar". Dos três procedimentos que os autores identificaram como permitidos pelo direito canônico,[68] argumentam que o propriamente inquisitorial era "o mais comum e mais usual, por ser secreto, e nenhum acusador ou informante precisa aparecer" (KRAMER; SPRENGER, 2002, p. 396-399). Neste sentido, no processo se instava, "em virtude da santa obediência e sob pena de excomunhão", a todo aquele que "souber, tiver visto ou ouvido a respeito de pessoas consideradas hereges ou bruxas, ou de pessoas que se suspeite terem

[68] Segundo os autores, o texto canônico previa, na época, três métodos para a instauração de um processo contra o crime da bruxaria. O primeiro, fundado em uma acusação concreta na qual o acusador se oferece a prová-la e se submete à lei de talião. O segundo, fundado em uma denúncia feita sobre uma pessoa, mas na qual o informante não se propõe envolver-se diretamente na acusação e não se submete à lei do talião. Finalmente, como terceiro método "tem-se a inquisição propriamente, ou seja, não se tem a presença de um acusador ou de um informante – apenas uma denúncia geral de que há bruxas em um determinado lugar ou determinada cidade" (KRAMER; SPRENGER, 2002, 396).

causado males a homens, ao gado ou aos frutos da terra, em prejuízo do Estado, que nos venha a revelar o caso" (KRAMER; SPRENGER, 2002, p. 396-397). Esses depoimentos eram *fielmente anotados* e constituíam a base de início do processo.

Entendida como uma tecnologia política desprendida de todo uso específico, esta é precisamente a função que assume a vigilância e que expressa o maior poder de condicionamento por trás do exercício do poder punitivo. É esta a orientação do estudo sobre o modelo Panóptico que Foucault (1983, p. 238) empreende em seu famoso livro *Vigiar e punir*, no qual argumenta que a relevância política desse modelo não reside em ser um modelo de desenho de instituições fechadas, mas, sim, um padrão de vigilância generalizada. É dessa forma que o autor o utiliza como chave de leitura dos regulamentos de organização urbana do século XVIII. De fato, como argumenta de maneira mais específica posteriormente, para Foucault, a vigilância tornou-se uma forma generalizada de governo das populações ou governamentalidade, entendida esta como uma maneira de "guiar os homens, de dirigir sua conduta, de forçar suas ações e reações" (FOUCAULT, 2008, p.4).[69]

Tentando não adiantar aquilo que será abordado em profundidade no capítulo seguinte, pode-se afirmar que é precisamente esta a racionalidade por trás do projeto de "coletar tudo e analisar tudo" (NSA, 2011) que, tal como expressado pelos protagonistas, orienta a prática da vigilância massiva de comunicações. Precisamente, o ponto central da análise de Foucault sobre a lógica punitiva é que, em termos de capacidade de condicionamento, o fundamental do exercício do poder punitivo não está dado tanto pelo castigo daqueles efetivamente identificados como *criminosos*, mas pela vigilância sobre o conjunto da sociedade.

[69] Vale a pena referir que na presente dissertação não pretende-se abordar o intenso, e por demais relevante, debate a respeito da caracterização em termos conceituais do dispositivo de vigilância contemporâneo e suas repercussões sobre o conjunto social. Em particular, diversos autores debatem a pertinência do modelo panóptico *tradicional* como ferramenta analítica que possibilite dar conta da complexidade do presente, dentre eles, salientamos a Lyon (2012), a Bauman e Lyon (2014) e a Bruno (2013). Além dessas considerações na presente pesquisa tenta-se enfatizar que nos elementos que marcam a continuidade histórica desta prática, tal como identificados por Foucault.

No presente capítulo, perseguiram-se dois pontos centrais. Primeiro, o de vincular os conceitos de *narrativa securitizadora* com o de discurso do poder punitivo. Segundo, o de desenvolver as categorias que servirão de base para a análise dos acontecimentos discursivos na segunda seção do capítulo seguinte.

Para tal fim, o capítulo iniciou argumentando a respeito da relevância das análises discursivas no marco dos estudos de Segurança Internacional, com base no marco analítico da securitização. No percurso do capítulo, abordaram-se as limitações que a perspectiva da securitização supunha para o desenvolvimento da pesquisa. Especificamente, contrapôs-se o enfoque orientado pela lógica da performatividade dos enunciados, característico dessa, com a perspectiva da análise discursiva do poder própria das perspectivas baseadas no pensamento de Foucault, dentre as quais se destaca, na presente dissertação, a da criminologia crítica. Neste sentido, introduziu-se o conceito de discurso do poder punitivo para finalizar com um detalhamento das suas características estruturais, baseado no estudo da sua formulação inquisitorial. Com isto, definiram-se as categorias a serem empregadas para a análise no próximo capítulo, com ênfase nas estratégias as quais o poder punitivo se vincula.

Tentou-se enfatizar os pontos de encontro entre ambos os enfoques, pretendendo com isto sustentar o argumento de que aquilo que os autores da Escola de Copenhague denominaram de *narrativa própria da securitização* constitui a expressão das regularidades do discurso punitivo. É neste sentido que se repete, com Zaffaroni, que a Idade Média não terminou.

O segundo, e último, capítulo da presente dissertação tem, na sua primeira seção, uma descrição analítica dos mecanismos concretos sob os quais se estrutura o monitoramento de dados digitais no século XXI. Considera-se que a compreensão de suas particularidades resulta um insumo fundamental para a discussão final da pesquisa, ligada aos princípios de racionalização de tal prática. Adicionalmente, acredita-se que, embora sua relevância, as características de tal sistema permanecem ainda pouco exploradas no âmbito acadêmico.

Por sua vez, na segunda seção é analisado um conjunto escolhido de pronunciamentos que enquadram a prática da vigilância de comunicações como uma ferramenta essencial na garantia da segurança doméstica e internacional. Como já referido, as categorias empregadas são aquelas surgidas do estudo empreendido por Zaffaroni sobre o discurso inquisitorial. Persegue-se o objetivo de mostrar que, embora a contemporaneidade do fenômeno aqui estudado e o caráter eminentemente atual das tecnologias empregadas, mantêm-se em essência idênticos mecanismos de racionalização que, cinco séculos atrás, eram empregados na queima de bruxas e outros terroristas da época.

3 O SISTEMA DE VIGILÂNCIA MASSIVA E GLOBAL DE COMUNICAÇÕES

> Como a informação quer ser livre, não escreva nada que não possa ser lido em voz alta diante de você num tribunal ou visto impresso na manchete de um jornal, pois o peixe morre pela boca. No futuro, o significado desse velho ditado será expandido para incluir não só o que você diz ou escreve, mas também os websites que visita, quem adiciona em sua rede, o que "curte" e o que suas conexões fazem, dizem ou compartilham (SCHMIDT; COHEN, 2013, p. 65).

> Não quero viver em um mundo no qual tudo o que diga, tudo o que faça, todos aqueles com que eu fale, toda expressão de criatividade e amor ou amizade seja gravada[70] (SNOWDEN, 2013 apud POITRAS, 2014, tradução livre).

O presente capítulo aborda de maneira específica os aspectos que caracterizam o sistema de vigilância massiva e global de comunicações. Para isto, o capítulo se inicia com uma abordagem a respeito de alguns aspectos chave das fontes de informação: os documentos que conformam o acervo Snowden.

Na segunda, a ênfase é colocada no funcionamento concreto do esquema de monitoramento: suas características, sua abrangência e a base material (econômica e institucional) sob a qual se desenvolve. Em específico, é enfatizado que o eixo central na estruturação do sistema de monitoramento, como referido, é a sua orientação massiva, ilustrada no princípio de *saber tudo, coletar tudo, analisar tudo* (NSA, 2011). Além de perseguir o objetivo de propiciar maior difusão e análise a um fenômeno que ainda resulta pouco abordado no âmbito

[70] No original: "I don't want to live in a world where everything I say, everything I do, everyone I talk to, every expression of creativity and love or friendship is recorded".

acadêmico, tem a intenção de se constituir em um auxílio para a compreensão do esquema de monitoramento central, para avaliar suas características e sua estreita ligação com os discursos que são estudados na subseção final da presente dissertação.

3.1 AS FONTES DE INFORMAÇÃO: O ACERVO SNOWDEN

Uma porção substancial da informação existente sobre as características da vigilância massiva e global de comunicações praticada pelos Estados Unidos da América provém do denominado *acervo Snowden.* Este se compõe de um amplo conjunto de documentos classificados do governo estadunidense, que o ex-agente de inteligência Edward Snowden disponibilizou originalmente para a documentarista Laura Poitras[71] e o jornalista Glenn Greenwald.[72] A sua publicação, ocorrida em meados do ano 2013, foi resultado da ação coordenada entre o próprio Snowden e três veículos jornalísticos internacionais: The Guardian, The New York Times e The Washington Post, aos quais posteriormente somou-se o restante da imprensa mundial.

À diferença de vazamentos precedentes, tais como os dos documentos correspondentes às ações militares estadunidenses no Iraque e a série *spyfiles* publicada pelo site Wikileaks,[73] este acervo não foi disponibilizado de forma massiva ao público. Não existem dados precisos em relação ao volume

[71] No ano 2014, Poitras lançou o documentário Citizenfour, filmado durante os encontros mantidos entre esta, Snowden, Greenwald e MacAskill em Hong Kong, na preparação da difusão dos documentos Snowden. Mais informações em: https://citizenfourfilm.com/ acessado em 13 de setembro de 2016.

[72] Na época, Greenwald era colunista do Jornal e site de noticias The Guardian e atualmente é um dos três co-fundadores do site de noticias The Intercept, o qual mantém edições em inglês e português. Ex-advogado, pesquisa sobre vigilância massiva desde o ano 2005, com matérias publicadas no seu blog "Unclaimed Territory" e em seus livros "How Would a Patriot Act" e "Tragic Legacy", nos anos 2006 e 2008, respectivamente. Em 2014, finalmente, publicou seu livro "Sem lugar para se esconder" no qual relata o processo que levou à divulgação do acervo Snowden e analisa seu conteúdo.

[73] Segundo sua própria descrição, Wikileaks constitui uma organização de mídia multinacional e uma livraria dos "documentos mais perseguidos a nível global". Fundada em 2006 por Julian Assange, especializa-se na publicação de grandes volumes de documentos secretos ligados "à guerra, à espionagem e à corrupção". Até o momento, publicou mais de 10 milhões de documentos (WIKILEAKS, 2015e).

total de documentos extraído por Snowden nem da quantidade que foi repassada para os jornalistas. De fato, segundo declarações dos protagonistas, sabe-se que uma significativa quantidade permanece ainda sem publicação, sendo anunciado que uma porção desses não serão publicados por considerar-se contrários ao direito à privacidade (como, por exemplo, o caso de publicações privadas) e que uma vasta parcela do acervo está reservada para futuras tarefas de pesquisa e redação de matérias para serem divulgados (THE INTERCEPT, 2016).

Greenwald argumenta que as características específicas que assumiu a publicação do material foram definidas a partir de duas demandas emanadas do próprio Snowden no momento de entregar o material. A primeira teria sido que todas as publicações dos documentos se dessem no marco de matérias jornalísticas que tornassem ditos documentos compreensíveis para o público e os contextualizassem. Adicionalmente, o ex-agente de inteligência estadunidense teria requerido que cada documento fosse trabalhado cuidadosamente, a fim de proteger "o bem-estar e as reputações de pessoas inocentes" (GREENWALD, 2016, parag. 1). É por este motivo que, dentre outros dados, todos os nomes dos funcionários de menor nível na estrutura das agências de inteligência (tais como os autores das reportagens e apresentações) têm sido suprimidos dos documentos antes destes serem publicados. É também por isto que os vazamentos têm se prolongado ao longo dos anos, na medida em que o esforço de pesquisa dos jornalistas consegue identificar documentos de interesse público e trabalhe sobre eles.[74]

[74] Até o momento de entrega da presente dissertação, o último conjunto de documentos foi publicado no dia 10 de Agosto de 2016 e corresponde a um conjunto de artigos da *SIDtoday,* a publicação interna da divisão mais importante da NSA: a diretoria de sinais de inteligência. No caso destes arquivos, o site The Intercept ilustra os procedimentos que tiveram de ser feitos pela equipe de pesquisadores para torná-los acessíveis. Salientam, entre outras questões, a necessidade de superar a limitação dos arquivos estarem desenhados para ser acessados desde dentro da rede privadas da NSA. Para isto, a equipe precisou criar um software específico, capaz de extrair o conteúdo dos arquivos originais e convertê-lo ao formato PDF. O trabalho posterior sobre o conteúdo incluiu a identificação de nomes pessoais que deveriam ser ocultos, elaborar resumos dos conteúdos e elaborar a pesquisa geral sobre os dados e suas possíveis ligações com outras histórias já publicadas sobre o assunto (THE INTERCEPT, 2016). O arquivo completo da publicação encontra-se disponível em: https://theintercept.com/snowden-sidtoday/update-reports/ acessado em 20 de setembro de 2016.

O acervo conforma-se de um conjunto heterogêneo de materiais tais como apresentações, comunicações internas e outros documentos. Dentre as primeiras, incluem-se documentos confeccionados pelos próprios funcionários da NSA, orientados a capacitar novos operadores dos sistemas ou a detalhar as características dos programas de coleta de informação, dos mecanismos de processamento e dos de armazenamento de informação. Inclui também correios eletrônicos, informes executivos (geralmente ligados ao cumprimento de alguma meta de gestão) e edições de boletins de circulação interna.

Ainda é por essa diversidade de materiais que se explica a riqueza e a importância do vazamento. Este aportou à opinião publica internacional um conjunto coerente de informações que melhorou significativamente a compreensão sobre a escala e sobre os aspectos operativos do sistema de monitoramento de comunicações. Possibilitou conhecer os recursos técnicos utilizados para a interceptação dos dados e as particularidades das agências vinculadas ao desenvolvimento do sistema, assim como apreender, através das diversas apresentações e comunicações oficiais, os objetivos pretendidos de tal sistema. Inclusive, cabe salientar que sua validade não foi questionada por parte do Governo dos Estados Unidos nos seus aspectos fundamentais (PARLAMENTO EUROPEU, 2014b, p. 9). Ainda mais, em diversas instâncias, oficialmente foi reconhecida a existência dos programas aos quais se faz referência nos documentos em questão, tal como exemplificam as declarações oficiais do Escritório do Diretor de Inteligência Nacional (ODNI, na sigla em inglês) (ODNI, 2013) e da própria NSA (2013b).

É por isto que, embora outras denúncias já viessem acontecendo[75], foram estes vazamentos que transformaram a percepção generalizada em relação à temática. Tal como salienta

[75] Outras denúncias antecederam a publicação dos referidos documentos. Destaca-se o caso de Tomas Drake, também ex-funcionário da NSA, que em novembro de 2005 contata a imprensa para denunciar os alcances do monitoramento de comunicações com especial foco no desperdiço de recursos públicos e a corrupção no interior da NSA. Para maiores informações sobre as denúncias realizadas por Drake ver Lefébure (2014, p. 260-264). Também se destaca a série de documentos inclusos na series *spyfiles* de Wikileaks. Esta última consiste em uma série de arquivos revelados pela organização Wikileaks, que registram contratos e diversas documentações, fundamentalmente de natureza comercial, que ilustram o funcionamento da indústria da vigilância massiva a nível global. Para maiores informações ver: https://wikileaks.org/the-spyfiles.html, acessado em 18 de janeiro de 2016.

Žižek (2013), a sua relevância explica-se porque eles oferecem à opinião pública internacional bases concretas sobre as quais avaliar as suspeitas de monitoramento existentes até então.

Na elaboração da descrição a seguir, foram consultados três tipos de fontes: os próprios documentos Snowden[76], tal como publicados pelos diversos veículos jornalísticos como suporte às diferentes matérias e, geralmente, disponibilizados nos sites DocumentCloud[77] e EdwardSnowden;[78] pesquisas de natureza jornalística; e, finalmente, as pesquisas e os inquéritos desenvolvidos pela Organização das Nações Unidas (ONU) e pelo Parlamento Europeu. Nos últimos três anos, ambas as instituições têm levado adiante uma série de processos que derivaram na publicação de dois relatórios que também conformam as fontes nas quais se funda a descrição das páginas seguintes.

3.2 SABER TUDO, COLETAR TUDO, ANALISAR TUDO: A RACIONALIDADE DO PODER PUNITIVO.

> A falta de uma visão sintética da Internet frustra os esforços para desenvolver a análise de ameaças na Internet e as

[76] Sempre que possível, estes documentos são referenciados de maneira direta, privilegiando os sites EdwardSnowden e DocumentCloud como referências de endereço eletrônico. As datas, de forma geral, correspondem presumivelmente à autoria ou à apresentação tal como figuram no próprio documento. Nos casos em que não figurou essa informação, foram consideradas as datas de classificação por parte da autoridade competente; e, quando não figurou nenhuma dessas datas, optou-se por fazer constar a data de publicação. Finalmente, salvo exceções, considera-se os documentos como de autoria institucional da NSA. Neste sentido, dada a pluralidade de agências estatais dos Estados Unidos com as quais se trabalha na presente dissertação, resolveu-se catalogar cada uma, diferenciando a autoria das diversos escritórios responsáveis pela elaboração dos mesmos.

[77] Fundado no ano 2009, o site DocumentCloud foi desenhado como uma ferramenta para administrar e publicar online documentos de fontes primária, tendo sido projetado fundamentalmente para o auxilio das tarefas de jornalistas, de pesquisadores e de arquivistas. Para maiores informações consultar: https://documentcloud.org/about. Acessado em 20 de setembro de 2016.

[78] Trata-se de um site que opera sob a órbita da Courage Foundation e está especificamente dirigido à difusão dos documentos vazados e a dar publicidade a evolução da situação legal de Snowden (sua condição de asilado na Rússia e as diversas das denúncias que pesam sobre ele nos Estados Unidos). Para maiores informações consultar: <https://edwardsnowden.com> acessado em 26/09/2016.

> capacidades de indicação e aviso[79] (EUA, 2002, p. 22, tradução livre).
>
> Estamos ingressando na idade de ouro da HLT [Tecnologia da Linguagem Humana, sigla em inglês]. Computadores poderosos e de baixo custo, redes de alta velocidade e algoritmos avançados estão sendo combinados para revolucionar a estação de trabalho do analista[80] (NSA, 2006, tradução livre).
>
> Nova postura de coleta: Farejar tudo, saber tudo, coletar tudo, processar tudo, explorar tudo, dividir tudo com parceiros (NSA, 2011, tradução GREENWALD, 2014, p. 104).

Os atentados acontecidos em 11 de setembro de 2001 nos Estados Unidos configuram um elemento chave para compreender a estrutura atual do sistema de vigilância massiva de comunicações. Após esses eventos uma serie de programas foram impulsionados por parte do executivo estadunidense com o objetivo declarado de monitorar as comunicações para *evitar um novo ataque terrorista*. Essa orientação ficou registrada na denominada Lei Patriota (EUA, 2001b) norma que, sancionada apenas seis semanas após os atentados, ampliou significativamente os poderes investigativos dos diversos órgãos de inteligência (FINLEY; ESPOSITO, 2014; LEFÉBURE, 2014) e levou a uma fusão nos esforços das agências de segurança e defesa (CAVELTY, 2007a, p. 105). Idêntica orientação tem servido de justificativa das restantes normativas públicas que modelaram o sistema dentre as quais se destacam: a Lei de Proteção dos Estados Unidos[81] (EUA, 2007), a Emenda à Lei de Vigilância da Inteligência Estrangeira (FISA, na sigla em inglês) (EUA, 2008c) assim como uma série de Autorizações Presidenciais de caráter classificado (EUA, 2009, p. 1-5). Em

[79] No original: “The lack of a synoptic view of the Internet frustrates efforts to develop Internet threat analysis and indication and warning capabilities”.
[80] No original: “We are entering a golden age for HLT. Powerful and inexpensive computers, high speed networking, and advanced algorithms are being combined to revolutionize the analyst desktop”.
[81] No original: “Protect America Act”.

definitiva, nesse período configurou-se um esquema de coleta de informações centralizado na NSA e que atingiu uma escala sem precedentes (EUA, 2009, p. 37-42).

Neste sentido, Uma primeira conclusão da leitura que conformam o acervo Snowden é que o sistema encabeçado pela NSA se orienta a abarcar o conjunto mais amplo possível de informações digitalizadas a nível global. Para tal fim destinam-se importantes recursos públicos que tem transformado à agência em uma estrutura administrativa de importante magnitude e escala transnacional. Segundo declarações oficias do seu Chefe na época, Michael Rogers, para o ano 2015 o complexo conformado pela NSA e pelo, mais recente, Serviço Central de Segurança (CSS, na sigla em inglês) possuía 40.000 empregados entre civis e militares. A força laboral era conformada de: "analistas, compiladores, operadores, matemáticos, lingüistas, criptógrafos, engenheiros e cientistas da computação"[82] , dentre outros. Aliás de sua sede central em Maryland, contava na época com estabelecimentos em 31 estados dos Estados Unidos assim como "presença em locais ao redor do mundo"[83] (ROGERS, 2015c, p.1).

De fato, ele define a agência como uma "organização global". Em ocasião de uma palestra celebrada nos Estados Unidos, perante um público composto por diversos executivos de companhias privadas transnacionais, o titular da NSA argumentou: "Vamos dar-lhe a oportunidade de viajar. Somos uma organização global como muitos de vocês. Então, se você gosta de se movimentar, se você gosta de ver muitas partes do mundo, nós podemos fazer isso por você"[84] (ROGERS, 2015b, p. 18).

O objetivo da presente seção, neste sentido, é o de fazer uma descrição analítica dos mecanismos concretos através dos quais tem se desenvolvido a vigilância massiva de comunicações com base na informação vazada pelo ex-analista de inteligência estadunidense.

---

[82] No original: "analysts, collectors, operators, mathematicians, linguists, cryptographers, engineers, computer scientists"

[83] No original: "presence at locations around the world".

[84] No original: "We're going to be giving you the opportunity to travel. We're a global organization just like many of you. So, if you like moving around, if you like seeing lots of parts of the world, we can do that for you".

Uma primeira dimensão a estudar neste sentido é que os programas de coleta, de processamento, de compartilhamento e de armazenamento das informações se sustentam: de um lado em uma rede de alianças transnacionais das quais participam agências de segurança de um conjunto seleto de estados nacionais e, de outro, no lugar central que os Estados Unidos ostentam na infraestrutura das telecomunicações globais.

A respeito do primeiro aspecto, nos documentos vazados se comprova a existência de associações internacionais[85] de dois níveis. Um primeiro nível, hierarquicamente mais elevado, é o derivado do denominado "Acordo dos cinco olhos"[86] que compreende a cooperação ativa das agências de segurança nacional da Nova Zelândia, do Canadá e da Austrália com os Estados Unidos. Através desta associação as agências participantes compartilham os dados coletados de forma massiva (PARLAMENTO EUROPEU, 2014b, p. 15) no marco de um esquema que a NSA denomina de "cooperação abrangente" (NSA, 2014b).

Um segundo nível de associação se da a respeito dos chamados pela NSA de parceiros de "terceiro nível" ou "grupo b", conformado por um listado notavelmente mais numeroso de países com os que a agência mantém vínculos de "cooperação focada" (NSA, 2014b): Alemanha, Arábia Saudita, Argélia, Áustria, Bélgica, Cingapura, Coréia do Sul, Croácia, Dinamarca,

[85] Na prática, estas formas de cooperação parecem amplamente coincidentes com aquilo que de um lado Martin Libcki (1998) e de outro, John Arquilla e David Ronfeldt (1999), reconhecidos pesquisadores da corporação RAND, no âmbito da defesa dos Estados Unidos propunham no sentido de dar origem a um sistema que servisse para "iluminar o cibrespaço". Já no final da década de 1990 ambos argumentavam a conveniência de criar "uma grade para os militares iluminarem o mundo- um sistema global de comando, controle, comunicações, computação, vigilância e reconhecimento, instalado e sustentado pelos Estados Unidos, cuja informação estaria disponível para os militares do mundo todo sempre que eles concordem em iluminar seus próprios desdobramentos militares e outras atividades" (ARQUILLA; RONFELDT, 1999, p. 43).

[86] Como se argumenta no relatório do Comitê de Liberdades Civis, Justiça e Assuntos Internos do Parlamento Europeu, a existência dessa aliança já tinha sido comprovada com anterioridade à publicação do acervo Snowden e se remonta à época do sistema ECHELON (sistema global de interceptação de comunicações privadas e comerciais). Nessa época, o *acordo dos cinco olhos* era conhecido como o *acordo UKUSA* (PARLAMENTO EUROPEU, 2014a, p. 80-82). O sistema ECHELON foi um sistema de vigilância baseado revelado no final da década de 1990. Através deste programa a NSA interceptava regularmente comunicações de alvos selecionados geralmente do âmbito empresarial europeu (LEFÉBURE, 2014, p. 101-108).

Emirados Árabes Unidos, Espanha, Etiópia, Finlândia, França, Grécia, Hungria Índia, Israel, Itália, Japão, Jordânia, Macedônia, Noruega, Países Baixos, Paquistão, Polônia, República Tcheca, Romênia, Suécia, Tailândia, Taiwan, Tunísia, Turquia (NSA, 2013f). Além do intercâmbio de informações essas parcerias envolvem transferências de recursos por parte da NSA em beneficio das agências dos terceiros países envolvidos (GREENWALD, 2014, p. 131-133).

Da multiplicidade de programas detalhados nos documentos Snowden e administrados de forma direta pelos Estados Unidos, descrevem-se, em seguida, aqueles considerados centrais para a prática da vigilância massiva por parte da NSA. Trata-se dos casos de dois programas de coleta (Upstream e Prism), um programa de decriptamento[87] (Bullrun) e dois programas de processamento e acesso para os analistas (Xkeyscore e Boundless informant).

O programa Upstream tem a ver com a interceptação dos fluxos de dados no momento que eles percorrem alguma instância específica da infraestrutura física das telecomunicações (tais como cabos de fibra óptica, switchers e routers).[88] Opera sob a divisão de fontes especiais (SSO, na sigla em inglês), que coordena tanto os denominados *programas unilaterais* quanto relacionamento com os *parceiros corporativos.* Sob essa última denominação, a NSA agrupa as "mais de oitenta grandes corporações globais" envolvidas nos diversos programas de coleta, dentre as quais uma das apresentações salienta as

[87] O termo criptografia remete à técnica através da qual se transformam conteúdos de sua forma original (chamada também de texto aberto) em um formato que os torna ininteligíveis (ou texto cifrado). As técnicas modernas se baseiam na aplicação de algoritmos cuja força do código criptográfico (isto é, a dificuldade de quebrar o código) reside em problemas matemáticos. Na atualidade, uma das principais áreas de aplicação da criptografia é na denominada *segurança na rede*, campo que engloba os assuntos vinculados à garantia da privacidade, à autenticação do ponto final (isto é, a confirmação da identidade), à integridade das mensagens e à segurança operacional (KUROSE; ROSS, 2005, p. 675–676). Quase a totalidade dos equipamentos e plataformas de uso cotidiano empregam algum tipo de ferramenta criptográfica, embora o usuário não esteja ciente disto.

[88] Trata-se de três componentes característicos do funcionamento das redes de computadores. Os cabos de fibra óptica são responsáveis, na atualidade, pelo transporte de uma porção ostensiva do tráfego global de dados. Router e switchers, por sua vez, constituem elementos centrais na organização dos dados enviados e recebidos. Para maior informação, consultar Kurose e Ross (2005, p. 22-35).

firmas: AT&T, CISCO, IBM, Oracle, Microsoft, HP, Verizon e Motorola (NSA, 2014a).

A centralidade da participação destas companhias refere-se ao fato de que se trata dos maiores operadores de infraestrutura de telecomunicações a nível global. Neste sentido, os acordos possibilitam à NSA explorar o acesso que estas empresas possuem aos sistemas internacionais, tanto por conta própria como estabelecendo esquemas de cooperação na criação, suporte ou melhoria de redes com outras companhias, as quais passam a redirecionar os fluxos de dados para repositórios da agência.

Em termos da estrutura organizacional, a coleta dos dados no marco do Upstream se efetua através de um complexo de programas orientados a explorar os diversos recursos estratégicos que o relacionamento com cada parceiro oferece. Segundo se depreende de uma das apresentações da agência, o subprograma Blarney é encarregado de: "obter parcerias-chave exclusivas com empresas que permitam o acesso a cabos de fibra óptica e/ou roteadores internacionais de alta capacidade localizados em diversas partes do mundo"[89] (NSA, 2013d, tradução GREENWALD, 2014, p. 110).

Um segundo subprograma é o Fairview sobre o qual se afirma, em uma das apresentações internas da agência da NSA (2015b, p. 5–6, tradução livre), que possibilita o "acesso a imensas quantidades de dados". Embora não se mencione a companhia envolvida, afirma-se no documento que se trata de um "parceiro corporativo chave com acesso a cabos, roteadores e comutadores internacionais". Neste sentido, no mesmo documento salienta-se o "esforço cooperativo associado à coleta de pontos intermediários" e se explica a grande relevância do parceiro porque "opera dentro dos Estados Unidos, mas tem acesso a informações que transitam pelo país e, graças às suas relações corporativas, proporciona acesso privilegiado a outras telecoms[90] e ISPs [Provedores de serviços de Internet]".[91]

[89] Segundo se afirma em uma matéria publicada no Wall Street Journal, a principal corporação participante do subprograma Blarney é o gigante das telecomunicações AT&T (GORMAN; VALENTINO-DEVRIES, 2013).

[90] Termo frequentemente empregado como referência às firmas atuantes no segmento das telecomunicações.

Um ponto adicional salientado pela agência é que o parceiro em questão "[r]ealiza modelagem de tráfego agressiva para fazer os sinais passíveis de interesse transitarem por nossos monitores" (NSA, 2015a, tradução GREENWALD, 2014, p. 111). Em uma linha similar opera o subprograma Stormbrew, que coleta dados desde sete locais de acesso, denominados pela agência "gargalos" internacionais, pelos quais passa a grande maioria do tráfego de internet do mundo em alguma fase da sua etapa de trânsito. Neste sentido, como salienta Greenwald (2014, p. 113), este programa constitui um subproduto residual do papel central desempenhado pelo país no desenvolvimento da rede.

Em resumo, pode-se afirmar que o que resulta característico das práticas de coleta resumidas dentro do programa Upstream é o aproveitamento da supremacia que, em termos da infraestrutura das telecomunicações, possuem os Estados Unidos. Esta supremacia pode ser vista desde duas perspectivas. A primeira, da centralidade que o território estadunidense possui na circulação dos dados a nível global (maioria dos pontos de intercâmbio passam em algum ponto por esse espaço geográfico), o que é referido pela agência como coleta em trânsito (NSA, 2013d, p. 3). A segunda, da liderança completamente superlativa que os operadores com sede legal nesse país têm sobre o restante da infraestrutura mundial.[92]

Em ambos os casos, o Estado estadunidense estabeleceu parcerias, presumidamente com diversos graus de coerção derivada da aplicação da legislação doméstica, que garantiram às suas agências de segurança um acesso praticamente irrestrito sobre os fluxos das comunicações globais – seja no momento da passagem física desses dados pelo território estadunidense, seja por sua remissão por parte dos operadores de telecomunicações. Assim, como expresso pelo então Diretor da NSA, Gen. Keith Alexander, ao prestar

---

[91] No original: "The partner operates in the U.S., but has access to information that transits the nation and through its corporate relationships provides unique access to others telecoms ISPs".

[92] Em ambos os casos, esta supremacia não constitui apenas um reflexo do diferencial tecnológico existente entre os Estados Unidos e o resto do mundo, mas ela produz assimetria de poder e é, por sua vez, reproduzida por essa assimetria. Neste sentido, tal como salienta Greenwald, as empresas do setor tecnológico estadunidense são desestimuladas a contratar fornecedores de equipamento de países potencialmente concorrentes, como a China (GREENWALD, 2014, p. 156).

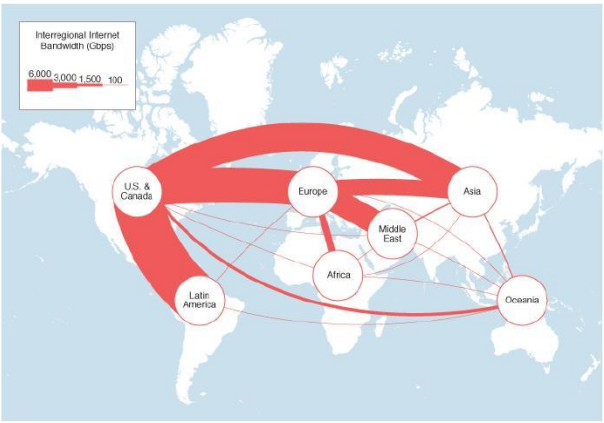
depoimento perante o Comitê judicial do Senado estadunidense no ano 2006, “uma das grandes vantagens em nosso esforço de coleta de inteligência estrangeira é nossa habilidade para acessar uma vasta proporção da infraestrutura de comunicações mundial que está localizada em nosso próprio território”[93] (ALEXANDER, 2006, parag. 5, tradução livre).

Neste sentido, cabe salientar que, embora a Internet se baseie em um desenho descentralizado, constitui uma rede fortemente hierarquizada que se articula em torno a um conjunto de pontos nodais, cuja distribuição territorial é marcadamente desigual (BUZAI, 2012, 2014). Como ilustrado a seguir, os Estados Unidos constituem o centro de maior circulação de dados de telecomunicações globais. Essa dependência resulta ainda maior no caso da América Latina, que praticamente não possui interconexões interregionais além das que mantém com o norte do continente.

Sobre este último ponto, cabe salientar que a maioria dos enlaces internacionais da região se efetua através de pontos de intercâmbio de tráfego (IXP, na sigla em inglês) localizados nos Estados Unidos, resultando em que, no ano 2011, mais de 80% do largo da banda estivesse conectado com esse país, numa proporção superior à de qualquer outra região do mundo (CEPAL, 2012).

[93] No original: “one of our greatest advantages in our effort to collect foreign intelligence- the ability to access a vast proportion of the world's communications infrastructure located in our own nation”.

Desenho 1 - Largo da Banda inter-regional. Ano 2016



Fonte: TeleGeography (2016).

O segundo dos grandes programas de coleta de informação é o Prism. Este se funda principalmente na exploração do predomínio sobre Internet, por conta do fato de que a quase totalidade das grandes firmas líderes no segmento de aprovisionamento de serviços online dessa rede encontram-se sediados nesse país. A coleta sobre este programa também se sustenta no estabelecimento de parcerias não só com gigantes das telecomunicações globais, mas também com operadores de serviços de Internet (ISP). Sempre segundo os documentos que compõem o acervo Snowden, através deste programa a NSA tem capacidade de acessar tanto a informação em fluxo quanto os dados armazenados nos repositórios das companhias privadas, os quais compreendem: correios eletrônicos, conversas (chats), vídeos, fotografias, arquivos diversos, dados de atividade (nomes de usuário, detalhes de atuação em redes sociais na Internet, etc.) dados de voz por IP (Protocolo de Internet, sigla em inglês) e videoconferência, dentre outros (NSA, 2013c, p. 5).

A conformação da escala que o Prism tinha no momento do vazamento foi o resultado de um processo de incorporação gradual de novas companhias operadoras de serviços online. Segundo detalha uma apresentação interna da Agência, a firma Microsoft teria sido a primeira a incorporar-se no programa de compartilhamento de informações no final do ano 2007, seguida

por Yahoo em 2008, Google, Facebook e PalTalk em 2009, YouTube em 2010, Skype e America On Line (AOL) em 2011 e, finalmente, a companhia Apple em finais de 2012 (NSA, 2013, p. 7).

Os alcances das práticas de cooperação com operadores do setor privado enquadradas sob este programa resultam expressivos. No caso da Microsoft, por exemplo, um dos documentos vazados por Snowden, que corresponde a uma comunicação interna da NSA do mês de abril de 2013, descreve o trabalho conjunto de técnicos dessa empresa e do FBI para "implantar" uma solução que possibilitasse aos analistas dispensar-se de apresentar uma solicitação especial para acessar os dados armazenados no Skydrive que, na época, contava com 250 milhões de usuários no mundo (NSA, 2013a). No mês seguinte, outra comunicação interna relata uma substantiva melhora nas capacidades de coleta ligadas às comunicações armazenadas no serviço Skype. O documento relata que, a partir desse momento, esperavam receber "registros de dados de ligações, informações de conta de usuários e outros materiais". Nesse sentido, destaca-se, no mesmo relatório, que "[a] coleta do PRISM no Skype criou, em menos de dois anos, um nicho vital de informações para a NSA cujos tópicos mais importantes foram terrorismo, oposição e regime na Síria, além de informações executivas/séries especiais" (NSA, 2013e, tradução GREENWALD, 2014, p.121).

Tal como referido no caso do programa Upstream, o Prism também possui uma abrangência global definida pelo predomínio indiscutível que as companhias participantes do sistema de coleta possuem no segmento de aplicações online. Cabe salientar que este segmento de atividade se caracteriza por possuir um elevado grau de concentração com um conjunto reduzido de grandes companhias que operam em escala global.[94]

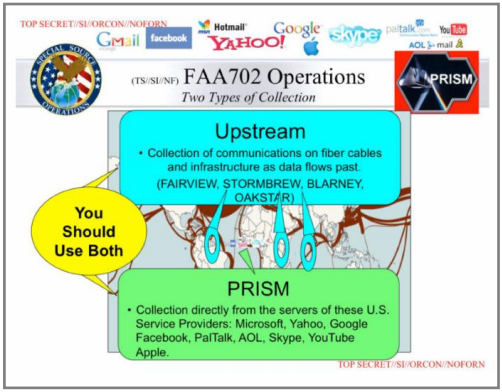
[94] O predomínio absoluto destes ofertantes é sustentado sobre a base de vantagens comparativas e efeitos de rede, resultando em elevadas barreiras para o acesso de competidores potenciais (KATZ, 2015). Estas barreiras são sustentadas e, por sua vez, reforçadas sob o domínio no âmbito das instituições no marco da denominada *governança* da Internet, as quais influem no desenvolvimento concreto da rede através da definição de protocolos e outros aspectos técnicos (COGBURN, 2016; DENARDIS, 2012, 2013; DENARDIS; MUSIANI, 2016; LACAZE, 2016a).

No caso do Prism, trata-se das empresas líderes nos segmentos de comunicações por correio eletrônico, por mensagens instantâneas e por vídeo-ligação, assim como também dos segmentos de redes sociais e ferramentas de buscas, os quais concentram uma porção substancial do tráfego global de dados.

A modo de exemplo, cabe salientar que a Google ostenta uma quota de mercado que atinge aproximadamente 88% dentro do segmento de ferramentas de busca, segundo dados correspondentes a meados de 2016 (STATISTA, 2016). No segmento de telefones inteligentes, o tipo de dispositivo de crescimento mais acelerado no mercado, Google também constitui um participante com posição absolutamente dominante. Através de seu sistema operativo Android, encontra-se presente em 85,2% dos novos aparelhos, segundo dados correspondentes ao primeiro semestre de 2016 (RICHTER, 2016). Em meados de 2013, ativavam-se 1,3 milhões de novos aparelhos funcionando sobre a plataforma Android por dia. Ainda, 2,34 bilhões de pessoas no mundo são usuários de redes sociais, isto é, 68,5% do total de usuários de Internet e 31% da população mundial (EMARKETER, 2016). Na média correspondente ao primeiro semestre de 2016, a plataforma Facebook teve 1,7 bilhões de usuários ativos, enquanto WhatsApp, outra grande líder das comunicações digitais pertencente ao mesmo grupo, teve 1 bilhão de usuários.

O grande diferencial do Prism, como ilustrado nas apresentações da NSA (Desenhos 2 e 3), é que ele possibilita o acesso a comunicações armazenadas nos próprios reservatórios das companhias de Internet, enquanto o Upstream só possibilita os organismos de segurança acessarem o fluxo de informações.

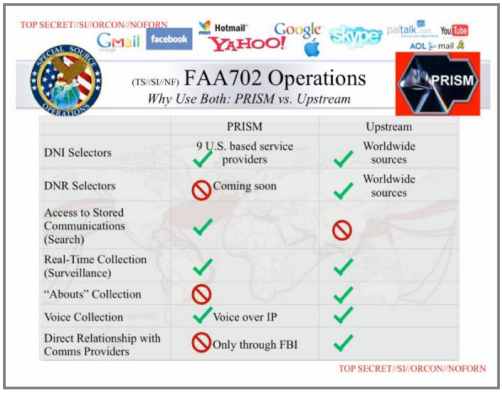
Desenho 2 - Características dos sistemas de coleta de dados



Dois tipos de coleta / Você deve usar ambos
UPSTREAM/ Coleta de comunicações em cabos de fibra e infraestruturas à medida que o fluxo de dados ocorre.
PRISM / Coleta direta dos servidores dos seguintes provedores de serviços dos Estados Unidos: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple.

Fonte: NSA (2012d, p.3)

Desenho 3 - Características dos sistemas de coleta de dados



Por que usar ambos: PRISM versus UPSTREAM
Coluna da esquerda: seletores de DNI/ seletores de DNR / Acesso a comunicações armazenadas (busca) / Coleta em tempo real (vigilância) / Coleta de "sobres" / Coleta de voz
Relação direta com provedores baseados nos EUA Em breve / Voz por IP / Somente via FBI
Coluna da direita: UPSTREAM / Fontes mundiais / Fontes mundiais.

Fonte: NSA (2012c, p.4).

A extrema relevância destas práticas de cooperação dos operadores privados no desenvolvimento do sistema de vigilância massiva de comunicações ficou ilustrada na época de debate sobra a Emenda à Lei FISA (EUA, 2008c) e de sua antecessora de 2007, a Lei de Proteção dos Estados Unidos[95] (EUA, 2007). Uma das previsões mais importantes destas legislações foi o desenho de um marco legal de proteção para a atividade de colaboração dos operadores privados no fornecimento de dados às agências de segurança. Em especial, na Emenda sobre a Lei FISA do ano 2008, outorgou-se uma imunidade de característica retroativa[96] para aquelas empresas que tivessem colaborado com os Estados Unidos entre o 11 de setembro de 2001 e a data de promulgação da Lei. Em um comunicado oficial, a Casa Branca afirmava que "a retroatividade na proteção de responsabilidade é crítica para nossa segurança nacional" (EUA, 2008a). E, a instâncias da promulgação da Emenda, em 2008, o então presidente estadunidense declarava que: "assegurará que aquelas companhias cuja assistência é necessária para proteger o país sejam elas mesmas protegidas de demandas legais por cooperações com o governo realizadas no passado ou no futuro"[97] (BUSH, 2012, p. 1007, tradução livre).

[95] Nesta, prevê-se que o Diretor Nacional de Inteligência possa aprovar a coleta de informações que pressupunham a "obtenção da informação de ou com o auxilio de provedores de serviços de comunicação, custódios ou outras pessoas […] que tenham acesso às comunicações, tanto quando armazenadas como na etapa de transmissão, ou ao equipamento empregado para transmitir ou armazenar ditas comunicações" (EUA, 2007, seç. 105B).

[96] A questão da imunidade retroativa foi um dos aspectos de maior controvérsia na época, sendo um dos pontos de maior interesse para as autoridades estadunidenses. Preocupados pela aparição de outras propostas de Emenda que não contemplavam dita disposição, a Casa Branca emitiu um comunicado salientando a total relevância da mesma. Nessa nota, argumentava-se que: "Não outorgar uma proteção retroativa sobre a responsabilidade irá minar a predisposição do setor privado a cooperar com a Comunidade de Inteligência, cooperação que é essencial para proteger [os Estados Unidos da] América. As companhias podem estar menos desejosas de assistir no futuro o governo enfrentar uma ameaça de ações judiciais privadas cada vez que são convocadas para brindar assistência" (EUA, 2008b). Um segundo comunicado oficial afirmava que: "A administração opõe-se a qualquer emenda que exclua uma proteção sobre responsabilidade retroativa porque quaisquer empresas que possam ter colaborado com o Governo após o 11 de setembro tiveram garantido que sua cooperação era legal e necessária" (EUA, 2008a).

[97] No original: "It will ensure that those companies whose assistance is necessary to protect the country will themselves be protected from lawsuits for past or future cooperation with the Government."

A efetiva capacidade de acessar os dados coletados de forma inteligível depende desta agência conseguir quebrar os códigos de encriptação que protegem a informação de intromissões na etapa de trânsito.[98] Na maioria das comunicações (como os correios eletrônicos, as ligações e os chats) e das transações (por exemplo, as bancárias ou de cartão de créditos), emprega-se algum tipo de ferramenta criptográfica como mecanismo de proteção dos conteúdos perante terceiros, geralmente sem que o usuário final seja plenamente consciente disso. Precisamente, o programa Bullrun (corrida de touros) agrupa várias ações orientadas a desenvolver mecanismos que possibilitem à NSA superar as travas que o uso de criptografia coloca para a capacidade da agência conseguir aproveitar os dados coletados.[99]

Em uma apresentação elaborada pela contraparte britânica da NSA, a Central de Comunicações do Governo[100] (GCHQ, sigla em inglês), afirma-se que, ao longo da última década, a agência estadunidense desenvolveu um "esforço agressivo voltado a quebrar as tecnologias de encriptação mais amplamente difundidas", [101] o que possibilitou que "grandes volumes de dados que até o momento tinham de ser descartados possam ser explorados na atualidade"[102] (GCHQ, 2014). Com essa orientação no marco do projeto, tem-se desenvolvido tarefas ligadas tanto à quebra dos códigos, quanto a acordos com as principais empresas do setor que possibilitassem à agência coletar dados com antecedência à sua encriptação ou

[98] Ver nota 87.

[99] Como salienta Cavelty (2007a, p. 48–53), a difusão no uso de ferramentas criptográficas constitui uma longa preocupação para o governo estadunidense. O autor afirma que, já na década de 1970, a NSA exercia um intenso controle sobre a publicação de resultados de pesquisas e sobre a cooperação no âmbito acadêmico. De fato, argumenta que já na década de 1980 as instituições de segurança nacional estadunidense se mostravam crescentemente preocupadas pela sua inabilidade para acessar as comunicações protegidas por mecanismos de encriptação. Inclusive, até o ano 1996, o governo estadunidense proibia as exportações de sistemas que oferecessem uma tecnologia de encriptação superior a 40 bits, as quais classificava como *munições*.

[100] Como destacado no começo da presente seção, a coordenação entre as agências estadunidense e britânica se deu no marco do denominado "Acordo dos cinco olhos".

[101] No original: "For the past decade, NSA has lead an aggressive, multi-pronged effort to break widely used Internet encryption technologies".

[102] No original: "Vast amounts of encrypted Internet data which have up till now been discarded are now exploitable".

que facilitassem as chaves que habilitam a agência a desencriptar os dados coletados (LARSON; SHANE, 2013). Ainda cabe salientar que, para atingir este propósito de superar as travas para o acesso aos dados digitais globais, a NSA explora o papel que ostenta como referência no desenho de protocolos criptográficos. Nesta linha, dos documentos orçamentários do programa Bullrun, depreende-se que a NSA investe USD 250 milhões em ações orientadas a influenciar os desenhos dos produtos oferecidos pelas companhias de tecnologia (GREENWALD; BALL; et al., 2013).

No caso do processamento e acesso aos dados por parte dos analistas, distinguem-se os programas Xkeyscore e Boundless Informant (informante sem limites).

O primeiro programa, Xkeyscore, está especificamente orientado a possibilitar consultas sobre metadados e conteúdo das comunicações. Processa e organiza em base de dados o conjunto de informações digitais coletadas, que compreende tanto aquelas identificadas como relevantes (na expressão da agência: *marcadas* ou *casos de êxito*), quanto as que não foram classificadas como de interesse. Em outras palavras, habilita consultas sobre todos os dados recebidos e sem filtrar, os quais são armazenados por um período que, em 2008, era de 3 a 7 dias no caso do conteúdo e de 30 a 45 dias no caso dos metadados,[103] em uma estrutura que na época se estendia sobre mais de 500 servidores distribuídos no mundo[104] (NSA, 2008). A quantidade e variedade desses dados são muito amplas, tornando um desafio técnico seu processamento e disposição para o acesso. Neste sentido, em uma das apresentações de capacitação para novos operadores do sistema, faz-se permanente referência à necessidade de que os analistas procurem realizar consultas utilizando seletores fortes, isto é, mecanismos de busca orientados a precisar os resultados da mesma. Por exemplo, salienta-se que o sistema extrai e organiza

[103] No caso dos dados serem efetivamente identificados como de interesse, segundo quaisquer critérios de análise, são conservados a largo prazo em repositórios da agência como, por exemplo, os que operam sob os programas Pinwale e Turmoil (NSA, 2010a).

[104] Segundo The Intercept, no ano 2008 a estrutura se estendia sobre 700 servidores em 130 pontos localizados, dentre outros países, nos Estados Unidos, no México, no Brasil, no Reino Unido, na Espanha, na Rússia, na Nigéria, na Somália, no Paquistão, no Japão e na Austrália (MARQUIS-BOIRE et al., 2015).

todos os dados de buscas geradas a partir de ferramentas de buscas web (tal como o site Google) e que essas podem ser consultadas de maneira retrospectiva, mas se enfatiza a necessidade do analista refinar os termos dessa consulta para limitar a quantidade de resultados devolvidos (NSA, 2008, p. 20).

Assim, as buscas podem ser feitas em retrospectiva, mas também em tempo real ou em prospectiva. Esta última, através da solicitação ao sistema de monitoramento sobre usuários que acessem a um determinado site, dando como resultado ao analista uma listagem de identificadores desses alvos (NSA, 2007). Dessa maneira, o programa possibilita monitorar pessoas baseado em padrões percebidos como correspondentes a atitudes suspeitosas, as quais se identificam com base nas suas localizações, nacionalidades e nos sites por eles visitados (MARQUIS-BOIRE et al., 2015).

Como explicado em outra apresentação de capacitação, os analistas podem iniciar consultas a partir de elementos específicos: endereços de correio eletrônico, metadados de documentos[105] (tais como os .pdf[106]) ou identificadores vinculados à atividade online dos usuários (nomes de usuários, imagens de câmera web, logins, informações de perfis como os aniversários, dentre outros) (NSA, 2009a).

As apresentações orientam os analistas a procurarem indicadores de comportamento suspeito: “Procure eventos anormais. Por exemplo: alguém está usando uma língua diferente daquela da região na qual se encontra; alguém está usando criptografia; alguém está buscando na web coisas suspeitas”.[107] Em relação à encriptação, na mesma apresentação se sugere aos analistas os seguintes termos de busca: “todos os documentos em formato word encriptados no Irã” ou “a totalidade

[105] Trata-se dos dados associados a um arquivo particular que se encontram nas suas propriedades (por exemplo: Título, autor, assunto, data), assim como os ligados aos códigos correspondentes a imagens que eventualmente podem estar inseridas nos mesmos. Tal como salientado na apresentação do programa, caso estes metadados sejam específicos, podem ser empregados com mecanismo de identificação (NSA, 2009b).

[106] O Formato de Documento Portátil (PDF, na sigla em inglês) constitui um “formato de arquivo usado para apresentar e trocar documentos de forma confiável, independente do software, hardware ou sistema operacional” (ADOBE SYSTEMS INCORPORATED, 2016).

[107] No original: “Look up for anomalous events: E.g. someone whose language is out of place for the region they are in; someone who is using encryption; someone searching the web for suspicious stuff”.

de usos de PGP[108] no Irã"[109] (NSA, 2008, p. 15–16, tradução livre).[110]

Como salientado, o programa oferece ao analista a possibilidade de rastrear documentos específicos. A apresentação interna da NSA salienta que os documentos, tais como arquivos no popular formato .pdf, podem ser seguidos em função de um conjunto de dados que os individualizam. Assim, argumenta-se na apresentação, embora "nem sempre saibamos quem está enviando esses documentos, essas pessoas são *culpadas por associação* no caso de receberem/enviarem o documento. Então quem são essas pessoas?"[111] (NSA, 2009b, p. 2, tradução livre).

O segundo programa, Boundless Informant, constitui uma ferramenta desenhada especificamente para processar metadados[112] com procedimentos característicos da análise de grandes dados (Big Data Analytics) e que opera de forma remota (isto é, *na nuvem*). Trata-se da aplicação de algoritmos de

---

[108] PGP é uma sigla que significa criptografia realmente boa (Pretty Good Privacy), uma metodologia de encriptação para proteger a integridade e a privacidade do conteúdo das comunicações.

109 No original: "show me all the encrypted word documents from Iran; show me all PGP usage in Iran".

[110] Em uma linha semelhante, um documento recentemente publicado pela agência The Intercept oferece precisões sobre a política que os funcionários do FBI seguem na hora de construir perfis na condução de investigações existentes ou, ainda, para focalizar os recursos de vigilância. Trata-se do "Guia para uso de fatores raciais, étnicas, de gênero, de origem nacional, religiosas, de orientação sexual ou de identidade de gênero na avaliação e fundamentação de investigações" (FBI, 2016). Este guia, que forma parte do "Guia para investigações e operações domésticas da agência", estabelece a possibilidade de considerar esses fatores como relevantes na avaliação de outros elementos de suspeita, os quais, inclusive, podem ser empregados na própria seleção daquelas comunidades sobre as quais recaem de maneira especial os esforços em termos de coleta de informações de inteligência (THE INTERCEPT, 2017).

[111] No original: "We don't always know who is sending the documents, but they are *guilty-by-association* if they send/receive the document. So, who are they?".

[112] Os metadados constituem informações associadas a atividades específicas, como conectar-se a uma rede, navegar pela Internet, fazer buscas ou manter uma conversação. Exemplos de metadados são: as informações de autenticação como nome de usuário, senha e identificação de login, endereços IP, datas e horários de conexões, listas de contatos e detalhes sobre os equipamentos utilizados, dentre outros. No caso específico dos correios eletrônicos, cabe salientar que os elementos que compõem o encabeçado (de, para, cópia oculta, etc.) constituem metadados da mensagem, assim como o horário e a data de envio e a sua extensão, dentre outros.

extração automatizada (data mining[113]) voltados à identificação de tendências nos dados analisados e a dimensionar o alcance da própria coleta da agência[114] (NSA, 2012a). Os documentos sobre este programa mostram que, ao longo de um período de 30 dias, processaram-se um total de 97 milhões de dados relativos a comunicações digitais (como, por exemplo, correios eletrônicos) e de 124 bilhões de ligações do mundo inteiro (GREENWALD; MACASKILL, 2013). No detalhe do documento especifica-se que, no período de um mês, coletou-se 13,5 bilhões de dados correspondentes a comunicações da Índia, 2,3 bilhões correspondentes ao Brasil[115] e 500 milhões à Alemanha (GREENWALD; BALL; et al., 2013, p. 99).

Os metadados constituem informações associadas à atividade dos usuários e dos sistemas que se registram de maneira automática. Cada vez que um dispositivo digital é utilizado, conserva-se um registro com informações a respeito da identidade e da localização do usuário, assim como horário, data e duração, dentre outras informações. Constituem, assim, um conjunto de informações de grande valia (basicamente, o quando, como, onde e com quem de cada conversação ou atividade online) que, por sua própria construção, facilitam a automatização dos mecanismos orientados ao seu processamento.

Neste sentido, como salienta Lefébure (2014, p. 174–175), mesmo com independência dos diversos meios de comunicação empregados pelos usuários (chamadas telefônicas,

---

[113] A mineração de dados pode ser definida como o "uso de tecnologias computacionais para examinar grandes conjuntos de dados procurando revelar neles relações, classificações ou padrões" (THE CONSTITUTION PROJECT, 2010, p. 8).

[114] Neste sentido, um documento voltado à capacitação interna sobre o programa salienta que uma das alternativas de consulta que este habilita para os usuários é a de "selecionar um país no mapa e ver o volume de metadados, assim como obter detalhes sobre a coleta contra esse país" (NSA 2012b).

[115] A respeito da coleta relativa ao Brasil, o então diretor da NSA, longe de negar a veracidade de tais informações, pretendeu minimizar a relevância dos metadados como fonte de informação. Em uma entrevista acontecida em 2013, logo após os vazamentos comentava que: "Quanto ao Brasil – sabe, a verdade é que não estamos nem coletando todos os e-mails das pessoas no Brasil nem escutando seus números de telefone [sic]. Por que faríamos isso? O que alguém pegou foi um programa que olha metadados ao redor do mundo, que você usaria para encontrar atividades terroristas que poderiam transitar, e saltou à conclusão de que, aha, metadados – eles devem estar escutando os telefones de todo o mundo; eles devem estar lendo os correios de todo o mundo" (ALEXANDER, 2013a, p. 23, tradução livre).

SMS, correio eletrônico, chat) ou da pluralidade de tipos de atividades na rede (navegação, busca, etc.) os metadados relativos a esses eventos podem ser operados de forma agregada. Desta maneira, constituem elementos passíveis de ser esquematizados conjuntamente, com o objetivo tanto de enriquecer os perfis dos alvos da vigilância quanto para a seleção de novos indivíduos. A combinação desses dados oferece informações muito sensíveis sobre pessoas e instituições, como as suas localizações físicas, e possibilita determinar, dentre outros, padrões de comportamento e de relacionamento com outros. De fato, o caráter extremadamente individualizante da análise de metadados levou a que se cunhasse o conceito de *rastro pessoal digital* (digital footprint) para se referir a ele.

O rastro pessoal digital pode ser definido como o conjunto de dados que ficam registrados nos diversos sistemas de computadores como consequência das atividades do uso de serviços digitais. Considerada desde a óptica do envolvimento do usuário, a literatura diferencia entre os conceitos de rastro digital *ativo* e passivo. O primeiro deriva do compartilhamento ativo de informação, enquanto o segundo se compõe de registros coletados de maneira automatizada, sem envolvimento expresso do indivíduo (CNPI, 2015).

Neste sentido, uma porção substancial das informações que conformam o *rastro pessoal digital* de uma pessoa é gerada sem a expressa intencionalidade do usuário, através de dados que são coletados de maneira automatizada e processados através de mecanismos de mineração de dados que os vinculam. O resultado é a criação de perfis configurados através do relacionamento de dados de identificação pessoal (nomes, lugares, endereços de IP), de atividade (sites visitados, termos de buscas web, etc.) e de relacionamento com outros usuários.

Em resumo, pode-se afirmar, com base nos documentos referidos, que o sistema de vigilância massiva abrange não só as comunicações (correios eletrônicos, chats, conversações telefônicas), mas também a transferência de arquivos e dados armazenados na nuvem, metadados sobre atividade e conversações dos usuários e transações financeiras,[116] dentre

[116] O programa de vigilância "sigam o dinheiro" (follow the money) é orientado precisamente a coletar e analisar informações ligadas a transferências bancárias,

outros (LEFÉBURE, 2014; SPIEGEL, 2013). Além disso, a coleta de informações massivas não se circunscreve à Internet, mas alcança também a redes privadas que sejam consideradas de interesse pela agência. Assim, constituem exemplos desta prática a coleta de dados sobre transações bancárias e de comunicações de companhias aéreas, dentre outros (NSA, 2010a).

Ilustrada no princípio de *coletar tudo* (NSA, 2011), a massividade é uma característica central do sistema de vigilância de comunicações, voltado a maximizar constantemente a massa de dados que se acessa, no limite ideal de que todos aqueles novos registros de comunicações cuja absorção e catalogação sejam possíveis incluem-se nesse sistema para serem armazenados por anos em repositórios de dados maciços (GREENWALD, 2014, p. 33).

Embora o ideal de exercer uma vigilância massiva e global não constitua necessariamente uma pretensão nova, ela se dá na atualidade em um contexto que a torna tecnicamente possível e economicamente viável. Neste sentido, a convergência no uso de tecnologias digitais para um espectro cada vez mais amplo de atividades tem como contrapartida a centralização de um conjunto cada vez mais variado de informações em um único veículo. Ao mesmo tempo, a queda dos custos tanto de armazenamento quanto das tecnologias disponíveis para a interceptação e análise desses dados possibilitaram práticas antigamente inviáveis (ASSANGE et al., 2013, p. 41–53).

---

operações realizadas com cartões de crédito e transferências de dinheiro e possuía, em 2011, um total de 180 milhões de registros na base de dados Tracfin, na qual seriam armazenados por um período de cinco anos. Adicionalmente, a NSA também monitora os dados de tráfego correspondentes à Sociedade de Telecomunicações Financeiras Globais (SWIFT, na sigla em inglês), que agrupa um total de 8000 instituições no mundo inteiro e as operações de companhias de cartões de crédito como Visa e Mastercard (POITRAS et al., 2013). Neste último caso, a NSA orienta a coleta em diversos pontos das redes ligadas ao processo de autorização dos pagamentos, que começa com o leitor do cartão nos comércios e culmina no servidor central da operadora. Segundo relatado na apresentação sobre as características deste programa, ele se volta principalmente a "coletar, analisar e gerir informações sobre transações correspondentes a associações de cartões de crédito, focando em regiões prioritárias" (NSA, 2010b, p. 1, tradução livre). Adicionalmente, salienta-se o objetivo de "identificar grandes armazenagens de dados sobre titulares de cartões de crédito" e de analisar e superar os desafios ligados à sua coleta (NSA, 2010b, p. 2, tradução livre).

Como argumentam Fuchs e Trottier (2015), nas últimas décadas tem-se assistido a uma convergência de práticas de monitoramento em grande escala, orientadas tanto por interesses econômicos, quanto pela lógica securitária.

Em relação ao primeiro aspecto, cabe salientar que a atividade de monitoramento dos usuários constitui, talvez, o aspecto mais característico do modelo de negócios de Internet. A exploração comercial da informação configura um aspecto distintivo deste segmento, já que, por uma parte, o advento das tecnologias de informação e comunicação constituiu sua condição de possibilidade e, por outra, foram as diversas estratégias baseadas na valorização da informação dos usuários, seguidas pelas empresas do setor, as que explicam o exponencial crescimento das companhias do setor. Neste sentido, o esquema de negócios mais característico se foca no acesso e armazenagem em massa de dados de tráfego e conteúdo cujo processamento se realiza seguindo procedimentos de mineração de dados, com o objetivo de detectar padrões nos dados que, posteriormente, são aplicados ao desenho de estratégias de publicidade e propaganda personalizadas que contam, desta maneira, com informações provenientes de universos completos (BRUNO, 2012). Em outras palavras, trata-se de modelos de acumulação baseados em estratégias de compilação, processamento e venda de informações produzidas pelos usuários de maneira automática na sua interação com as diversas plataformas.[117]

Neste sentido, embora possa se falar que o cenário atual se caracteriza por uma vigilância distribuída, incorporada através de diversos dispositivos de uso cotidiano com propósitos e

[117] Provavelmente, um dos exemplos mais característicos é o das empresas que provêm o serviço de ferramentas de buscas. Estas não percebem recursos por parte dos usuários ativos, obtendo lucros fundamentalmente através das atividades de marketing, tanto pela venda dos dados da atividade dos seus usuários (por exemplo, termos de buscas e localizações) quanto de espaço publicitário. A própria empresa Google é identificada pela literatura como uma das primeiras a adotar o novo esquema de negócios da Internet com seu sistema AdWords. Adicionalmente, dados também são coletados com fins de melhora do próprio serviço de buscas, neste sentido a atividade de cada usuário constitui um insumo para os algoritmos adaptarem os resultados oferecidos, isto é para personalizá-los e torná-los assim mais pertinentes para o usuário (BATTELLE, 2006).

funções diferentes (BRUNO, 2009, p. 3),[118] o acervo Snowden mostra que existem estratégias orientadas a concentrá-la, organizadas em torno do princípio securitário.

Como destacado previamente, identifica-se que as estratégias delineadas após os atentados de 11 de setembro constituíram um ponto de inflexão que deu ao critério de coletar tudo ou de maximização da coleta de dados globais uma condição de emergência tanto dentro do discurso securitário contemporâneo, quanto da aplicação de recursos coletivos para tal fim.[119]

A Lei Patriota (2001b, seç. 201–225) outorgou autoridade para interceptar comunicações orais, por fio e eletrônicas, relativas ao terrorismo, à fraude com computadores e a outras ofensas, habilitando a obtenção de registros em massa. Adicionalmente previu a possibilidade de retardar a comunicação a respeito da existência de uma ordem judiciária, ofereceu imunidade àqueles provedores que entregam dados em observância da Lei e, em geral, submeteu a coleta de informação relativa a objetivos estrangeiros às provisões da Lei Federal de Inteligência Estrangeira (FISA), a qual opera sob uma estrutura de tribunais secretos. Em particular, na sua seção 217, substituiu o princípio de causa provável pelo da relevância como guia em matéria de investigação (GREENWALD, 2014, p. 37). Com a Lei de Proteção da América (EUA, 2007) e a Lei de Emendas FISA, essas capacidades legalmente atribuídas às agências estatais de segurança se ampliaram, assim como também a proteção legal oferecida aos operadores privados, como já foi referido. Em especial, a seção 702 da Lei de Emendas FISA ofereceu o enquadre legal para a atividade ligada à recopilação de dados, correspondente ao programa PRISM (EUA, 2008c; NSA, 2012c).

Como se destacou na introdução, essas provisões, junto com o esquema de monitoramento revelado a partir do acervo

[118] Além de Bruno (2013), em relação ao estudo dos diversos dispositivos de vigilância contemporâneos recomenda-se a leitura de Lyon (2007) e Fuchs (2012, 2015a, b), dentre outros.

[119] Cabe salientar, neste sentido, que as previsões legais da Lei Patriota foram acompanhadas de um incremento substancial dos recursos orçamentários destinados à NSA. Entre 2000 e 2013, a agência recebeu mais de USD 40 bilhões em investimentos e incorporou uma cifra ao redor dos 10.000 funcionários. Adicionalmente, dentre outras aplicações em infraestrutura, destaca-se o anúncio efetuado no ano 2013, quanto à criação de um banco de dados capaz de integrar 20 bilhões de comunicações por dia (LEFÉBURE, 2014, p. 205).

Snowden, foram avaliadas como contrárias aos tratados internacionais em matéria de direitos humanos e ao princípio de soberania territorial. O Parlamento Europeu argumentou que o fato de se tratar de um sistema de vigilância "sem discriminação e sem base de suspeitas" (2014b, p. 22) resulta violador do direito à privacidade tal como consagrado pela Declaração Universal dos Direitos Humanos e pelo Artigo 17 do Pacto Internacional dos Direitos Políticos e Civis (2013b).[120]

Isto porque, tal como desenvolvida pelos Estados Unidos, a vigilância de comunicações vulnera os princípios que o direito internacional exige para justificar qualquer ingerência no direito à privacidade como consagrado no Pacto Internacional sobre Direitos Civis e Políticos (ONU, 1966). Isto porque, argumenta, violam-se os princípios de necessidade e de proporcionalidade na ingerência nas comunicações privadas.[121] Assim como

[120] Como salienta Doneda (2006, p.4-91) a consagração da privacidade como um direito fundamental é resultado de um processo histórico aberto após a Segunda Guerra Mundial momento no qual esse direito passou a ter abrigo em várias declarações de direitos internacionais. Neste sentido, o autor remonta a primeira menção desse direito ao ano 1948 com a Declaração Americana dos Direitos e Deveres do Homem e a Declaração Universal dos Direitos do Homem aprovada, esta última, pela Assembléia Geral das Nações Unidas. O referido Pacto Internacional dos Direitos Políticos e Civis é um dos dois tratados sobre direitos humanos da ONU que possuem força legal após serem ratificados pelos estados membros. Nele se consagram os denominados *direitos humanos de primeira geração* que abarcam um conjunto de garantias de cunho individualistas a respeito do exercício de liberdades individuais, de acesso à justiça e de participação política (LAFER, 1997). Em específico, o Pacto estabelece no seu Artigo 17 que: "1. Ninguém será objeto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação. 2. Toda e qualquer pessoa tem direito à proteção da lei contra tais intervenções ou tais atentados." (ONU, 1966).

[121] A respeito deste assunto, a dimensão da proteção contra a ingerência externa na forma de interceptação de comunicações é apenas uma das dimensões que podem ser consideradas como objeto do direito à privacidade. Embora não seja especificamente ligado aos debates próprios do objeto da presente dissertação, cabe salientar que a própria noção de direito à privacidade não é alheia a controvérsias ligadas a um devir histórico no qual tem se assistido não somente a transformações tecnológicas, mas também do próprio paradigma a respeito da tutela da pessoa. Neste sentido, existe uma ampla literatura a respeito dos debates na matéria desenvolvidos tanto no âmbito acadêmico quanto no jurídico e que discorrem a respeito dos objetos e bens que são, ou é desejável que sejam, protegidos pela legislação, da pertinência da separação das esferas da privacidade e da intimidade e da própria evolução desse direito fundamental na sociedade contemporânea (PILATI; VIEIRA CANCELIER DE OLIVO, 2014, p. 288-298).

Marcado pelas profundas transformações socioeconômicas acontecidas a literatura reconhece uma evolução na conceituação desse direito partindo desde sua primeira

também o de qualidade da Lei dado que já que permite a coexistência de estatutos de proteção assimétrica que garantem um tratamento diferenciado para nacionais e estrangeiros, e de salvaguardas previstos no Artigo 17 do Pacto.

O fato de o sistema sustentar-se legalmente no marco jurídico estadunidense foi qualificado pelas Nações Unidas (2014) como uma *ação extraterritorial* em matéria de interceptação de comunicações. [122] Idêntica consideração foi realizada no relatório supracitado do órgão parlamentar da União Europeia, que enfatizou que as atividades de vigilância massiva "comportam ações ilegais por parte dos serviços de informação e suscitam questões relativas à extraterritorialidade[123] das

---

formulação nos finais do século XIX diretamente ligada ao "direito de ser deixado só" até uma conceituação mais contemporânea no qual se o liga à "liberdade de autodeterminação informativa" (que compreende a capacidade de controle amplo das informações pessoais) (MACHADO, 2014, p. 338). A respeito disto Doneda (2006) argumenta que o advento das TICs modificou substancialmente o cenário de desenvolvimento desse direito. Com as novas dinâmicas associadas à informação (basicamente as abertas através do barateamento dos custos da sua produção, do seu armazenamento, do seu compartilhamento e do seu processamento) mudou sensivelmente o volume e o alcance da circulação de dados pessoais. Isto levou, sempre segundo o autor, a uma complexificação da gama de interesses ligados a eles e fez com que o direito a privacidade deixasse de ser uma prerrogativa meramente *elitista*, reservada a *extratos sociais bem determinados.* Neste sentido, argumenta, independentemente da sua origem histórica a complexidade que na atualidade assume a garantia de uma esfera privada, livre de ingerências externas é de crescente importância que excede os moldes do direito subjetivo "a ser tutelado conforme as conveniências individuais". Segundo o autor, nessa mudança a privacidade assume uma posição de destaque na proteção da pessoa humana não apenas como uma proteção perante o exterior mas como um elemento positivo como elemento indutor de atividade política em sentido amplo (DONEDA, 2006, p. 87-91). É por isto que, para o autor, a abordagem desta questão apenas partindo do paradigma da interceptação abrange "apenas uma parcela dos problemas que podem ocorrer no tratamento de dados com a utilização das novas tecnologias" sendo necessário "outorgar a tutela efetiva aos dados pessoais na amplitude que a importância do tema hoje merece" (DONEDA, 2011). Desde já que esta consideração implica, como sugere Rodriguez (2014), superar a perspectivas individuais na consideração a respeito do direito a privacidade, calcadas nas conceituações a respeito do *recolhimento* e a *exposição* e apresenta a necessidade de problematizar o papel do instituto do consentimento dentre outras dimensões.

[122] Em relação à evolução desta temática no âmbito das Nações Unidas, cabe salientar que, no mês de março de 2015, foi aprovada uma resolução que estabelece a criação do cargo de relator para direito à privacidade na era digital. Informação disponível em:
http://www.unmultimedia.org/radio/portuguese/2015/03/onu-nomeia-relator-para-direito-a-privacidade-na-era-digital/

[123] No mesmo informe da Comissão, define-se a Extraterritorialidade no sentido da "aplicação extraterritorial por parte de um terceiro país de suas leis, legislações e

legislações nacionais" (2014b, p. 25). Acrescenta-se, nesse mesmo documento, a rejeição às características secretas dos tribunais da Lei de Inteligência Estrangeira (FISA) e a declaração dessa prática como contrária ao Estado de Direito.[124]

Uma consideração similar, no sentido de apontar as características específicas do atual sistema em oposição a outras técnicas desenvolvidas no passado, foi realizada pelo Relator especial sobre a promoção e a proteção dos direitos humanos e as liberdades fundamentais na luta contra o terrorismo das Nações Unidas. No seu relatório (EMMERSON, 2014, p. 3–5), o mesmo salienta que podem ser diferenciados dois tipos de técnicas: as de vigilância seletiva e as de vigilância massiva. As primeiras, analisa o Relator, contemplam instâncias de avaliação independente da informação que gerou as suspeitas e de proporcionalidade das medidas de vigilância. As segundas, pelo contrário, apresentam como particularidade essencial o fato de que o acesso aos dados, tanto de tráfego quanto de conteúdo, faz-se em massa e sem necessidade de suspeitas prévias, sendo que a análise efetuada sobre este vasto conjunto de informações realiza-se através de procedimentos de mineração de dados empregados para detectar padrões de comunicação entre as pessoas e entre as organizações. Como explica Bruno, neste caso o "individuo emerge como um alvo *a posteriori*, como um resultado do processo de vigilância, em lugar de estar presente desde o começo."[125] (2012, p. 349, tradução livre).

De fato, anteriormente à publicação dos documentos Snowden, essa diferenciação já vinha sendo problematizada como uma característica central dos esquemas de vigilância montados sobre as comunicações digitais, praticados tanto por empresas quanto por estados nacionais. Assange et al (2013, p. 41–53) argumentaram que um aspecto diferenciado deste sistema define-se pela prática de coleta massiva de dados, disponibilizados para sua análise posterior uma vez

---

outros elementos legislativos e executivos em situações que estejam dentro da jurisdição da União Europeia".

[124] De fato, a particular interpretação que esses tribunais fizeram sobre as habilitações previstas pela lei foi questionada, recentemente, pela própria justiça dos Estados Unidos, em um caso apresentado pela União Americana pelas Liberdades Civis (ACLU, pela sigla em inglês) (TOOMEY; YACHOT, 2015).

[125] No original: "the individual emerges as an a posteriori target, as the result of a surveillance process, instead of being present from the outset".

individualizados os alvos ou, ainda mais, para que as informações coletadas formem parte do próprio processo de identificação.

Como sintetizado pela própria NSA, a orientação seguida pelo sistema de vigilância massiva de comunicações é a “saber tudo, coletar tudo, processar tudo, explorar tudo” (NSA, 2011) e essa orientação, precisamente, expressa aquilo que é central ao dispositivo punitivo. Como foi analisado no capítulo precedente, embora o seu objetivo declarado aponte para o combate a um fenômeno discursivamente restrito a uma população alvo, os dispositivos de vigilância se orientam a monitorar o conjunto populacional.

A articulação entre esse ideal preventivo que racionaliza o discurso punitivo e as estratégias concretas ligadas à verticalização social é o objeto pontual da análise realizada no capítulo seguinte. Nele são apresentados os resultados da análise dos documentos que selecionados para conformar amostra da presente pesquisa. Como adiantado, a ideia que conduz esse estudo é o de identificar o conteúdo específico com o qual as regularidades próprias do discurso do poder punitivo se expressam no caso da vigilância massiva de comunicações. Em outras palavras, tenta-se mostrar quais as formas específicas que estes elementos assumem na atualidade enfatizando as vinculações funcionais que mantém com aquelas noções estudas no primeiro capítulo em ocasião de analisar o discurso demonológico inquisitorial retratado no Malleus Malleficarum.

4 DISCURSOS SOBRE VIGILÂNCIA MASSIVA DE COMUNICAÇÕES

> É vital que nossa Nação fale com uma voz clara, e, quando falamos, queremos dizer o que dizemos. É essencial que esta Nação não seja uma nação de palavras vazias, mas uma nação que está determinada a cumprir com nosso dever[126] (BUSH, 2007d, p. 292, tradução livre).

> O governo tentou justificar o programa secreto da NSA evocando exatamente o tipo de teoria extremista de poder executivo que havia me motivado a começar a escrever: a ideia de que a ameaça do terrorismo internacional dava ao presidente autoridade praticamente ilimitada para fazer qualquer coisa de modo de *garantir a segurança da nação* (GREENWALD, 2014, p. 11, ênfase no original).

Este terceiro capítulo marca a culminação da presente pesquisa. Como antecipado ele tem o foco principal na análise de um conjunto de acontecimentos discursivos considerados representativos da conceituação oficial que estadunidense a respeito da vigilância massiva e global de comunicações.

O procedimento seguido para a seleção dos documentos inclusos na amostra detalha-se na primeira seção. Nesta é quantificado e caracterizado o total de documentos analisados e especificada a metodologia seguida na analise. Na segunda seção apresenta-se o resultado da pesquisa. Como referido, esta se baseia nas categorias que tem sido identificadas como próprias do discurso do poder punitivo e que foram detalhadas na segunda no primeiro capítulo.

[126] No original: “It is vital our Nation speak with a clear voice, and when we speak, we mean what we say. It’s essential that this Nation not be a nation of empty words but a nation that is determined to do our duty”.

4.1 COMPOSIÇÃO DA AMOSTRA E METODOLOGIA DE ANÁLISE

Para conformar a amostra foram escolhidos três tipos de documentos: textos normativos, documentos doutrinários e manifestações públicas de atores do sistema político estadunidense, considerados relevantes no âmbito da pesquisa. Em todos os casos, a seleção da amostra compreende o período entre 11 de setembro de 2001 e 30 de junho de 2016. Trata-se em total de 152 documentos cuja composição se ilustra na Tabela 1 e que se encontram listados de maneira integral no Apêndice à presente dissertação

Tabela 1 - Composição da amostra segundo tipo de documento

Tipo	Total
Documentos Doutrinarios	**9**
Textos normativos	**9**
Manifestações públicas	**134**
Presidente	71
Secretaria de Estado	42
NSA	21
Total	**152**

Fonte: Elaboração da autora

A seguir detalha-se o método empregado na seleção dos documentos:

Documentos Doutrinários: Dentre os diversos tipos de documentos inclusos na presente amostra, os doutrinários,[127] são de maneira geral os mais alheios às considerações públicas. Neste sentido, eles possibilitaram acessar

[127] Por documentos doutrinários, entendem-se aqueles que oferecem um "conjunto harmônico de ideias e de entendimentos que define, ordena, distingue e qualifica as atividades de organização, preparo e emprego das Forças Armadas" (BRASIL, 2007, p. 12).

conceituações mais aprofundadas em matéria de exploração das Tecnologias de Informação e Comunicações como ferramenta na garantia da segurança e defesa nacionais. Embora abarquem documentos que orientam as ações em segurança e defesa nacionais, detém-se especificamente naqueles ligados à ação no denominado *ciberespaço*. Estes se distribuem de maneira muito mais homogênea ao longo dos anos analisados dado seu caráter relativamente mais desvinculado dos assuntos que ocupam a agenda política a cada momento.

Textos normativos: Estes aportaram clarificação sobre as disposições concretas e a sua vinculação com objetivos declarados. Nesta categoria foram inclusos três tipos de documentos: Leis, normas administrativas emanadas do poder executivo (Diretivas Presidenciais e Ordens Executivas) e notas de esclarecimento publicadas pelo Departamento de Justiça dos Estados Unidos as quais, embora não ser estritamente normativas, vinculam-se à interpretação das mesmas. No total foram inclusos 9 documentos.

Manifestações Públicas: Incluem transcrições de pronunciamentos e entrevistas, textos de opinião. Por suas características possibilitaram captar os argumentos dominantes sobre valoração desta prática por parte daqueles que possuem responsabilidades no comando político da sociedade. Estes pronunciamentos foram especialmente enriquecedores da análise, fundamentalmente naqueles contextos nos quais o sistema de vigilância foi foco do debate como, por exemplo, as instâncias de debate legislativo ou vazamentos através dos quais aspectos pontuais das práticas executadas ganharam estatuto público.

Dadas as limitações próprias do desenho de uma pesquisa no âmbito do mestrado o estudo das manifestações públicas, restringiu-se exclusivamente aos representantes no âmbito do Poder Executivo. Especificamente a amostra contemplou às figuras do Presidente, do Secretario de Estado (subsetor de Relações Exteriores) e do Chefe da NSA como responsável máximo diretamente vinculado à prática da vigilância massiva e global de comunicações.

3.a. No caso da administração do Presidente George W. Bush (2001 – 2009), a totalidade dos discursos presidenciais encontra-se editados na publicação oficial da série

"Documentos públicos dos Presidentes dos Estados Unidos". [128] Assim, a seleção dos pronunciamentos baseou-se nesta publicação e resultou da na procura através de quatro palavras-chave: "Patriot Act" (Ata Patriota), "FISA", "NSA, "surveillance" (vigilância) e "cyber" (ciber), "tools to track terrorists" (ferramentas para rastrear terroristas) e "privacy" (privacidade). Como resultado desse processo obteve-se uma seleção preliminar de 564 discursos. Dado o elevado número de casos positivos, e sendo a presente uma pesquisa qualitativa na qual resultavam esperáveis um grande número de reiterações, decidiu-se refinar a amostra aplicando o critério de exigência de presença de pelo menos dois desses termos o qual derivou numa lista final de 37 casos.

3.b. No caso da administração do Presidente Barak Obama (2009 – 2017), seguiu-se uma estratégia mista na seleção dos pronunciamentos. Considerando-se que, no momento de elaboração da presente amostra, a publicação "Documentos públicos dos Presidentes dos Estados Unidos" abarcava somente até o primeiro semestre do ano 2011, completou-se o período com buscas no portal oficial do Escritório Oficial de Publicações Governamentais[129]. Neste caso aos termos supracitados acrescentou-se a palavra-chave: "Snowden" no intuito ajustar os parâmetros da busca à terminologia empregada pelo ator em questão. Isto derivou na seleção preliminar de 336 pronunciamentos que, refinada através do critério de exigência de presença de pelo menos três desses termos, derivou em uma lista final de 34 declarações.

3.c. No caso dos sucessivos Secretários de Estado,[130] foram efetuadas buscas no arquivo disponível no sitio web do

[128] No original: "Public papers of the Presidents of the United States". Disponível em: https://www.gpo.gov/fdsys/search/home.action acesso em 20/12/2016.

[129] Trata-se da Compilação de documentos Presidenciais realizada pela *United States Government Printing Office*. Disponível em: https://www.gpo.gov/fdsys/browse/collection.action?collectionCode=CPD, acesso em 20/12/2016.

[130] O período analisado abrange as atuações de quatro chefes do Departamento de Estado, a saber: Colin Powell (2001-2005), Condolezza Rice (2005-2009), Hillary Clinton (2009-2013) e John Kerry (2013 – 2017).

Departamento,[131] em base às sete palavras-chave listadas no caso dos presidentes Bush e Obama: “Patriot Act” (Ata Patriota), “FISA” (tribunais da Lei de Inteligência Estrangeira), “surveillance” (vigilância), “cyber” (ciber), “privacy” (privacidade), “NSA”, Snowden e “tools” (ferramentas). Aplicando o critério supracitado se selecionaram 42 textos finais.

3.d. Finalmente, no caso da NSA o período sob análise compreende três chefias: Michael Hayden (1999 – 2005), Keith Alexander (2005 – 2014) e Michael Rogers (2014 – 2017). Na seleção, consideraram-se os pronunciamentos que figuram no sítio oficial da instituição[132] já pronunciados pelos seus diversos chefes, quanto os institucionais totalizando 21 documentos.

Como resultava esperável, os documentos não se distribuem de maneira homogênea ao longo do período. Neste sentido, uma série de mudanças no contexto político internacional e doméstico tem condicionado a aparição dos casos positivos.

A defesa mais comprometida dos programas de vigilância foi realizada durante a presidência de George W. Bush, quando se promulgaram não somente a Lei Patriota, mas também: a Lei de Proteção da América, a Emenda sobre a Lei FISA e as periódicas autorizações das mesmas. Toda esta atividade legislativa, em conjunto com os episódios de denúncias especialmente relacionadas ao ex-analista da NSA Thomas Drake em 2006,[133] geraram um amplo debate público no qual o Governo assumiu a postura de defender os programas em questão. Para o que a pesquisa se refere, esse contexto ofereceu a oportunidade de acessar uma multiplicidade de pronunciamentos nos quais se manifestaram com clareza os principais eixos argumentativos na avaliação política do sistema. Assim, como pode ser observado no Gráfico 1, os anos 2005 e

[131] Para o período 2001 – 2009: http://2001-2009.state.gov/secretary/, acesso em 14/04/2016 e para o período 2009 – 2017: https://2009-2017.state.gov/ acesso em 20/02/2017.

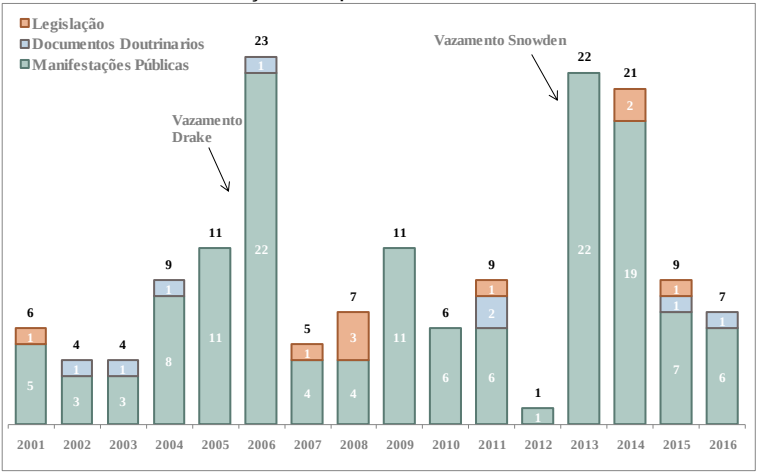
[132] Disponível em: https://www.nsa.gov/public_info/_files/speeches_testimonies/ acceso em 20/04/2016.

[133] Ver nota 75.

2006 concentram uma porção substancial dos documentos analisados correspondentes a esse período.

O contexto na presidência Obama é diferente. Neste caso, não houve praticamente debate substancial sobre a vigilância de comunicações durante o primeiro mandato. Por isto, embora existiram certas referencias ao assunto no período correspondentes ao Presidente Obama e a Secretária de Estado Clinton, elas são de características gerais sem focar pontualmente no monitoramento de comunicações. De fato, enquanto Senador, Barack Obama tinha sido amplamente crítico da vigilância de comunicações por parte da NSA (BAMFORD, 2016; LEFÉBURE, 2014, p. 33–35). Assim, o debate tornou-se significativo só após o vazamento dos documentos por parte de Snowden fato que pode ser percebido na mesma **¡Error! No se ncuentra el origen de la referencia.** através do incremento substancial na quantidade de documentos inclusos na amostra nos anos 2013 e 2014.

Gráfico 1 - Distribuição temporal dos documentos da amostra



Fonte: Elaboração da autora

Combinado com este enfoque relativamente exaustivo na seleção dos documentos procurou-se executar uma análise de tipo estrutural, voltada ao estudo da lógica perante a qual o discurso articula-se.

Fairclough (2003) denomina este método de análise da *ordem do discurso*, destacando que se trata do estudo daquelas estruturas sociais relativamente duráveis sob a qual o discurso se organiza. Em uma linha similar, Silverman (2006) denomina-o *análise de estruturas narrativas*, explicitando que se trata de um tipo de estudo que parte do entendimento de que o discurso está estruturado pela função que os elementos assumem na construção dos argumentos. Em consequência, a leitura visou identificar nos acontecimentos discursivos analisados o eixo argumentativo segundo o qual se faz referência à pratica da vigilância de comunicações, tentando estabelecer como esses argumentos se interrelacionam com os restantes. Em outras palavras, seguindo as categorias analíticas antes descritas, procurou-se identificar nessas narrativas qual o objetivo declarado da vigilância (o que), por que é relevante ou necessária, quando deve se desenvolver, como deve ser exercida para ser eficaz e quem deve fazê-lo.

Assim, o que se buscou estudar em uma primeira instância foram os acontecimentos discursivos em si mesmos, procurando identificar os padrões de formação dos seus elementos componentes e as vinculações existentes entre os diversos enunciados. Em específico, seguindo aquilo expressado por Foucault no livro “A arqueologia do saber” (1987), a orientação foi a de estudar o discurso como uma prática concreta sujeita a um conjunto de regras que lhe são inseparáveis. Neste sentido, através a leitura se conduziu à identificação as formas concretas de composição dos seus elementos componentes e as vinculações existentes entre os diversos enunciados. Em outras palavras, não se pretendeu somente a de identificar as regularidades presentes neles e a reiteração de conceitos, mas fundamentalmente focar nos seus nexos que é o que, em definitiva configura o discurso em sua unidade conceitual.

Para organizar a exposição seguiu-se idêntica estrutura que a desenvolvida no primeiro capítulo orientada a expor a matriz discursiva do poder punitivo em sua versão demonológica, organizada em torno às funções que organizam um relato: o quê, quem, por quê, quando e como. Como salientado, a ideia de seguir esse modelo é a de enfatizar precisamente que a os diversos elementos ou regularidades não se apresentam no discurso de forma aleatória, mas que se vinculam seguindo uma lógica unificadora orientada à produção de sentido.

Sendo amplo o volume de pronunciamentos com o qual se trabalhou nesta seção, procurou-se oferecer como resultado uma leitura analítica do conteúdo específico com o qual cada uma das regularidades discursivas se manifestaram nos documentos da amostra. Tentando evitar a saturação própria da reiteração discursiva, esta leitura foi exemplificada com referências textuais só naqueles casos considerados como mais representativo daquilo que se estava buscando mostrar. Em consequência, não se citou de forma exaustiva a aparição de reiterações discursivas na amostra, mas se identificou aqueles casos avaliados como mais significativos. Quando possível procurou-se refletir na análise a evolução temporal que tiveram os diversos elementos, a presença de continuidades e descontinuidades, assim como de interpretar esses fenômenos. Especialmente neste ponto, procurou-se enriquecer a leitura através dos aportes de autores mais identificados de maneira mais direta com o campo da segurança internacional.[134]

O segundo aspecto enfatizado foi o de reiteração das estratégias. Neste aspecto, a leitura não se orientou a gerar um contraste negativo entre as diversas manifestações com a documentação vazada na procura de declarações falsas ou inexatas por parte das autoridades políticas, dimensão que tem sido explorada principalmente pela produção jornalística. Pelo contrário tentou-se enfatizar os pontos de vinculação entre a produção discursiva e as características concretas da vigilância massiva de comunicações no entendimento de que a importância política do discurso é a de mediar o processo de leitura da realidade. O que se estuda, portanto, não é a narrativa como uma manifestação puramente literária, mas o discurso como parte integrante de um dispositivo no qual práticas concretas e narrativas estão integradas. Através do discurso é que se constrói o sentido específico de interpretação de práticas concretas, que tem consequências específicas em termos de poder, e só no marco daquelas práticas a narrativa possui um sentido lógico concreto. Assim, as manifestações e as normativas

[134] Em especial se procurou incorporar alguns estudos especificamente sobre narrativas em matéria de política de segurança internacional após o 11 de setembro e sobre as *ciberameaças*. No primeiro caso, salienta-se a coletânea Terror, inseguridade e liberdade: práticas não liberais em regimes liberais após o 11 de setembro (BIGO; TSOUKALA, 2008) e, no segundo ,as obras de Cavelty (2007a, b) e Hansen e Nissembaum (2009).

estudadas não surgiram no vácuo. Os discursos e a lógica em torno à qual estão articulados remetem, de maneira mais ou menos direta, às práticas concretas cujas características foram estudadas no capítulo precedente.

4.2 UMA ANÁLISE DO DISCURSO ESTADUNIDENSE EM MATÉRIA DE VIGILÂNCIA DE COMUNICAÇÕES NO PERÍODO 2001 – 2016

Na seção a seguir se procede a detalhar os resultados da análise realizada sobre os acontecimentos discursivos inclusos na amostra. Como antecipado, a exposição segue a idêntica ordenação que aquela empregada no primeiro para a apresentação das características estruturais do discurso do poder punitivo na sua versão demonológica.

De maneira resumida, no primeiro capítulo enfatizou-se que é característico desse discurso se orientar pelo princípio de racionalização da prevenção, que se orienta pelo ideal da intervenção antecipada. Fundado naquilo que Zaffaroni (2006, p.22) conceitua como o *confisco do conflito* deriva na afirmação de uma autoridade que centraliza as instâncias legitimas de toma de decisões. Essa autoridade é apresentada como especialmente capacitada para encarar a intervenção a qual se manifesta deve ser encarada de forma urgente, toda vez que se configura uma ameaça iminente que configura um estado de emergência. A narrativa empregada na caracterização do cenário e da ameaça é frequentemente moralizante, sustentada em uma oposição do bem e o mal e apoiada aos preconceitos da época. Finalmente, que o combate a ameaça requer ações extraordinárias. Sendo o princípio de racionalização ligado à prevenção vincula-se logicamente com dispositivos orientados à detecção antecipada os quais longe de se circunscrever à identificada como alvo declarado da ação a caracterização do inimigo como difuso, coordenado e voltado à exploração de vulnerabilidades, aponta a necessidade de operar mecanismos de monitoramento da totalidade da população.

A continuação procede-se a detalhar, com base na análise dos discursos da amostra, o conteúdo com que esse discurso se expressa na atualidade em relação à vigilância massiva de comunicações. Neste sentido, embora existam marcadas e inegáveis diferenças entre a conjuntura do presente

e aquela na qual se desenvolveu a função inquisitorial medieval, considera-se que se repete idêntica ordem discursiva ligada às mesmas estratégias em termos de poder.

Como debatido no primeiro capítulo, considera-se que a importância política do discurso é a de mediar o processo de leitura da realidade. O que se estuda, portanto, não é a narrativa como uma manifestação puramente literária, mas o discurso como parte integrante de um dispositivo no qual práticas concretas e narrativas estão integradas. Através do discurso é que se constrói o sentido específico de interpretação de práticas concretas, que tem consequências específicas em termos de poder, e só no marco daquelas práticas a narrativa possui um sentido lógico concreto.

A análise dos documentos e pronunciamentos a seguir deve ser entendida desde esta perspectiva. As manifestações e as normativas estudadas não surgiram no vácuo. Os discursos e a lógica em torno à qual estão articulados remetem, de maneira mais ou menos direta, às práticas concretas cujas características foram estudadas na seção precedente.

Em consequência a análise é conduzida pelo objetivo de salientar essas reiterações. A ênfase é colocada nas particularidades com as quais as diversas noções aparecem nos documentos da amostra e nas relações que mantêm respeito daquelas conceituações que assumiram idêntica função no discurso inquisitorial demonológico.

i. O quê? – De maneira generalizada, os documentos analisados definem a prática da vigilância massiva de comunicações como um elemento central no marco de intervenções punitivas cujo fim declarado é o de prevenir que uma série de eventos aconteça.
   Seguindo as definições da própria Lei Patriota, as ações preventivas estarão focadas em fenômenos de duas ordens. Em primeira instância, os atos terroristas e, secundariamente, aqueles conceituados como ciberterroristas. Nessa norma define-se que os "procedimentos melhorados de vigilância",[135] nela prescritos, constituiriam "uma ferramenta apropriada requerida para interceptar e obstruir o

[135] No original: "Enhanced surveillance procedures".

terrorismo”[136] (EUA, 2001b, p. 1, tradução livre) ao mesmo tempo em que também se regulamentou em matéria da “dissuasão e prevenção do ciberterrorismo”[137] (EUA, 2001b, seç. 814, tradução livre). Embora o termo *ciberterrorismo* constitua um conceito logicamente ligado ao de terrorismo, ele também remete a uma série de fenômenos diferenciados. Apesar da sua definição imprecisa, pode-se afirmar que se refere a eventos ligados à utilização de redes de computadores como ferramenta principal de atuação e relacionados a conceitos como *ciberameaças* ou *ciberataques.* Em outras palavras, trata-se do uso das tecnologias de informação e comunicações como arma ou da sua identificação como alvo de um ataque (CAVELTY, 2007b, p. 22).

Esse objetivo declarado se manteve como uma constante nos diversos textos normativos estudados na presente pesquisa, de fato, um progressivo incremento na variedade de fenômenos passíveis a justificar as práticas de monitoramento. Assim, no caso da Lei de Emenda FISA[138] se estabelece como critério válido para solicitar o auxílio dos operadores privados na coleta de informação a declaração da autoridade competente de que estes estivessem “destinados a detectar ou impedir um ataque terrorista ou atividades preparatórias para um ataque terrorista contra os Estados Unidos”[139] (EUA, 2008c, seç. 802, tradução livre). Já na Diretiva Presidencial de Política Nº 28 do ano 2015, habilita-se o uso dos dados coletados através de procedimentos massivos para a detecção e combate de um conjunto ostensivamente mais amplo de fenômenos que incluem: ameaças terroristas, proliferação de armas de destruição massiva, ciberameaças e de forma ainda mais genérica e ameaças relativas ao crime transnacional[140] (EUA, 2014, seç. 2).

---

[136] No original: “appropriate tools required to intercept and obstruct terrorism”.
[137] No original: “Deterrence and prevention of cyberterrorism”.
[138] A relevância de ambas normativas no desenvolvimento do sistema de vigilância de comunicações, especialmente no que tange à cooperação por parte dos operadores privados, foi abordada no capítulo precedente.
[139] No original: “designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States”
[140] No original: “In particular, when the United States collects nonpublicly available signals intelligence in bulk, it shall use that data only for the purposes of detecting and

O combate ao terrorismo e às ciberameaças, como objetivo declarado primordial da vigilância massiva de comunicações, configura uma constante presente nas diversas manifestações públicas analisadas assumindo diversos graus de ênfase em cada período. Em linhas gerais, pode-se afirmar que a ação terrorista configura o fenômeno de maior relevância na agenda política estadunidense durante a administração Bush; no entanto, durante a administração Obama, o fenômeno *ciber* ocupa um lugar de maior relevância como objeto declarado da vigilância de comunicações.[141] Tomando como um indicador imperfeito a respeito da centralidade na agenda desta questão resulta ilustrativo que, considerando exclusivamente os pronunciamentos inclusos na amostra, em 15% dos casos correspondentes ao Presidente Bush se faz menção do prefixo "cyber" (em referência ao "ciberterrorismo", ao "cibercrime" ou de maneira mais geral às "ciberameaças"), ao tempo que o uso de esse termo atinge um 50% quando são consideradas as manifestações proferidas pelo Presidente Obama.

Assim como no Malleus Maleficarum argumentava-se que o foco da ação inquisidora era o de aplicar remédios contra a heresia para prevenir a destruição de almas inocentes (KRAMER; SPRENGER, 2002, p. 44); no conjunto de documentos analisados, de maneira recorrente a noção da ação preventiva, antecipada, aparece como orientação geral da atuação das agências de segurança e, em específico, como objetivo declarado da coleta de dados sobre comunicações.

---

countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section."

[141] Sobre este ponto, Hansen e Nissembaum (2009, p. 1171) argumentam que ao longo dos anos estes conceitos de ciberameaças e do terrorismo têm exibido um processo de *fertilização cruzada*, pelo qual o que se refere especificamente às TICs (ciberameaças) adicionaram periculosidade à natureza da ameaça terrorista, tanto que a existência da ameaça terrorista justificou a atenção especial sobre as tecnologias de comunicação.

> Nos diversos documentos estudados o ideal antecipatório se manifesta como orientação geral da ação das agências de segurança do Estado e, de forma mais específica, como objetivo declarado dos programas de coleta de dados sobre comunicações.
> O ideal preventivo orienta também a produção doutrinária na matéria. Publicada no ano 2003, a *Estratégia Nacional para proteger o ciberespaço* é a primeira do seu tipo nos Estados Unidos e define que:
>
> > A Nação procurará prevenir, deter e reduzir significativamente os ciberataques através da garantia de identificação dos perpetradores reais ou intencionais, seguida de uma resposta apropriada do governo. No caso do cibercrime, esta incluirá uma apreensão rápida e uma apropriada e severa punição[142] (EUA, 2003, p. 29, tradução livre).

Neste sentido, em ambas as administrações faz-se especial ênfase na mudança acontecida na orientação das agências estatais de inteligência após o 11 de setembro. Em particular, o então Presidente Bush (2006, p. 1136) destacava, em 2003, a maior relevância das tarefas de prevenção de ataques futuros por parte do FBI, cujo lugar na estruturação do sistema de vigilância foi salientado no capítulo precedente. De maneira mais geral, no ano 2004, o Presidente estadunidense avaliava que: "A Lei Patriota marcou também uma mudança maiúscula nas prioridades das agências de segurança. Já não seguimos enfatizando unicamente a investigação dos crimes passados, mas também a prevenção de ataques futuros"[143] (BUSH, 2007g, p. 600, tradução livre).

Idêntica consideração seria reiterada por Obama, no contexto do amplo debate que sucedeu ao vazamento dos documentos realizado por Snowden. Neste sentido, o então mandatário argumentava que os procedimentos de vigilância de

[142] No original: "The Nation will seek to prevent, deter, and significantly reduce cyber attacks by ensuring the identification of actual or attempted perpetrators followed by an appropriate government response. In the case of cybercrime this would include swift apprehension, and appropriately severe punishment."
[143] No original: "The Patriot Act also marked a major shift in law enforcement priorities. We're no longer emphasizing only the investigation of past crimes but also the prevention of future attacks."

comunicações em debate tinham de ser entendidos no contexto das demandas realizadas às agências de inteligência e de segurança para melhorar as suas capacidades e para se focar "mais em prevenir ataques antes que aconteçam do que em perseguir terroristas após terem atacado"[144] (OBAMA, 2014, p. 2, tradução livre).

É neste contexto que o monitoramento das comunicações é apresentado como uma ferramenta essencial para atingir esse ideal antecipatório. Como argumentado pelo Presidente Bush em ocasião de seu pronunciamento perante o Congresso nove dias após os atentados, a orientação foi a de oferecer às agências as "ferramentas adicionais necessárias" para "conhecer os planos dos terroristas antes que eles atuem e para encontrá-los antes que eles ataquem" (BUSH, 2005a, p. 1143, tradução livre). Dias depois, em ocasião da promulgação da Lei Patriota, o Presidente estadunidense argumentava que a vigilância de comunicações constituía uma ferramenta essencial para "perseguir e deter terroristas antes que eles ataquem"[145] (BUSH, 2005c, p. 1307, tradução livre). Idêntica formulação foi reiterada ao longo das diversas manifestações estudadas no sentido servir ao propósito de "detectá-los antes que ataquem"[146] (BUSH, 2005d, p. 1313, tradução livre), de "prevenir outro ataque terrorista"[147] (BUSH, 2006b, p. 226, tradução livre) ou de "prevenir ataques futuros"[148] (BUSH, 2007g, p. 600, tradução livre). É neste sentido que o presidente Bush argumentava no ano 2004: "estamos reformando nosso serviço de inteligência para que possamos obter melhor inteligência e compartilhar melhor a inteligência para interromper as conspirações terroristas"[149] (BUSH, 2007c, p. 1762, tradução livre).

Com poucas variantes discursivas, a administração Obama manteve idêntico sentido sobre este assunto. Assim a pouco de assumir como Presidente dos Estados Unidos reiterava a

[144] No original: "to focus more on preventing attacks before they happen than prosecuting terrorists after an attack."
[145] No original: "surveillance of communications is another essential tool to pursue and stop terrorists before the strike".
[146] No original: "to detect them before they strike".
[147] No original; "to prevent another terrorist attack".
[148] No original: "preventing future attacks".
[149] No original: "We're now reforming our intelligence service so we can get better intelligence and share the intelligence better to disrupt terrorist plots".

orientação de “descobrir atentados terroristas antes que eles aconteçam”[150] e, de maneira mais geral, das agências de segurança “se manter um passo a frente daqueles que estão fora da lei”[151] (OBAMA, 2010, p. 565, tradução livre). Essa noção esteve singularmente presente após o vazamento dos documentos Snowden. Assim, ao tempo que o então Presidente Obama reconhecia na época a necessidade de encarar uma reforma integral dos serviços de inteligência estadunidenses, salientava a importância dos programas de coleta em tanto constituíam “uma ferramenta importante no nosso esforço de interromper planos terroristas”[152] (OBAMA, 2013b, p.1, tradução livre). De maneira análoga, meses depois, salientava que tratavam-se de esforços orientados a “perseguir indícios que levem a impedir ameaças iminentes”[153] (OBAMA, 2014, 2, tradução livre).

Em sentido análogo, o então Chefe da NSA definia a missão da agência perante os membros do Comitê de Inteligência do Senado estadunidense: Uma das nossas mais importantes missões de SIGINT [inteligência de sinais] é a luta contra o terrorismo: descobrir planos, intenções, comunicações e locais de terroristas para interromper e derrotar seus ataques[154] (ROGERS, 2015c, p. 3).

Em resumo, os documentos analisados apresentam a vigilância massiva de comunicações como um dispositivo orientado pelo princípio racionalizador da prevenção, em particular a intervenção voltada a castigar de forma antecipada e evitar, assim, a ocorrência de um conjunto de acontecimentos. Como salientado no capítulo precedente, trata-se de uma regularidade própria do discurso do poder punitivo, em torno do qual se articulou o discurso inquisitorial do Malleus Maleficarum e que também se destaca como elemento próprio à narrativa securitizadora, conforme os teóricos da Escola de *Copenhague*.

---

[150] No original: “uncover terrorist plots before they take hold”

[151] No original: “to stay one step ahead of all who step outside of the law”.

[152] No original: “this program is an important tool in our effort to disrupt terrorist plots”.

[153] No original: “pursue leads that may thwart impending threats”.

[154] No original: “One of our most important SIGINT missions is counter-terrorism: discovering terrorists' plans, intentions, communications, and locations to disrupt and defeat their attacks”.

ii. Quem? – Outra noção que permeia a totalidade dos documentos que conformam a amostra é a de que os Estados Unidos possuem legitimidade para intervir em escala global. Atrelados a uma prática de vigilância de comunicações que, como foi analisada na seção precedente, abrange a totalidade do planeta, apresentam-se uma série de argumentos articulados à ideia central de que as autoridades desse país devem assumir um papel central no processo de tomada de decisões na matéria.

ii.a. A afirmação da autoridade e o *confisco do conflito:* Sobre este particular, é possível reconhecer dois tipos de argumentos que, embora apresentem diferenças em termos de conteúdo que justificam sua separação analítica, orientam-se por construção de idêntico sentido.

No caso específico do terrorismo, já no próprio texto da Lei Patriota define-se que se trata de "Uma Lei para deter e castigar atos terroristas nos Estados Unidos e ao redor do mundo"[155] (EUA, 2001b, p. 1, tradução livre) sendo essa *orientação transfronteriça* mantida ao longo dos diversos textos normativos aqui estudados. Assim, por exemplo, a Emenda sobre a Lei FISA acrescentou os objetivos declarados da coleta (e o uso de informações coletadas) a fenômenos tais como o: "sabotagem, terrorismo internacional ou a proliferação de armas de destruição massiva"[156] (EUA, 2008c, seç. 110, tradução livre).

O argumento central, trabalhado com matizes ao longo de todo o período analisado, é de que, embora global, o terrorismo afeta a dinâmica da segurança doméstica dos Estados Unidos, fundando-se nesta última a legitimidade de agir. Essa ideia foi sintetizada na Diretiva Presidencial para a Segurança Doméstica Nº 1, na qual se define o cenário da época como caracterizado por um "terrorismo global com implicações domésticas"[157] (EUA, 2001a, p. 1, tradução livre). Em termos concretos, essa noção se traduz em que:

---

[155] No original: "An act To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes."

[156] No original: "sabotage, international terrorism, or the international proliferation of weapons of mass destruction".

[157] No original: "global terrorism with domestic implications".

> A única maneira de defender os nossos cidadãos onde vivemos é ir atrás dos terroristas onde vivem. Assim, a segunda parte da nossa estratégia é levar a luta contra os terroristas no estrangeiro antes que eles possam nos atacar aqui em casa. Esta é a missão mais difícil e perigosa na guerra contra o terror[158] (BUSH, 2007e, p. 1339, tradução livre).

Essa leitura, caracterizada como doutrina dos estados falidos, foi mantida em essência ao longo da administração Obama (OLSSON, 2008, p. 153–155). Por meio desta, invoca-se a incapacidade das autoridades territoriais legitimamente estabelecidas e, em consequência, outorgar-se aos Estados Unidos a autoridade para agir. Assim, como argumenta Zaffaroni (2011b, parag. 2, tradução livre), "a luta contra o terrorismo tem se transformado na nova doutrina planetária de segurança nacional, que pretende legitimar procedimentos extraordinários internacionais".[159]

No caso específico da vigilância de comunicações, este argumento foi reforçado com outra ideia extensamente trabalhada na qual se apela que, dadas as particularidades do meio digital, as noções preexistentes ligadas às questões de soberania nacional seriam aí inaplicáveis. Isto opera a através da reiteração de duas ideais que remetem a idêntico sentido, a saber: que a mudança tecnológica tem tornado irrelevantes as fronteiras nacionais e que conformam um espaço em si mesmo, implícito no próprio conceito ciberespaço.[160]

---

[158] No original: "Vast oceans and friendly neighbors are not enough to protect us. A policy of re- treat and isolation will not bring us safety. The only way to defend our citizens where we live is to go after the terrorists where they live. So the second part of our strategy is to take the fight to the terrorists abroad be- fore they can attack us here at home. This is the most difficult and dangerous mission in the war on terror. And like generations before them, our soldiers and sailors and airmen and marines have stepped forward to accept the mission."

[159] No original: "La lucha contra el terrorismo se ha convertido en la nueva doctrina planetaria de la seguridad nacional, que pretende legitimar procedimientos extraordinarios internacionales."

[160] Neste sentido, como salientado por Eissa et al (2012, p.15), a dimensão global que atingem as tecnologias de comunicação não deve ser confundida com a ausência de limites geográficos e/ou geopolíticos. Em particular, salientam que: "O ciberespaço não é um espaço em si, mas uma dimensão que atravessa espaços físicos. Este 'erro

Como definido na já referida *Estratégia Nacional para proteger o ciberespaço*, "no ciberespaço as fronteiras nacionais têm pouco significado"[161] (EUA, 2003, p. 7, tradução livre). Em idêntico sentido, o Presidente Obama (2014, p. 2, tradução livre) sustentava a ideia de que "a tecnologia tem apagado as fronteiras".[162] Em sentido análogo, os máximos dirigentes da empresa Google afirmam que "Isso é a internet, o maior espaço sem governo do mundo" (SCHMIDT; COHEN, 2013, p. 11). Neste contexto, os discursos salientam o papel a ser exercido pelos Estados Unidos. Nas palavras do ex-Diretor da NSA:

> Não existe uma entidade, nem do setor privado nem da comunidade de nações que esteja 'a cargo' do ciberespaço, o que significa que não há uma entidade que possa mudar o ciberespaço para limitar o negativo e conservar os benefícios. Portanto, o ciberespaço é um ambiente perfeito para que os adversários dos Estados Unidos se conduzam e um domínio que os Estados Unidos devem proteger vigilantemente[163] (ALEXANDER, 2009a, parag. 12, tradução livre).

Assim como no Malleus a narrativa busca conciliar a função inquisidora com as estruturas políticas territoriais seculares argumentando que os Inquisidores intervinham por representação de Deus, principal prejudicado pelo pecado da heresia (KRAMER; SPRENGER, 2002, p. 377–395), nos documentos analisados na presente seção o argumento central é que os Estados Unidos intervêm, principalmente, em nome das vítimas domésticas do terrorismo global e das

---

interessado' nas palavras de Ernesto Lopez, não se diferencia muito daquelas análises que, interessadas em tirar proveito do enfraquecimento das unidades políticas individuais, declararam o fim dos Estados nacionais em meados dos anos 90".

[161] No original: "In cyberspace national boundaries have little meaning."

[162] No original: "technology erased borders".

[163] No original: "There is no one entity, be it from the private sector or from the community of nations, "in charge" of cyberspace, which means that there is no one entity that can change cyberspace to eliminate the negatives while keeping the benefits. Thus, cyberspace is a perfect environment for United States adversaries to thrive and a domain that the United States must vigilantly protect".

vítimas globais de um (ciber*)*espaço que careceria de autoridade legítima de intervenção.

As consequências concretas desta racionalidade, como detalhadas na seção precedente, são uma vigilância global de comunicações, estruturada sobre a base da aplicação extraterritorial da legislação nacional (EMMERSON, 2014; PARLAMENTO EUROPEU, 2014b).

ii.b.As capacidades superlativas da autoridade para encarar a intervenção: Ao afirmar a legitimidade de intervenção dos Estados Unidos, nos discursos analisados, apela-se frequentemente à afirmação das capacidades diferenciais que as agências desse país têm para intervir.

Aqui não se apela, como no Malleus, a uma percepção privilegiada fundada na imunidade aos feitiços (KRAMER; SPRENGER, 2002, p. 197-198), mas na superioridade tecnológica. Sobre esse particular, Presidente Obama afirmou que:

> [os Estados Unidos da] América têm responsabilidades especiais como única superpotência do mundo; […] nossas capacidades de inteligência são fundamentais para o cumprimento dessas responsabilidades e que eles mesmos confiaram nas informações que obtemos para proteger seu próprio povo. Como eu indiquei, os Estados Unidos têm responsabilidades exclusivas quando se trata de coleta de informações. Nossas capacidades ajudam a proteger não apenas nossa nação, mas também nossos amigos e aliados[164] (OBAMA, 2014, p. 9, tradução livre).

Na conceituação dos atores estudados na presente pesquisa essa superioridade funda-se, dentre outras dimensões, na capacidade diferencial para coletar e

[164] No original: "America has special responsibilities as the world's only superpower; that our intelligence capabilities are critical to meeting these responsibilities, and that they themselves have relied on the information we obtain to protect their own people. As I've indicated, the United States has unique responsibilities when it comes to intelligence collection. Our capabilities help protect not only our nation, but our friends and our allies, as well."

processar informações que tem os Estados Unidos em geral e suas agências em particular.

Neste sentido, apenas 6 meses após o 11 de setembro, o General Hayden explicava em uma audiência no Congresso que:

> A missão da NSA é explorar as comunicações estrangeiras secretas e produzir informações de inteligência estrangeiras enquanto protege as comunicações dos EUA. As comunicações de "exploração" são referidas como inteligência de sinais (SIGINT); "Proteção" é conhecida como garantia de informação (AI). São capacidades nas quais os Estados Unidos lideram o mundo. A maior força da NSA reside na sua força de trabalho civil e militar altamente talentosa. Possuindo uma riqueza de habilidades críticas e conhecimentos, esta força de trabalho inclui matemáticos, analistas de inteligência, linguistas, cientistas da computação e engenheiros. Na verdade, a NSA é conhecida por ser o maior empregador de matemáticos nos Estados Unidos e talvez no mundo. A NSA é também um dos centros mais importantes de análise e pesquisa de línguas estrangeiras dentro do Governo [...] continuaremos a fornecer as informações vitais que permitirão aos Estados Unidos manter uma vantagem decisiva na superioridade da informação[165] (HAYDEN, 2002, p. 1-6, tradução livre).

[165] No original: NSA's mission is to exploit secret foreign communications and produce foreign intelligence information while protecting U.S. communications. "Exploiting" communications is referred to as signals intelligence (SIGINT); "protecting" is known as information assurance (IA). These are capabilities in which the United States leads the world. NSA's greatest strength lies in its highly talented civilian and military workforce. Possessing a wealth of critical skills and expertise, this workforce includes mathematicians, intelligence analysts, linguists, computer scientists, and engineers. In fact, NSA is said to be the largest employer of mathematicians in the United States and perhaps the world. NSA is also one of the most important centers of foreign language analysis and research within the Government [...] we will continue to provide the vital information that will enable the United States to maintain a decisive edge in information superiority."

Em uma linha semelhante seu sucessor à frente da NSA argumentava que a agência representava o "centro de gravidade para os cripto matemáticos"[166] (ALEXANDER, 2009b, tradução livre).

Na narrativa se faz referência de maneira reiterada a importância dos Estados Unidos na manutenção da segurança global em tanto a sua capacidade superlativa de *conhecer* o que acontece: "Nosso trabalho também ajuda os Estados Unidos e seus aliados a capturar os fabricantes de bombas, detectar transferências de fundos ilícitas e explicar a outras nações como os terroristas esperam transitar seu território"[167] (ROGERS, 2015a, p. 3, tradução livre).

Precisamente, na conceituação de Rogers, a capacidade de prover informação em qualquer lugar do planeta é a marca por excelência da NSA. Nesta linha , no marco de uma conferência sobre cibersegurança realizada no ano 2015, o então Chefe da agência argumentava a respeito do risco aberto trás serem impostas limitações a coleta de informações após as revelações de Snowden. Consultado pelo entrevistador a respeito de possíveis *pontos cegos* como consequência das mudanças introduzidas trás os vazamentos, Rogers argumenta que se trata de uma situação que o "preocupa muito", sendo que:

> Dada a missão da Agência Nacional de Segurança, dada a nossa pegada em todo o mundo, eu quero dizer, nós como uma nação, quando eu penso sobre a nossa capacidade de fornecer entendimento para ajudar a proteger os cidadãos, onde quer que estejam [...] hoje, claramente, eu estou muito preocupado, assim como nossos principais aliados e amigos[168] (ROGERS, 2015, p. 10, tradução livre).

---

[166] No original: "We have the world's center of gravity for crypto mathematicians"

[167] No original: "Our work also helps the United States and its allies to capture bomb makers, spot illicit funds transfers, and explain to other nations how terrorists hope to transit their territory"

[168] No original: "Given the mission of the National Security Agency, you know, given our footprint around the world, I mean, us as a nation, you know, when I think about our ability to provide insights to help protect citizens, wherever they are, whether they be out there doing good things to try to help the world, whether they be tourists, whether they be serving in an embassy somewhere, whether they be wearing a

iii. Por quê? – Os diversos documentos estudados também oferecem um conjunto coerente de argumentos relativos à necessidade de encarar tal ação preventiva ou a explicitar as razões dessa intervenção. Tal como estudado no caso do Malleus Maleficarum, nos discursos aqui analisados também se argumenta a existência de um estado emergencial.

A emergência vincula-se a fenômenos diferentes, mas sua configuração segue as mesmas regularidades analisadas por Zaffaroni como características do discurso punitivo e, desde outra perspectiva, também identificadas como parte fundamental da narrativa securitizadora por parte dos autores da Escola de Copenhague. Assim, tal como no passado, no presente também se verifica que:

iii.a. A ameaça é máxima: Se no século XV os autores do Malleus afirmavam que a bruxaria excedia "todos os pecados já permitidos por Deus" (KRAMER; SPRENGER, 2002, p. 169), em 2001 o Presidente dos Estados Unidos assegurava que esse país enfrentava "uma ameaça como nenhuma outra nação jamais enfrentou"[169] (BUSH, 2005c, p. 1306, tradução livre) ou "uma das mais graves ameaças que o nosso país enfrentou"[170] (BUSH, 2007d, 317, tradução livre).

A função específica deste tipo de afirmações, tal como identificado pelos teóricos da *securitização*, é a de hierarquizar, elevar sobre os demais os esforços por combater o fenômeno em questão (BUZAN et al., 1998, p. 24). Este é o sentido preciso, tal como ilustrado por Bush no ano 2004:

> Em outras palavras, fizemos da prevenção ao terror uma importante prioridade do nosso Governo – simplesmente fazendo tudo o que pudemos para assegurar-nos que estamos tão seguros quanto podemos estar. O FBI agora tem a prevenção de ataques terroristas como sua prioridade máxima[171] (BUSH, 2007b, p. 606, tradução livre).

---

uniform and they End themselves in the battle field in Afghanistan or Iraq today, clearly, I'm very concerned, as well as our key allies and friends."

[169] No original: "a threat like no other our Nation has ever faced".

[170] No original: ""one of the gravest threats our country has ever faced".

[171] No original: "In other words, we've made prevention of terror an important priority of our Government—just doing everything we can to make sure that we're as safe as we

O caráter emergencial e ao mesmo tempo original do cenário também foi expresso pela então Secretária de Estado Rice. Por ocasião de um discurso sobre as transformações na diplomacia, a funcionária asseverava que "[os Estados Unidos da] América seguiram engajados por muitos anos em um novo tipo de confronto global, diferente de tudo o que já enfrentamos"[172] (RICE, 2008, p. 4, tradução livre). Em igual sentido o terrorismo é apresentado como "a ameaça de uma nova era"[173] (BUSH, 2006b, p. 226, tradução livre) ou como característico das "novas ameaças do nosso tempo"[174] (BUSH, 2006a, p. 1133, tradução livre). Tal como salientado no apartado precedente o apelo à qualificação de *novidade* tem uma função precisa no discurso que é a de afirmar a necessidade de encarar ações extraordinárias, por fora dos parâmetros de intervenção existentes. No caso da vigilância de comunicações essa vinculação foi expressa com singular clareza pelo então Presidente estadunidense quando, consultado pelos programas de monitoramento de comunicações no ano 2005, argumentava que:

> Logo após o 11 de setembro, eu sabia que estávamos lutando um tipo diferente de guerra. E assim eu pedi a povos em minha administração para analisar como melhor para mim e nosso governo para fazer o trabalho que as pessoas esperam que façamos, que é detectar e prevenir um possível ataque. Isso é o que o povo americano quer. Nós olhamos para os possíveis cenários. E as pessoas responsáveis por nos ajudar a proteger e defender surgiram com o programa atual, porque nos permite avançar mais rapidamente. E isso é importante. Temos que ser rápidos em nossos pés, rápidos para

possibly can be. The FBI now has the prevention of terrorist attacks as their number one priority."

[172] No original: "America will remain engaged for many years in a new global confrontation unlike anything that we've ever faced".

[173] No original: "threats of a new era".

[174] No original: "the new threats of our time".

> detectar e prevenir[175] (BUSH, 2007f, p. 1878, tradução livre).

Como salientado no ponto i, nos anos posteriores a ênfase foi deslocada para esse outro conjunto de fenômenos designados como *ciberameaças*. Neste sentido,

> as ameaças emergentes de grupos terroristas e a proliferação de armas de destruição em massa colocaram novas e, de certa forma, mais complicadas exigências [...] os desafios colocados por ameaças como o terrorismo e a proliferação e os ataques cibernéticos não desaparecerão em breve. Vão continuar a ser um grande problema[176] (OBAMA, 2014, p. 2 – 7, tradução livre).

Ainda mais, tal como se destaca no documento "Ciber estratégia", a partir do ano 2013, "o Diretor de Inteligência Nacional nomeou à ciberameaça como a ameaça estratégica número um para os Estados Unidos, localizando-a acima do terrorismo pela primeira vez, desde os ataques do 11 de setembro de 2001"[177] (EUA, 2015, p. 9, tradução livre).

Em resumo, o que se destaca é que tanto no caso do denominado "terrorismo" quanto a ligada a um conjunto muito mais impreciso de fenômenos vinculados ao uso de Tecnologias de Informação e Comunicações ("ciberameaças), a narrativa se orienta a destacar o caráter

---

[175] No original: "right after September the 11th, I knew we were fighting a different kind of war. And so I asked people in my administration to analyze how best for me and our Government to do the job people expect us to do, which is to detect and prevent a possible attack. That's what the American people want. We looked at the possible scenarios. And the people responsible for helping us protect and defend came forth with the current program, because it enables us to move faster and quicker. And that's important. We've got to be fast on our feet, quick to detect and prevent."

[176] No original: "emerging threats from terrorist groups, and the proliferation of weapons of mass destruction placed new and in some ways more complicated demands [...] the challenges posed by threats like terrorism and proliferation and cyber-attacks are not going away any time soon. They are going to continue to be a major problem."

[177] No original: "From 2013-2015, the Director of National Intelligence named the cyber threat as the number one strategic threat to the United States, placing it ahead of terrorism for the first time since the attacks of September 11, 2001".

extremo dessa ameaça, transformando-a em um objetivo legitimamente articulador de toda a ação estatal.

iii.b. Configura-se uma narrativa na qual se exaltam os valores positivos associados ao que é identificado como em situação de risco. A retórica de contraposição de *o bem* e *o mal* é um elemento absolutamente saliente de todos os discursos sobre esta questão[178]. Se nos tempos da inquisição a bruxaria era definida como *praticar o mal e blasfemar contra a Fé verdadeira* (KRAMER; SPRENGER, 2002, p. 77), na Lei Patriota o terrorismo se define como atividades que "envolvem perigo para a vida humana" e que "parecem estar voltados a intimidar a população"[179] (EUA, 2001b, seç. 802, tradução livre). Em consequência, no momento da promulgação da Lei, o Presidente estadunidense afirmava que "[e]sta legislação é essencial, não somente para perseguir e castigar os terroristas, mas também para prevenir mais atrocidades nas mãos dos malvados"[180] (BUSH, 2005c, p. 1307, tradução livre). Seguindo idêntica orientação, na *Estratégia Nacional de Segurança dos Estados Unidos de 2002* definia-se que "o objetivo desta estratégia é ajudar a tornar o mundo não só mais seguro, mas melhor"[181] (EUA, 2002, p. 1, tradução livre).

Se em tempos da inquisição a bruxaria comportava um risco para *as almas* e, portanto, configurava um perigo de *danação eterna* (INOCÊNCIO VIII, 2002, p. 44), os pronunciamentos sob análise argumentam que o que está sob ameaça é nada menos do que a vida, assim como

---

[178] Campbell (1992), entre outros, faz um histórico detalhado da evolução da narrativa de diversas autoridades políticas dos Estados Unidos sobre assuntos ligados à segurança salientando, entre outras questões, o uso reiterado desse tipo de narrativa de contraposição do bem contra o mal.

[179] No original: "(5) the term 'domestic terrorism' means activities that— "(A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; "(B) appear to be intended— "(i) to intimidate or coerce a civilian population; "(ii) to influence the policy of a government by intimidation or coercion; or "(iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping; and "(C) occur primarily within the territorial jurisdiction of the United States."

[180] No original: "This legislation is essential not only to pursuing and punishing terrorists but also preventing more atrocities in the hands of the evil ones".

[181] No original: "The aim of this strategy is to help make the world not just safer but better".

outros valores conotados positivamente na cultura ocidental. Nos discursos analisados, registra-se, neste sentido, um uso recorrente de expressões como *salvar vidas*, mas também se inclui de forma reiterada a referência a conceitos tais como liberdade e democracia. Assim, se no caso do Malleus o lugar pré-configurado de representante do bem era ocupado pela Igreja Católica, nestes discursos, o foi pelos Estados Unidos. Isto foi expresso com singular clareza pela então Secretária de Estado Clinton, que definiu a ação desse país nos seguintes termos:

> O poder americano [dos Estados Unidos] é um poder do bem, que tem ajudado a liberar centenas de milhões de pessoas ao redor do mundo, que tem ajudado a incrementar as oportunidades das pessoas e tem oferecido a meninas e meninos a oportunidade de viver segundo o potencial que lhes foi dado por Deus[182] (CLINTON; PANETTA, 2011, p. 11, tradução livre).

iii.c. O conteúdo específico atribuído ao perigo vincula-se com os preconceitos da época. Uma reiteração marcada nos discursos que conformam a amostra é a referência aos eventos do 11 de setembro de 2001. A constância no uso da imagem destes acontecimentos nos Estados Unidos tem uma função precisa, que é a de evocar emoções nos receptores da mensagem; emoções que não são necessariamente "novas", mas ligadas a essas imagens através de processos associativos irracionais que, por força de reiteração, acabam fixando um sentido concreto para essas palavras, como explica Gómez (2016, p. 13).

A intencionalidade de evocar essas emoções fica explícita em um discurso de Bush do ano 2004, quando defendia o projeto de renovação das previsões da Lei Patriota:

> As vidas de todas as pessoa aqui presente mudaram com os eventos do 11 de setembro de 2001. Nesse dia, sentiram a raiva e o sentimento de perda. […]

[182] No original: "American power is a power for the good, that it has helped to liberate hundreds of millions of people around the world, that it has helped to enhance the opportunities for people and to give young girls and boys the chance to live up to their own God-given potential".

> As memórias do 11 de setembro nunca nos abandonarão. Não esqueceremos das torres ardendo, das últimas ligações telefônicas e da fumaça sob Arlington. Não esqueceremos os resgatadores que correram em direção ao perigo nem os passageiros que enfrentaram os jihadistas. Não esqueceremos os homens e as mulheres que saíram para trabalhar em um dia típico e não retornaram às suas casas. Não esqueceremos a morte das crianças que estavam em viagem escolar[183] (BUSH, 2006, p. 1134, tradução livre).

De forma regular, os pronunciamentos aqui analisados tendem a reforçar a ideia, o preconceito ou a noção pré-reflexiva de que existe um inimigo permanentemente planejando ataques sobre os estadunidenses. Neste sentido, tal como há cinco séculos asseverava-se que o demônio de maneira incessante procurava infringir o maior dano possível aos cristãos (KRAMER; SPRENGER, 2002, p. 92), hoje se argumenta que: "Os ataques a essa Nação revelaram as intenções de um inimigo determinado e cruel que continua conspirando contra o nosso povo. As forças do terrorismo global não podem ser apaziguadas, e nem podem ser ignoradas"[184] (BUSH, 2006, p. 1135, tradução livre). E também: "Terroristas em terras estrangeiras ainda têm esperança de atacar nosso país. Eles ainda esperam

[183] No original: "The lives of every person here were changed by the events of September the 11th, 2001. You felt the anger and the sense of loss that day. You stood ready to serve your country in a time of need. And each of you now has a part in protecting America against the threats of a new era. […] Tomorrow, America will mark a sad anniversary. The memories of September 11th will never leave us. We will not forget the burning towers and the last phone calls and the smoke over Arlington. We will not forget the rescuers who ran toward danger and the passengers who rushed the hijackers. We will not forget the men and women who went to work on a typical day and never came home. We will not forget the death of schoolchildren who were on a school trip."

[184] No original: "The attacks on this Nation revealed the intentions of a determined and ruthless enemy that still plots against our people. The forces of global terror cannot be appeased, and they cannot be ignored".

assassinar os nossos cidadãos”[185] (BUSH, 2007e, p. 1339, tradução livre).

Em termos concretos, esse inimigo foi frequentemente identificado com o estereótipo do terrorista islâmico. Apenas nove dias após os atentados o então presidente estadunidense definia a prática terrorista como “uma forma marginal de extremismo islâmico” (BUSH, 2005a, p.1141). Em idêntico sentido, anos depois, a Secretária de Estado na época argumentou:

> Os islamistas radicais atuais estão nadando contra a maré do espírito humano. Eles agarram as manchetes com sua brutalidade implacável, e eles podem ser brutais. Mas eles estão habitando nas margens exteriores de uma grande religião mundial. E são radicais de um tipo especial. Eles estão em revolta contra o futuro.[186] (RICE, 2005c, p. 3, tradução livre).

No caso das chamadas *ciberameaças*, também se trabalha sobre noções instaladas a respeito das características daqueles grupos enquadrados dentro do lugar dos perigosos. Assim, como argumenta Cavelty, existe uma ideia instalada de que potencialmente qualquer pessoa com um computador conectado à Internet tem a possibilidade de encarar um ciberataque. Argumenta-se que ferramentas de hackers são de simples obtenção e que sua operação, de baixa complexidade técnica. Nesta linha, ao longo das décadas instaurou-se a ideia dos perigos envolvidos nas atividades online de jovens hackers e ativistas políticos

> Baixas barreiras no acesso às ciberatividades maliciosas, incluindo a ampla disponibilidade de ferramentas de hacker, significa que tanto um indivíduo quanto um pequeno grupo de ciberatores podem

[185] No original: “All these steps to protect the homeland have made us safer, but we’re not yet safe. Terrorists in foreign lands still hope to at-tack our country. They still hope to kill our citizens”.

[186] No original: “Today's radical Islamists are swimming against the tide of the human spirit. They grab the headlines with their ruthless brutality, and they can be brutal. But they are dwelling on the outer fringes of a great world religion; and they are radicals of a special sort. They are in revolt against the future.”

> potencialmente ocasionar um dano significativo ao Departamento de Estado e à segurança econômica e nacional dos EUA[187] (EUA, 2011b, p. 3, tradução livre).

Na sua análise a respeito dos discursos ligados à ideia das *ciberameaças*, Cavelty (2007b, p. 27) conclui que não houve uma mudança substancial em relação ao enquadramento dessas ameaças após o 11 de setembro. O que pode ser reconhecido nos documentos oficiais, argumenta, é uma mudança na atenção das agências que deslocaram o foco de hackers apresentados como terroristas a terroristas hackers e, especialmente, de origem muçulmana.

Como foi argumentado no capítulo precedente, ao longo da história foram enquadrados diversos grupos sociais, fenômeno que expressa o caráter estruturalmente seletivo do poder punitivo, o qual se funda na capacidade de escolher de forma arbitrária o seu inimigo. Assim, Saint-Pierre (2015, p.12) salienta que a noção de terrorismo "tornou-se politicamente versátil para identificar o inimigo em três planos diferentes, substituindo a função que desempenhou o conceito polemo-lógico (sic) do 'comunismo' durante toda a Guerra Fria".[188]

Neste sentido, Bush, em 2005, assegurava que: "A liberdade já se enfrentou com as ideologias odiosas no passado. Derrotamos o fascismo, derrotamos o comunismo e agora derrotaremos esta ideologia odiosa dos terroristas que atacaram [os Estados Unidos da] América"[189] (BUSH, 2007e, p. 1341, tradução livre).

---

[187] No original: "Low barriers to entry for malicious cyber activity, including the widespread availability of hacking tools, mean that an individual or small group of determined cyber actors can potentially cause significant damage to both DoD and U.S. national and economic security. Small-scale technologies can have an impact disproportionate to their size; potential adversaries do not have to build expensive weapons systems to pose a significant threat to U.S. national security."

[188] A respeito deste assunto, cabe salientar que, embora Saint-Pierre identifique na "ambiguidade conceitual" da noção de terrorismo o fundamento de tal versatilidade, a orientação seguida na presente pesquisa é que este constitui um elemento estrutural do discurso do poder punitivo. A arbitrariedade na seleção e na caracterização da população-alvo da ação punitiva é uma constante e não uma variável do seu exercício.

[189] No original: "Our Nation has accepted a mission, and we're moving forward with resolve. Spreading freedom is the work of generations, and no one knows it better

Ainda, cabe salientar que a própria NSA, agência que encabeça o sistema de vigilância de comunicações, foi criada em tempos do Presidente Truman, com o mandado de contribuir para a produção de informação de inteligência no marco da luta contra o inimigo comunista. Nas palavras do Presidente Obama:

> nos primórdios da Guerra Fria, o Presidente Truman criou a Agência Nacional de Segurança, ou NSA, para nos dar uma compreensão acerca do bloco soviético e fornecer aos nosso líderes as informações que precisavam para confrontar a agressão e evitar a catástrofe[190] (OBAMA, 2014, p. 1, tradução livre).

iii.d.A veracidade da narrativa em torno à ameaça é inquestionável: ao mesmo tempo em que se caracteriza a ameaça, também se defende a veracidade do relato. Para isto:

iii.d.1.Inverte-se a valoração dos fatos: Cavelty (2007a) estuda, precisamente, alguns dos cenários que têm sido trabalhados na história das Tecnologias de Informação e Comunicações. O argumento central da autora consiste em que a mídia e diversos atores estatais têm reiteradamente difundido uma narrativa que envolve a construção de um cenário de *ciberameaças*, enquanto os acontecimentos reais estão longe de resultar em mortes ou danos significativos. "De fato, cenários ameaçantes de grandes ocorrências disruptivas no domínio cibernético […] desencadeadas por atores maliciosos permaneceram apenas nisso – cenários" (CAVELTY, 2007a, p. 3, tradução livre).

Isto, cabe salientar, dá-se em um contexto de mudança tecnológica acelerada, no qual a profundidade e a complexidade das modificações configuram um cenário

---

than you. Freedom has contended with hateful ideologies before. We defeated fascism; we defeated communism; and we will defeat the hateful ideology of the terrorists who attacked America".

[190] No original: "in the early days of the Cold War, President Truman created the National Security Agency, or NSA, to give us insights into the Soviet bloc, and provide our leaders with information they needed to confront aggression and avert catastrophe".

em que uma porção substantiva da população, ainda que usuária, tem dificuldades de compreender os mecanismos e processos envolvidos e, assim, as capacidades de avaliar de forma independente as implicações técnicas daquilo que é relatado.

Em idêntica linha, Cavelty argumenta que existe um amplo debate entre os especialistas em relação à avaliação das ciberameaças, enquanto que as publicações oficiais deixam essa avaliação numa *nuvem de especulações*, com a utilização reiterada de expressões como “poderia, haveria e talvez” (CAVELTY, 2007b, pp. 124-138). Assim, por exemplo, na *Estratégia para proteger o ciberespaço*, definia-se que:

> Enfrentamos adversários, incluindo estados-nação e terroristas, que poderiam lançar ataques cibernéticos ou procurar explorar nossos sistemas. Em tempo de paz, os inimigos da América conduzirão espionagem contra o nosso governo, centros de pesquisa universitários e empresas privadas. As atividades provavelmente incluirão o mapeamento de sistemas de informação dos EUA, identificando metas-chave, atando nossa infraestrutura com "portas traseiras" e outros meios de acesso. Em tempos de guerra ou de crise, os advogados podem tentar intimidar, atacando infraestruturas críticas e funções econômicas fundamentais, ou prejudicando a confiança do público nos sistemas de informação. Eles também podem tentar diminuir a resposta militar dos EUA ao interromper sistemas do Departamento de Defesa (DoD), da Comunidade de Inteligência e de outras organizações governamentais, bem como de infraestruturas críticas[191] (EUA, 2003, p. 49–50, tradução livre).

[191] No original: “We face adversaries, including nation states and terrorists, who could launch cyber attacks or seek to exploit our systems. In peacetime America’s enemies will conduct espionage against our government, university research centers, and private companies. Activities would likely include mapping U.S. information systems, identifying key targets, lacing our infrastructure with ‘back doors’ and other means of

iii.d.2. Tenta-se neutralizar qualquer fonte de autoridade que estabeleça uma interpretação contrária à manifestada.

Logo após os vazamentos de Snowden, no momento de maior intensidade dos questionamentos (domésticos e internacionais) sobre o sistema de vigilância massiva de comunicações, a posição oficial dos Estados Unidos foi de voltar o debate em direção ao suposto êxito do monitoramento em atingir o objetivo declarado.

Neste marco é que foi introduzido no debate, pela primeira vez, a ideia de que o sistema de vigilância da NSA teria levado a desarticular uma série de *eventos terroristas* e, assim, vidas teriam sido salvas.

Em junho de 2013, duas semanas após a publicação do primeiro artigo relacionado aos documentos Snowden, o Presidente Obama afirmou, por ocasião de uma conferência de imprensa conjunta com a Chanceler Merkel em Berlim, que o sistema de vigilância de comunicações tinha servido para salvar vidas. Nas suas palavras: "Sabemos de pelo menos 50 ameaças que foram evitadas por causa desta informação, não apenas nos Estados Unidos, mas em alguns casos, ameaças aqui na Alemanha. Então vidas foram salvas."[192] (OBAMA, 2013d, p. 5, tradução livre).

Nos meses seguintes, a narrativa ligada à quantidade e aos aspectos específicos desses supostos ataques frustrados esteve no centro do debate público. O então Diretor da NSA referiu-se a "54 eventos" dos quais 42 teriam sido conspirações neutralizadas ao longo do planeta.

> "Cinquenta e quatro atividades terroristas foram interrompidas; zero violações intencionais. Quando você pensa sobre como o nosso governo opera e o que nós

---

access. In wartime or crisis, adversaries may seek to intimidate by attacking critical infrastructures and key economic functions or eroding public confidence in information systems. They may also attempt to slow the U.S. military response by disrupting systems of the Department of Defense (DoD), the Intelligence Community, and other government organizations as well as critical infrastructures".

[192] No original: "We know of at least 50 threats that have been averted because of this information not just in the United States, but in some cases, threats here in Germany. So lives have been saved."

> fizemos para reunir os três ramos, acho que é algo para se orgulhar. Defendemos a nação e nossos aliados 54 vezes e asseguramos a proteção de nossas liberdades civis e privacidade na supervisão de todos os três ramos do nosso governo. Acho que é isso que a nação espera que nosso governo faça: interrompa atividades terroristas, defenda nossas liberdades civis e nossa privacidade." (ALEXANDER, 2013b, p. 2–3, tradução livre).

Além da questão a respeito da veracidade dessas afirmações, que têm sido longamente questionada (ELLIOTT, 2013), o ponto central deste debate foi o de tentar desacreditar aqueles pronunciamentos críticos sobre o funcionamento do programa.

iv. Quando? – Outra regularidade do discurso do poder punitivo consiste em argumentar em relação à necessidade de uma intervenção de caráter urgente sobre a base de um fenômeno cuja ocorrência apresenta uma frequência alarmante.

iv.a. Argumenta-se que a intervenção tem que ser realizada com urgência: Como analisado no caso do Malleus Maleficarum, a narrativa inclui, de maneira recorrente, expressões tendentes a afirmar que o fenômeno em questão apresenta uma elevada frequência. Em referência a eventos qualificados de terroristas, o mandatário estadunidense afirmava que: "A guerra veio até nossas costas na manhã do 11 de setembro de 2001. Desde esse momento, os terroristas têm continuado a atacar em Bali, em Riade, em Istambul, em Madrid, em Bagdá, em Londres, em Sharm el- Sheikh e em qualquer outro lugar"[193] (BUSH, 2007e, p. 1338, tradução livre).

Neste sentido, consultada sobre as características da vigilância por trás das denúncias acontecidas em 2005, a então Secretaria Rice argumentava que:

[193] No original: "The war came to our shores on the morning of September the 11th, 2001. Since then the terrorists have continued to strike in Bali, in Riyadh, in Istanbul, and Madrid and Baghdad and London and Sharm el- Sheikh and elsewhere".

> "Existe uma certa urgência a respeito do tipo de informação ligada à detecção de ameaças terroristas no interior dos Estados Unidos, uma certa urgência que está ligada à compreensão das comunicações entre pessoas que estão se comunicando do interior dos Estados Unidos com organizações terroristas fora dos Estados Unidos"[194] (RICE, 2005a, parag. 5, tradução livre).

Em linhas gerais, evoca-se a noção de que existe um risco iminente que configura, portanto, uma situação emergencial. Nas palavras de Obama: "Os americanos reconheceram que tínhamos de nos adaptar a um mundo em que uma bomba pode ser construída em um porão e que nossa rede elétrica pode ser cortada por operadores a um oceano de distância"[195] (OBAMA, 2014, p. 3, tradução livre).

No caso específico das ameaças ligadas ao uso de tecnologias digitais, Cavelty argumenta que, nos relatórios oficiais visando documentá-las, verifica-se uma tendência à teorização a respeito de eventuais acontecimentos futuros e o progressivo descolamento entre essas hipóteses e as ocorrências efetivamente registradas. A respeito dos relatórios oficiais, a autora afirma: "eles se transformaram em histórias para provar a necessidade de atuar",[196] (CAVELTY, 2007a, p. 124–138, tradução livre).

Assim, a ideia de que é preciso intervir para neutralizar o perigo iminente configurado pela possibilidade de ataques terroristas é adicionada à noção de que as ciberameaças também configuram um fenômeno de elevada frequência e, portanto, uma emergência. Nesta linha, o Presidente estadunidense estabelecia, através de uma Ordem Executiva no ano 2015, que:

---

[194] No original: "There is a certain urgency to the kind of information that is attached to detecting terrorist threats within the United States, a certain urgency that is attached to understanding communications between people who are communicating inside the United States with terrorist organizations or activities outside of the United States".

[195] No original: "Americans recognized that we had to adapt to a world in which a bomb could be built in a basement, and our electric grid could be shut down by operators an ocean away".

[196] No original: "they turned into stories to prove the need for action".

> a crescente prevalência e severidade de ciberatividades maliciosas, originadas ou dirigidas por pessoas localizadas, no todo ou em parte substancial, fora dos Estados Unidos, constituem uma ameaça singular e extraordinária à segurança nacional, à política externa e à economia dos Estados Unidos. Portanto, declaro uma emergência nacional para lidar com esta ameaça[197] (EUA, 2015a, p. 1, tradução livre).

iv.b.Afirma-se a veracidade da situação emergencial. Além do efeito ligado à própria reiteração argumentativa em relação às ameaças, na narrativa incluem-se de forma recorrente expressões orientadas a reafirmar a veracidade da situação emergencial. Em paralelo ao argumentado na Bula do Papa Inocêncio VIII (2002), em relação à *desfaçatez* das manifestações que negavam que a bruxaria fosse praticada em regiões específicas, o Presidente Bush advertia sobre o perigo de duvidar da situação emergencial:

> "Existe outra importante lição que deixa o 11 de setembro e que não devemos esquecer, isto é, não podemos mais considerar as ameaças que podem existir no exterior como superadas. Em outras palavras, quando o Presidente e / ou qualquer outra figura de autoridade vê uma ameaça, devemos levá-la a sério"[198] (BUSH, 2007b, p. 606, tradução livre).

Um aspecto também característico é a referência a informações que não são de acesso público, para referendar a veracidade daquilo que se afirma. Tanto Bush quanto Obama fazem menção aos relatórios de inteligência

[197] No original: "I, BARACK OBAMA, President of the United States of America, find that the increasing prevalence and severity of malicious cyberenabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. I hereby declare a national emergency to deal with this threat".

[198] No original: "There's another very important lesson about September the 11th that we must never forget, and that is, we can no longer take threats that may exist overseas for granted. In other words, when the President and/or anybody else in authority sees a threat, we must take it seriously".

reservados ao Presidente da Nação, como se exemplifica nas seguintes frases:

> "Sou informado com os últimos dados a respeito das ameaças ao nosso país, e essas ameaças são reais. O inimigo está ferido, mas ainda engenhoso e ativamente recrutando e ainda perigoso. Não podemos nos permitir um momento de complacência"[199] (BUSH, 2006, p. 1136, tradução livre).

v. Como? – As regularidades agrupadas neste ponto reúnem os aspectos mais específicos da racionalidade por trás da vigilância massiva. No discurso, ela se apresenta como um tipo de intervenção voltada especificamente à superação dos desafios das "novas ameaças" para a segurança doméstica e internacional. Nas palavras de Bush, a vigilância de comunicações autorizada pela Lei Patriota "toma em consideração as novas realidades e perigos causados pelos terroristas modernos" (BUSH, 2005c, p. 1306, tradução livre). De toda maneira, como analisado a seguir, os termos nos quais se definem as características específicas destas demandas "novas e em alguma medida de maior complexidade"[200] (OBAMA, 2014, p. 2, tradução livre), no que se refere à manutenção da segurança, guardam uma correspondência estrutural com aquelas que cinco séculos atrás problematizavam os Inquisidores Kramer e Sprenger.

v.b. Retórica belicista: A presença de uma estrutura retórica centrada na noção de um conflito de características bélicas permeia os diversos documentos analisados. Como argumenta Saint-Pierre (2014, p. 10, ênfase no original): "George W. Bush declarou uma guerra global contra o 'terrorismo'" sendo esse o referencial que caracterizou a política sobre o assunto durante toda a administração Bush (HUYSMANS, 2006; BURKE, 2006; BIGO; TSOUKALA, 2008; BUZAN; WÆVER, 2009).

---

[199] No original: "I am briefed from the latest information on the threats to our country, and those threats are real. The enemy is wounded but still resourceful and actively recruiting and still dangerous. We cannot afford a moment of complacency".

[200] No original: "emerging threats from terrorist groups, and the proliferation of weapons of mass destruction placed new and in some ways more complicated demands".

Neste sentido, nos discursos analisados o sistema de vigilância massiva de comunicações é referido em tanto dispositivo para auxiliar às agencias de segurança em um conflito de conceituação eminentemente bélica, seja na sua forma original de "guerra ao terror"[201] (BUSH, 2010c; POWELL, 2002, 2004, RICE, 2005a, 2006c, a, 2007), seja na sua formulação posterior de "guerra global ao terror"[202] (RICE, 2005b, c) ou na sua forma alternativa de "guerra contra o terror"[203] (BUSH, 2007c).

Além dessas referencias mais obvias, o uso de uma retórica que apela à ideia de um confronto bélico espalha-se ao longo de todo o período analisado. Assim, nos documentos doutrinários se identifica às Tecnologias de Informação e Comunicações alternativamente como "espaço" de batalha, quanto um instrumento ou alvo de ataques. Isto é retratado nos diversos documentos doutrinários através de conceitos tais como: "ciberespaço como um domínio de guerra" (EUA, 2006, tradução livre); "ciberespaço como domínio operacional das Forças Armadas" (EUA, 2011b); "ciberarmas" (EUA, 2011a); "ciberataques" (EUA, 2015); dentre outros.

Na administração Obama, por sua vez, abandona-se a referencia literal a uma guerra contra o terrorismo, mas se manteve aquilo que é central da retórica bélica que é a figura do inimigo. Assim, segundo o então presidente Obama a capacidade de "penetrar as comunicações digitais" configura um elemento central no confronto aos "inimigos" e as ameaças que afetam os Estados Unidos. Assim, em referência específica aos programas que configuram o sistema de vigilância massiva de comunicações, após o vazamento dos documentos Snowden, o então presidente dos Estados Unidos argumentava que:

> Em primeiro lugar, todos os que examinaram estes problemas, incluindo os céticos dos programas existentes, reconhecem que temos verdadeiros inimigos e ameaças e que a inteligência desempenha um papel vital na sua confrontação. Não podemos impedir

[201] No original: "war on terror".
[202] No original: "global war on terror".
[203] No original: "war against terror".

> ataques terroristas ou ameaças cibernéticas sem alguma capacidade de penetrar nas comunicações digitais, seja para desvendar uma trama terrorista, para interceptar malware que vise uma bolsa de valores, para garantir que os sistemas de controle de tráfego aéreo não sejam comprometidos ou para que garantir que hackers não esvaziem suas contas bancárias. Espera-se que protejamos o povo americano; isso exige que tenhamos capacidades neste campo[204] (OBAMA, 2014, tradução livre).

Tal como no Malleus argumentava-se um estado de guerra entre homens e demônios (KRAMER e SPRENGER, 2002, p. 363) que impunha a necessidade de adotar medidas extraordinárias para vencer o inimigo, idêntico argumento, embora com conteúdo diferente, é reiterado nestes discursos. Aquilo que Tsoukala (2008, p. 54) denomina a *associação dupla do terrorismo com a guerra*, que compreende a declaração dos atentados do 11 de setembro como um ato de guerra e o engajamento no início de uma guerra contra eles, tem o efeito político de invocar um estado de emergência.

> Antes de mais nada, o programa da NSA é um programa importante para proteger [os Estados Unidos da] América. Estamos em guerra e, como Comandante em Chefe, tenho que usar os recursos à minha disposição, dentro da lei, para proteger o povo americano. […] Penso que a maioria dos americanos entende a necessidade de descobrir o que o inimigo está pensando e o que está fazendo. Estamos em guerra com um bando de assassinos de sangue frio que

[204] No original: "First, everyone who has looked at these problems, including skeptics of existing programs, recognizes that we have real enemies and threats and that intelligence serves a vital role in confronting them. We cannot prevent terrorist attacks or cyber threats without some capability to penetrate digital communications, whether it's to unravel a terrorist plot, to intercept malware that targets a stock exchange, to make sure air traffic control systems are not compromised, or to ensure that hackers do not empty your bank accounts. We are expected to protect the American people; that requires us to have capabilities in this field."

> matarão num instante[205] (BUSH, 2010d, p. 1–2, tradução livre).

Assim, como salientado pelos teóricos da securitização, a retórica belicista apela, por um lado, à necessidade de níveis maiores de discricionariedade (WÆVER, 1988, p. 4) e, por outro, à impossibilidade de debater publicamente as ações encaradas. Isto é, invoca-se o direito ao segredo (BUZAN et al., 1998, p. 208). Isto se reflete de forma evidente no enquadramento normativo do sistema de vigilância massiva de comunicações, que, como referimos, centra-se em cortes cuja atuação é secreta (EUA, 2001b, 2008c), mas também foi especialmente destacado por ocasião das denúncias sobre o sistema formuladas por ex-membros da comunidade de inteligência. Neste sentido, tanto no caso de Drake quanto no de Snowden, salientou-se que as alternativas do programa não poderiam ser debatidas publicamente porque conformavam parte das operações secretas de uma nação em guerra.

No primeiro caso, o então Presidente estadunidense afirmava que toda publicidade sobre mecanismos e procedimentos supunha fortalecer a posição do inimigo: "Minha opinião pessoal é que a publicação de informações sobre este importante programa em um tempo de guerra foi um ato vergonhoso. O próprio fato de que estejamos debatendo este programa está ajudando o inimigo"[206] (BUSH, 2007f, p. 1878, tradução livre). Essa ideia foi reforçada na época pela Secretária de Estado Condolezza Rice, que, em entrevista na cadeia noticiosa Fox News, argumentava:

> Quanto maior seja a exposição destes programas sensíveis, mais se mina nossa habilidade de perseguir terroristas, de

[205] No original: "First of all, the NSA program is an important program in protecting America. We're at war, and as the Commander in Chief, I've got to use the resources at my disposal, within the law, to protect the American people. […] I think most Americans understand the need to find out what the enemy is thinking, and that's what we're doing. We're at war with a bunch of cold blooded killers who will kill on a moment's notice."

[206] No original: "My personal opinion is it was a shameful act for someone to disclose this very important program in a time of war. The fact that we're discussing this program is helping the enemy".

> conhecer suas atividades. Temos de lembrar que, nesta guerra contra o terrorismo, não estamos falando em atividade criminosa na qual pode se permitir que alguém cometa um crime e posteriormente seja aprisionado e questionado. No caso dos terroristas terem êxito em cometer seu crime, então centenas ou, de fato, milhares de pessoas morrerão[207] (RICE, 2005a, parag. 13, tradução livre).

Sete anos depois, questionado durante uma coletiva sobre a severidade na aplicação da legislação penal estadunidense no caso de Snowden e de outros denunciantes, o então Secretário de Estado Kerry empregou um argumento semelhante:

> O que eu vejo é um indivíduo que ameaçou seu país e colocou os americanos em risco através das suas ações. Pessoas morrerão como consequência do que esse homem tem feito. Este é um ato muito perigoso, e qualquer um que queira torná-lo um herói está julgando mal como se mantém a salvo e como é complicado proteger a [os Estados Unidos da] América, no mundo de hoje, de terroristas autodidatas, da radicalização na Internet e de outras coisas que ocorrem[208] (KERRY, 2013, p. 3, tradução livre)

v.c.<u>O inimigo é difuso, mas sua ação é coordenada:</u> Tanto na hipótese do terrorismo na sua versão mais diretamente ligada ao 11 de setembro, como naquela que enfatiza nas ameaças ligadas às Tecnologias de Informação e

[207] No original: “The more that we get the exposure of these very sensitive programs, the more it undermines our ability to follow terrorists, to know about their activities. We have to remember that in this war on terrorism we're not talking about criminal activity, where you can allow somebody to commit the crime and then you go back and you arrest them and you question them. If they succeed in committing their crime, then hundreds or indeed thousands of people die”.

[208] No original: “What I see is an individual who threatened his country and put Americans at risk through the acts that he took. People will die as a consequence of what this man did. This is a very dangerous act, and anybody who wants to make him a hero is misjudging how they stay safe and how complicated it is to protect America in today’s world of self-made terrorists and of internet radicalization and other things that take place.”

Comunicações, conceitua-se o inimigo como tendo características difusas, mas ação coordenada. No âmbito acadêmico, este enfoque ficou ilustrado com singular clareza por Joseph Nye (2010), quem, em um ensaio publicado pela Universidade de Harvard, identificou o fenômeno da difusão de poder como próprio do ciberespaço. Segundo o autor, a conjuntura atual está marcada por um crescente desafio à capacidade de controle dos estados e de manutenção do uso da força. Isto, segundo Nye, tem sua causa nas transformações introduzidas em matéria de comunicações, as quais teriam modificado a *natureza do poder*, fortalecendo mais que proporcionalmente aos atores tradicionalmente considerados mais débeis e dando lugar a uma *assimetria na vulnerabilidade*.[209] Em idêntico sentido, Samuel Liles (2010, p. 49) argumentou, na *Conferência sobre ciberconflito,* organizada pela Organização do Tratado do Atlântico Norte (OTAN), que o conflito contemporâneo é definido pela luta contra um *adversário diverso e distribuído*. Assim, a vigilância de comunicações é apresentada como uma ferramenta imprescindível para detectar terroristas que estão *escondidos à vista,* como propõe Bonelli (2008). Uma vez escondidos, mas não isolados, propõe-se rastreá-los através das suas comunicações, de forma que a vigilância emerge como uma "ferramenta para rastrear terroristas"[210] (BUSH, 2005a, 2006; EUA, 2001b; RICE, 2005c, 2006b), para "caçar terroristas"[211] (OBAMA, 2015b) e uma "ferramenta para detectar planos terroristas[212] (BUSH, 2007a, c, OBAMA, 2013b, 2014). Como resume o Presidente Obama, trata-se de um cenário no qual seria preciso encontrar a *agulha na palheiro*: "Precisamos de novos pensamentos para uma nova era. Agora temos que desvendar terroristas, encontrando uma agulha no palheiro

[209] O autor define esse conceito no sentido de que: "Assimetrias na vulnerabilidade significa que os atores menores têm mais capacidade de exercer poder duro e macio no ciberespaço do que em muitos outros domínios mais tradicionais da política mundial." NYE, 2010, p. 19). Como elementos chave dessas transformações, salienta idênticos argumentos que aqueles que se enunciam nos acontecimentos discursivos da amostra, a saber: baixas barreiras à entrada e anonimato.
[210] No original: "tools to track terrorists before they harm Americans".
[211] No original: "hunt down terrorists".
[212] No original: "tool for detecting terrorist plots".

das telecomunicações globais"[213] (OBAMA, 2013b, p. 4, tradução livre).

Idêntica avaliação se faz no momento de caracterizar as ameaças que envolvem o uso específico de Tecnologias de Informação e Comunicações. Neste caso, o argumento consiste em que, dadas as particularidades destas tecnologias, em especial do funcionamento da Internet, a ação terrorista ou criminal se vê facilitada ao passo que a detecção e a punição são dificultadas.

Neste sentido, tal é a definição na doutrina estadunidense para o ciberespaço: "O ciberespaço fornece um meio de ataque organizado à nossa infraestrutura à distância. Esses ataques exigem apenas tecnologia corriqueira e permitem que os atacantes ofusquem suas identidades, locais e caminhos de entrada"[214] (EUA, 2003, p. 6–7, tradução livre).

Assim, tal como no caso dos terroristas *convencionais*, também se argumenta que: "Os Estados Unidos estão rastreando e detendo de forma agressiva criminosos e terroristas online"[215] (CLINTON, 2011b, p. 3, tradução livre).

Em definitivo, tal como os demônios se ocultavam entre a população perante o uso de encantamentos, os inimigos atuais o fazem empregando as modernas TICs. Como refere o ex-Diretor da NSA:

> O que estamos fazendo é coletando metadados para perseguir os maus que usam os mesmos dispositivos e os mesmos equipamentos que nós usamos. Eles se escondem entre nós para matar o nosso povo[216] (ALEXANDER, 2013a, p. 3, tradução livre).

---

[213] No original: "We need new thinking for a new era. We now have to unravel terrorist plots by finding a needle in the haystack of global telecommunications".

[214] No original: "Cyberspace provides a means for organized attack on our infrastructure from a distance. These attacks require only commodity technology, and enable attackers to obfuscate their identities, locations, and paths of entry".

[215] No original: "The US is aggressively tracking and deterring criminals and terrorists online".

[216] No original: "My mission, the mission of NSA and Cyber Command, is to defend this country. That's our mission. And in order to do that we need programs that we didn't have prior to 9/11[…] to solve 9/11 we needed some capabilities to connect the dots that we couldn't do prior to 9/11. And if you think that we would listen to everybody's telephone calls and read everybody's email to connect the dots, how do you do that? And the answer is that's not logical. That would be a waste of our

v.d.Esse inimigo é desvalorizado e merece um trato diferencial. Outra regularidade encontrada nos discursos analisados é a de se referir ao inimigo de maneira a localizá-lo em uma posição inferior. Nas palavras do então Presidente estadunidense: “Não reconhecem parâmetros morais. Não têm consciência. Não se pode racionalizar com os terroristas”[217] (BUSH, 2005c, p. 1306, tradução livre).

A retórica usada tem amplas conotações negativas,[218] como por exemplo: atores maliciosos[219] (EUA, 2003, p. 6, tradução livre); malfeitores[220] (BUSH, 2005b, p. 31, tradução livre); malvados[221] (BUSH, 2005c, p. 1307, tradução livre); extremistas violentos[222] (OBAMA, 2013a, p. 15, tradução livre); extremistas radicais[223] (KERRY, 2014, p. 3, tradução livre).

Como argumenta Tsoukala (2008, p. 62–64), a narrativa salienta a suposta *inferioridade moral* na definição do inimigo terrorista. Isto está logicamente ligado à conceituação do conflito entre o bem e o mal. O conflito fica então enquadrado em um tipo de enfrentamento entre a *civilização e a barbárie*, no qual se legitimam procedimentos extraordinários cujo objetivo declarado é o de se aplicar exclusivamente sobre essa população inferiorizada.

É precisamente essa ideia de que as medidas de vigilância são práticas exercidas de maneira restrita sobre uma população-alvo a qual se buscou difundir com os termos “Programa de Vigilância de Terroristas” (BUSH, 2005a, 2010e, b, a) ou um “programa de vigilância de conversações

---

resources to get there. And from my perspective, what you need is a way to focus on the bad guy. […] And one of the key misunderstandings is, you’re listening to our phone calls, you’re reading our emails, for the American people. That’s flat not true. What we’re doing is we’re collecting metadata to go after bad guys who use the same devices and the same equipment that we do. They hide amongst us to kill our people.”

[217] No original: “They recognize no barrier of morality. They have no conscience. The terrorists cannot be reasoned With”.

[218] De fato, Saint-Pierre (2015, p.14) foca no próprio “sentido pejorativo com que pragmaticamente empregou-se essa palavra ao longo da história”.

[219] No original: “Malicious actors”.

[220] No original: “Evildoers”.

[221] No original: “Evil ones”.

[222] No original: “violent extremists”.

[223] No original: “radical extremists”.

terroristas e comunicações terroristas"[224] (RICE, 2006, p. 2, tradução livre). Em igual sentido, o Presidente Obama afirmava: "quero esclarecer mais uma vez que [os Estados Unidos da] América não está interessada em espionar pessoas comuns. Nossa inteligência está focada, sobretudo, em obter informação necessária para proteger nosso povo e, em muitas oportunidades, proteger os nossos aliados"[225] (OBAMA, 2013b, p. 5, tradução livre). Essa ideia será reiterada por ocasião de uma declaração conjunta com a chanceler Merkel em Berlim, na qual o presidente dos Estados Unidos asseverava que:

> Esta não é uma situação em que estamos a passar pelos e-mails normais de cidadãos alemães, de cidadãos americanos ou de cidadãos franceses, ou de qualquer outra pessoa. Esta não é uma situação em que simplesmente entramos na Internet e começamos a procurar de qualquer maneira que desejarmos. Trata-se de um sistema circunscrito, estreito, dirigido para que possamos proteger nosso povo[226] (OBAMA, 2013d, p. 5, tradução livre).

v.e.A estratégia do inimigo se apresenta sempre como orientada à exploração de vulnerabilidades. Segundo a narrativa conformada a partir dos documentos analisados, um elemento central destas ameaças é sua orientação à exploração de vulnerabilidades. Como se define na Estratégia Nacional para proteger o ciberespaço:

> Os atores maliciosos no ciberespaço podem adotar diversas formas, incluindo indivíduos,

[224] No original: "a surveillance program of terrorist conversations and terrorist communications".
[225] No original: "I want to make clear once again that America is not interested in spying on ordinary people. Our intelligence is focused, above all, on finding the information that's necessary to protect our people, and -- in many cases – protect our allies".
[226] No original: "This is not a situation in which we are rifling through the ordinary e-mails of German citizens or American citizens or French citizens or anybody else. This is not a situation where we simply go into the Internet and start searching any way that we want. This is a circumscribed, narrow system directed at us being able to protect our people.".

> cartéis criminosos, terroristas ou estados nacionais. Ao mesmo tempo que os atacantes adotam formas variadas, todos eles procuram explorar as vulnerabilidades, seja de desenho ou de implementação de software, hardware, redes ou protocolos, para atingir um amplo espectro de efeitos políticos e econômicos[227] (EUA, 2003, p. 27, tradução livre).

Isto não se limita exclusivamente ao *ambiente cibernético* no qual, tal como adverte Cavelty (2007a, p. 131), a ideia de que existe uma vulnerabilidade inerentemente associada às TICs é longamente trabalhada já desde a década de 1980, mas também ao terrorismo convencional. Um aspecto recorrente é a ideia da vulnerabilidade associada à intimidação e radicalização da população. De fato, como argumentou a então Secretária de Estado Clinton:

> Assim como os terroristas aproveitaram a abertura de nossa sociedade para conspirar, extremistas violentos usam a internet para radicalizar e intimidar. À medida que trabalhamos para o avanço das liberdades, devemos também trabalhar contra aqueles que usam as redes de comunicação como ferramentas de ruptura e medo[228] (CLINTON, 2011a, p. 4, tradução própria).

Assim, tal como no século XV a debilidade mental das mulheres as fazia vulneráveis à ação de Satã (o inimigo), no século XXI se afirma, como o fazem os dirigentes da empresa Google, que estamos perante uma *juventude alienada.* Neste sentido, os autores argumentam que *a*

[227] No original: "Malicious actors in cyberspace can take many forms including individuals, criminal cartels, terrorists, or nation states. While attackers take many forms, they all seek to exploit vulnerabilities created by the design or implementation of software, hardware, networks, and protocols to achieve a wide range of political or economic effects".

[228] No original: "Just as terrorists have taken advantage of the openness of our society out their plots, violent extremists use the internet to radicalize and intimidate. As we work to advance freedoms, we must also work against those who us communication networks as tools of disruption and fear".

> *batalha por corações e mentes chega à Internet*, na qual "jovens e pouco instruídos, terão rancores que os extremistas explorarão em proveito próprio". Esses sentimentos, concluem, "são comuns a muitos jovens. No entanto, a novidade é que um grande número deles expressa seus rancores na internet de maneira que, intencionalmente ou não, os expõem a recrutadores e terroristas" (SCHMIDT; COHEN, 2013, p. 186–187). Em idêntico sentido o Presidente estadunidense na época afirmava, em referência aos acontecimentos em San Bernardino,[229] que: "ao tempo que a Internet ofusca a distância entre países, vemos os crescentes esforços por parte dos terroristas para envenenar as mentes das pessoas"[230] (OBAMA, 2015b, p. 1, tradução livre).
>
> Além da sua função normatizante, esta questão da vulnerabilidade aponta para um sentido específico, que é o de orientar a ação de vigilância não só a um grupo presumidamente reduzido de potenciais grupos de ameaças, como objetivo declarado no ponto precedente, mas à população em geral. Como explicitado no ano 2008 pela então Secretária de Estado Rice:
>
> > os principais especialistas em segurança, de maneira crescente, argumentam que a guerra contra o terrorismo constitui um tipo de contra-insurgência global. Isto significa que o centro de gravidade do conflito não são simplesmente os terroristas, mas as populações que eles procuram influenciar, radicalizar e, em muitos casos, aterrorizar[231] (RICE, 2005c, p. 4, tradução livre).

Como salientado no capítulo precedente, de forma recorrente argumenta-se a respeito da existência de um estado de exceção vinculado à emergência que tem como consequência o apelo ao uso de meios extraordinários. Isto é a legitimação de

---

[229] Ver nota 6.

[230] No original: "and as the Internet erases the distance between countries, we see growing efforts by terrorists to poison the minds of people".

[231] No original: "Leading security experts are increasingly thinking about the war on terrorism as a kind of global counterinsurgency. What that means is that the center of gravity in this conflict is not just the terrorists themselves, but the populations they seek to influence and radicalize and in many cases, terrorize".

maiores margens de discricionariedade e a ampliação das capacidades das agências.

De maneira semelhante os tempos do Malleus, quando Papa Inocêncio VIII (2002, p. 44) afirmava a necessidade de remover os *obstáculos que dificultavam a tarefa dos inquisidores,* o presidente Bush argumentava sobre a necessidade de eliminar as travas burocráticas sobre os processos investigativos. Enfatizando o suposto aspecto de novidade e ameaça ao cenário da época (ligado à ideia da ameaça máxima do ponto iii), apela-se à necessidade de empregar meios extraordinários no seu combate. Como resumido por Cavelty (2007b, p. 28, tradução livre, ênfase no original), "a ameaça é frequentemente chamada de *nova* para indicar a incapacidade de estruturas e instrumentos estabelecidos para lidar com ela".[232] Este sentido, precisamente, era acionado pelo Presidente estadunidense que, no momento de promulgar a Lei Patriota em outubro de 2001, discursou que:

> O projeto perante mim leva em conta as novas realidades e perigos colocados pelos terroristas modernos […] Esta nova Lei que estou assinando hoje permitirá a vigilância de todas as comunicações utilizadas por terroristas, incluindo e-mails, Internet e telefones celulares. A partir de hoje, seremos capazes de enfrentar melhor os desafios tecnológicos que esta proliferação de tecnologias de comunicação representa"[233] (BUSH, 2005c, p. 1306–1307, tradução livre).

Como foi abordado no capítulo precedente, dentre outras medidas, a substituição do princípio de causa provável pelo de relevância na coleta de informações foi já prevista na Lei Patriota (EUA, 2001b, seç. 218), em conjunto com outras disposições que alteraram os procedimentos convencionais de investigação estadunidenses e as normas internacionais em matéria de Direitos Humanos e Direitos Civis e Políticos.

---

[232] No original: "the threat is frequently called new in order to indicate the inability of established structures and instruments to deal with it"

[233] No original: "The bill before me takes account of the new realities and dangers posed by modern terrorists […] This new law that I sign today will allow surveillance of all communications used by terrorists, including e-mails, the Internet, and cell phones. As of today, we'll be able to better meet the technological challenges posed by this proliferation of communications technology. "

Especificamente nesta linha se expressou o então Diretor da NSA quando, em audiência perante o Comitê sobre o Judiciário do Senado dos Estados Unidos, afirmava que:

> Obter uma ordem judiciária, baseada no requisito constitucional de exibir uma causa provável, retarda, e em alguns casos impede totalmente, os esforços do Governo para conduzir a vigilância das comunicações que acredita como significativa para a segurança nacional. Nesse sentido, frequentemente sacrificamos um processo detalhado e rigoroso, uma das nossas maiores vantagens em nosso esforço, para coletar inteligência estrangeira - a capacidade de acessar uma grande parte da infraestrutura de comunicações do mundo localizada em nossa própria nação[234] (ALEXANDER, 2006, p. 1, tradução livre).

Neste sentido, na já referida *Estratégia Nacional para proteger o ciberespaço*[235], aponta-se que a orientação era a de solicitar a cooperação dos operadores privados para conseguir gerar uma *visão sinóptica* da Internet. Em particular, no documento se argumenta que: "A falta de uma visão sinóptica da Internet frustra os esforços para desenvolver uma análise de ameaças da Internet e capacidades de indicação e de aviso"[236] (EUA, 2003, p. 21–23). Em consequência, salienta-se que o estabelecimento de um sistema nacional de resposta em matéria de cibersegurança ofereceria possibilidade de combinar análises de tipo *tático* com outras de tipo *estratégico* na avaliação de ciberataques. Neste sentido, argumenta-se que, enquanto o primeiro tipo é direcionado à avaliação de casos pontuais, o

[234] No original: "Obtaining a court order, based on the constitutionally required showing of probable cause, slows, and in some cases prevents altogether, the Government's efforts to conduct surveillance of communications it believes are significant to the national security. In that respect, we frequently sacrifice to detailed and rigorous process one of our greatest advantages in our effort to collect foreign intelligence- the ability to access a vast proportion of the world's communications infrastructure located in our own nation".

[235] No original: "The national strategy to secure cyberspace".

[236] No original: "The lack of a synoptic view of the Internet frustrates efforts to develop Internet threat analysis and indication and warning capabilities".

estratégico vincula-se a estudos compreensivos, focados na detecção de padrões e na produção de informação antecipatória.

A vinculação entre a lógica antecipatória que orienta o discurso do poder punitivo e a prática de uma vigilância massiva e global fica especialmente ilustrada, nos discursos analisados, em duas noções: na orientação a *unir os pontos* como ideal da ação pós 11 de setembro e na busca de *sinais de radicalização.*

Em particular, de maneira reiterada expressa-se a ideia de que os eventos acontecidos no 11 de setembro nos Estados Unidos poderiam ter sido evitados, caso as agências de segurança houvessem tido a capacidade de *unir os pontos.* Nos discursos analisados, esta recorrência começa a aparecer de forma expressiva no marco das críticas ao programa de vigilância, que se seguiram às denúncias realizadas pelo ex-analista da NSA à imprensa estadunidense nos finais de 2005. Neste sentido, o ex-Diretor da NSA assegurava que: "Se este programa estivesse em vigor antes do 11 de setembro, é minha opinião profissional que poderíamos ter detectado alguns dos agentes do Al Qaeda do 11 de setembro nos Estados Unidos e poderíamos tê-los identificado como tais".[237] No mesmo evento declarava que:

> O objetivo de tudo isso não é o de coletar toneladas de inteligência, mas o de detectar e prevenir ataques. A comunidade de inteligência não tem nem o tempo nem os recursos, nem a autoridade legal para ler as comunicações que não estão vinculadas à nossa proteção, nem a NSA tem a vontade de fazê-lo (HAYDEN, 2006, tradução livre).

Essa ideia de "conectar os pontos antes que os terroristas consigam atacar"[238] foi reiterada pelo presidente Bush (BUSH, 2010, p. 124, tradução livre) e também pelo presidente Obama. Este último, em particular, afirmava que: "Nosso governo falhou em conectar os pontos de uma forma que poderia ter impedido que um conhecido terrorista embarcasse em um avião

[237] No original: "Had this program been in effect prior to 9/11, it is my professional judgment that we would have detected some of the 9/11 Al Qaeda operatives in the United States, and we would have identified them as such."

[238] No original: "The 9/11 Commission made clear, in this era of new dangers, we must be able to connect the dots before the terrorists strike, so we can stop new attacks. And this NSA program is doing just that."

para [os Estados Unidos da] América”239 (OBAMA, 2013c, p. 8, tradução livre).

Seguindo o mesmo sentido da orientação pelo ideal disciplinar da intervenção antecipada, o dispositivo punitivo se volta à detecção de *sinais* sobre o possível comportamento futuro – neste caso, *sinais de radicalização*.

> Mas a tecnologia e a Internet aumentam sua frequência e, em alguns casos, de maneira letal. Hoje uma pessoa pode consumir propaganda odiosa, comprometer-se com uma agenda violenta e aprender como assassinar sem sair da sua casa. [...] a melhor maneira de prevenir o extremismo violento inspirado em jihadistas violentos é trabalhar em conjunto com a comunidade muçulmana americana – que de maneira consistente tem rejeitado o terrorismo – para identificar sinais de radicalização e nos associar com as agências de segurança para intervir quando um indivíduo está à deriva em direção à violência (OBAMA, 2013a, p. 17, tradução livre).

É neste marco que se expressa o sentido da vigilância massiva e global. A ação antecipatória contra uma ameaça máxima configurada por um inimigo hostil, de características difusas e voltada à exploração de vulnerabilidades, exige o reconhecimento de sinais para prever o futuro. É neste ponto que o poder punitivo, de maneira discricionária, atribui características concretas a esses sinais, transformando um conjunto populacional específico em alvo da sua ação declarada. Como manifesto nas apresentações da NSA (2008, 2009b), para a agência alguns desses sinais de periculosidade são identificados no receber ou enviar um determinado arquivo, usar criptografia ou fazer uma busca em uma linguagem diferente à região na qual se encontra o usuário.

As tecnologias de mineração de dados aparecem como uma forma intencionalmente objetiva de recortar o universo dos vigiados. Dentro desta racionalidade, indicadores e perfis

[239] No original “our Government failed to connect the dots in a way that would have prevented a known terrorist from boarding a plane for America”.

gerados de maneira automática possibilitam detectar o *bandido* dentre o palheiro dos dados, ao mesmo tempo em que as tendências nos dados oferecem sinais sobre os possíveis pontos a serem conectados.

> Minha missão, a missão da NSA e do Cibercomando, é defender o país. Essa é a nossa missão. E para isso precisamos de programas que não tivemos antes do 11 de setembro [...] para resolver o 11 de Setembro, precisávamos de algumas capacidades para ligar os pontos que não podíamos fazer antes do 11 de Setembro. E se você acha que gostaríamos de ouvir as chamadas telefônicas de todos e ler o e-mail de todos para conectar os pontos, como você faz isso? E a resposta é que não é lógico. Isso seria um desperdício de nossos recursos para chegar lá. E, da minha perspectiva, o que você precisa é de uma maneira de se concentrar no cara mau. E se você pensar nisso, é como olhar para uma dessas telas grandes, na verdade, como olhar para mil telas grandes, cada uma com um elemento de imagem, e você tem alguns bilhões de elementos de imagem lá. Encontre o elemento de imagem ruim. E, ao fazê-lo, você tem que ter uma metodologia para olhar para os elementos de imagem. Essa metodologia é usar algo que chamamos metadados. […] E um dos principais mal-entendidos para o povo americano é 'você está ouvindo nossos telefonemas', 'você está lendo nossos e-mails'. Isso não é verdade. O que estamos fazendo é coletando metadados para perseguir os maus que usam os mesmos dispositivos e os mesmos equipamentos que nós usamos. Eles se escondem entre nós para matar o nosso povo[240] (ALEXANDER, 2013a, p. 3, tradução livre).

[240] No original: "My mission, the mission of NSA and Cyber Command, is to defend this country. That's our mission. And in order to do that we need programs that we didn't have prior to 9/11[…] to solve 9/11 we needed some capabilities to connect the dots that we couldn't do prior to 9/11. And if you think that we would listen to

everybody's telephone calls and read everybody's email to connect the dots, how do you do that? And the answer is that's not logical. That would be a waste of our resources to get there. And from my perspective, what you need is a way to focus on the bad guy. […] And one of the key misunderstandings is, you're listening to our phone calls, you're reading our emails, for the American people. That's flat not true. What we're doing is we're collecting metadata to go after bad guys who use the same devices and the same equipment that we do. They hide amongst us to kill our people."

5 CONSIDERAÇÕES FINAIS

A presente pesquisa começou na pretensão de problematizar a articulação entre uma prática de vigilância massiva e global, que atenta contra o direito humano à privacidade e contra o princípio de soberania territorial, e uma série de pronunciamentos que a apresentam como uma ferramenta essencial na manutenção da segurança internacional.

Em consequência, a dissertação iniciou abordando essa questão desde a perspectiva dos estudos no âmbito da Segurança Internacional. No primeiro capítulo, detalharam-se os lineamentos centrais do marco analítico da securitização, tal como desenvolvido pelos teóricos da Escola de Copenhague. Um dos aportes centrais desse enfoque ao desenvolvimento do campo foi o de salientar que a articulação dos discursos em matéria de segurança internacional, longe de se constituir em simples avaliações sobre uma realidade observada de maneira objetiva, emerge como resultado de um processo político. Neste sentido, apresentou-se, no primeiro capítulo, o argumento dos autores de que se articula um discurso em torno da ideia da presença de uma ameaça, com o objetivo específico da legitimação de procedimentos que se apartam daquilo geralmente aceito, isto é, da quebra de normas no âmbito internacional.

Como abordado no final dessa primeira seção, os teóricos da securitização reconhecem que esses pronunciamentos seguem uma estrutura argumentativa específica que denominaram *narrativa securitizadora*. Suas características centrais foram explicitadas nessa seção e, resumidamente, colocam o foco na enunciação da necessidade de intervir de maneira urgente para neutralizar uma ameaça existencial, que configura uma situação emergencial. Nesse cenário, argumentam os autores da Escola de Copenhague, apela-se à necessidade de acionar meios extraordinários, legitimando um aumento nas margens de discricionariedade daquela autoridade identificada com o combate à ameaça.

O eixo desse primeiro capítulo, então, foi o de argumentar que essa narrativa nem é própria dos enunciados em matéria de segurança internacional, nem das caracterizações do

conflito no século XX ou século XXI. Pelo contrário, elas podem ser pensadas como expressões das regularidades próprias daquilo que Foucault conceituou como características do discurso do poder punitivo.

A introdução deste novo enfoque não implicou uma simples mudança terminológica sobre conceitos análogos. Ao invés, supôs uma mudança analítica, principalmente a respeito do que foi trabalhado pelos autores da securitização em relação à abordagem sobre a prática discursiva. Adotando as considerações de Foucault, a presente pesquisa se estruturou através da noção de que o discurso se orienta segundo uma lógica ligada às práticas para as quais remete, conformando com estas um dispositivo único.

Na caracterização do discurso do poder punitivo, seguiu-se a Zaffaroni, quem, dando seguimento à orientação da arqueologia discursiva aberta por Foucault, propôs que a primeira formulação condensada do discurso do poder punitivo está no Malleus Maleficarum, obra sob a qual se estruturou a prática inquisitorial medieval.

Na segunda seção do primeiro capítulo, elaborou-se uma descrição das características do discurso do poder punitivo, ao longo da qual procurou-se salientar os pontos de conexão dessas regularidades com aquilo que fora identificado como próprio da narrativa securitizadora. Enfatizou-se que, embora as diversas características desta última possam ser reconhecidas já no Malleus, o enfoque analítico do discurso do poder punitivo possibilita focar nas relações existentes entre os diversos componentes do relato e na sua articulação com as práticas concretas às quais este remete.

O capítulo culminou expondo aquilo que se considera a consequência política fundamental do dispositivo punitivo. A noção, tal como trabalhada por Foucault e Zaffaroni, consiste em que a maior capacidade de condicionamento social por trás deste dispositivo provém não tanto da intervenção repressiva sobre um conjunto restrito dos perigosos, enquadrados como objetivos declarados da ação repressiva, quanto da articulação de uma estrutura de monitoramento sob o conjunto da população.

Em consequência, o segundo capítulo teve começo com a descrição do funcionamento do sistema de vigilância massiva e global de comunicações. Na primeira seção, detalharam-se suas

bases de sustentação materiais (isto é econômicas e institucionais), assim com seus princípios de organização.

Em específico, o argumento central foi que, tal como provado pelos documentos secretos publicados pelo ex-agente de inteligência estadunidense Edward Snowden, os Estados Unidos estruturaram um esquema de coleta, análise e armazenamento de informações que circulam nas redes de computadores, de orientação massiva e em escala planetária.

Tal como ilustrado pela própria NSA, tal sistema se dirige a *saber tudo, coletar tudo e analisar tudo*, sendo esta estratégia declaradamente orientada a detectar padrões e indicadores que possibilitem *prever* o comportamento futuro e, assim, reprimir preventivamente.

Em outras palavras, esta seção buscou expor as características salientes do sistema de vigilância massiva de comunicações e a argumentar que este se orienta seguindo, precisamente, a racionalidade característica do dispositivo punitivo.

Isto deu espaço para o início da segunda seção do capítulo e final da presente dissertação. Nesta, apresentaram-se os resultados da análise sobre um conjunto de pronunciamentos oficiais dos Estados Unidos referidos à vigilância de comunicações, sob a base das categorias analíticas detalhadas no Primeiro capítulo. O argumento central desta seção e, por sua vez, o eixo central que articula a dissertação no todo, é que, embora tenha havido uma mudança em termos de conteúdo, a estrutura da narrativa configurada a partir dos documentos da amostra é idêntica a do Malleus Maleficarum.

Assim, como se vagando por um *museu de grandes novidades,* nesta seção final da dissertação enfatizou-se que se repetem idênticas considerações a respeito do ideal de castigar com antecedência e a respeito da necessidade de intervir de maneira urgente. Apesar da pretendida novidade do cenário contemporâneo, o inimigo apresenta as mesmas características com que a visão dos inquisidores caracterizavam a bruxas e demônios: ele é difuso e sua ação orientada à exploração de vulnerabilidades.

Assim, o objetivo da presente dissertação não foi o de estudar os discursos oficiais dos Estados Unidos à procura de imprecisões ou inexatidões em contraste com a documentação vazada. Também não foi o de focar especificamente nos

aspectos efetivamente novos do cenário contemporâneo, abertos pela emergência de novas tecnologias que possibilitam, na atualidade, fazer aquilo que era impensável cinco séculos atrás. Pelo contrário, o objetivo central foi o de focar nos elementos de continuidade, naquilo que une duas práticas que, intuitivamente, parecem tão diferentes como a inquisição medieval e a vigilância massiva e global de comunicações digitais. Essa continuidade se faz presente nos idênticos esquemas de racionalização que orientam a ação, com iguais consequências em termos de poder – pois, embora o discurso se oriente pelo ideal de prever o futuro, aquilo que tem consequências é o que está sendo feito no presente.

Como adverte Zaffaroni, o discurso do poder punitivo constitui uma ferramenta de verticalização social, de centralização das instâncias de tomada de decisão. Aquilo que no século XV operou como estratégia de reafirmação de uma autoridade papal questionada, no século XXI leva à concentração, nos Estados Unidos, de um conjunto crescente de informações sobre uma porção substancial da população global, avançando por cima do direito à privacidade e por cima do princípio de soberania territorial.

REFERÊNCIAS

BIBLIOGRAFIA

ARQUILLA, John; RONFELDT, David. **The emergence of noopolitik: toward an American information strategy.** Santa Monica, CA: Rand, 1999.

ASSANGE, Julian et al. **Criptopunks: la libertad y el futuro de internet**. Tradução Nicolás Lerner. Buenos Aires: Marea Editorial, 2013.

AUSTIN, John. **How to do things with words: [the William James lectures delivered at Harvard University in 1955]**. 2. ed., [repr.] ed. Cambridge, Mass: Harvard Univ. Press, 2009.

BAMFORD, James. **Every move you make**. Foreign Policy, n. 220, p. 56–63, 2016.

BATTELLE, John. **The search: how Google and its rivals rewrote the rules of business and transformed our culture**. Reprint ed. New York: Portfolio, 2006.

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Rio de Janeiro: Zahar, 2014.

BIGO, Didier. Globalized (in)security: the field and the ban-opticon. TSOUKALA, A.; BIGO, D. (Org.). . **Terror, insecurity and liberty: illiberal practices of liberal regimes after 9/11**. Routledge studies in liberty and security. London; New York: Routledge, 2008. p. 10–48.

BIGO, Didier; TSOUKALA, Anastassia. Understanding (in)security. BIGO, D.; TSOUKALA, A. (Org.).. Terror, insecurity and liberty: illiberal practices of liberal regimes after 9/11. Routledge studies in liberty and security. London; New York: Routledge, 2008. p. 1–9.

BIGO, Didier; TSOUKALA, Anastassia (Org.).**Terror, insecurity and liberty: illiberal practices of liberal regimes after 9/11**. London; New York: Routledge, 2008. (Routledge studies in liberty and security).

BONELLI, Laurent. “Hidden in plain sight”: intelligence, exception and suspicion after 11 September 2001.BIGO, D.; TSOUKALA, A. (Org.). . **Terror, insecurity and liberty: illiberal practices of liberal regimes after 9/11**. Routledge studies in liberty and security. London; New York: Routledge, 2008. p. 100–120.

BRUNO, Fernanda. **Mapas de crime: vigilância distribuída e participação na cibercultura**. E-compós Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação, v. 12, n. 2, Ago 2009. Disponível em: <www.compos.org.br/seer/index.php/e-compos/article/viewFile/409/352>. Acesso em: 12 dez 2016.

_____. **Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade**. Porto Alegre: Sulina, 2013.

_____. Surveillance and participation on Web 2.0.LYON, D.; HAGGERTY, K. D.; BALL, K. (Org.). . **Routledge handbook of surveillance studies**. Abingdon, Oxon□; New York: Routledge, 2012. p. 343–351.

BURKE, Anthony. **Beyond security, ethics and violence: war against the other.** Abingdon, Oxon, [England]; New York: Routledge, 2007.

BUZAI, Gustavo. **El ciberespacio desde la geografía. Nuevos espacios de vigilancia y control global**. Meridiano, Revista de Geografía, n. 1, 2012.

_____. **Fronteras en el ciberespacio: el nuevo mapa mundial visto desde Buenos Aires (Argentina)**. Revista Colombiana de Geografía, Cuadernos de Geografía. v. 23, n. 2, p. 85–92, Dez 2014.

BUZAN, Barry; HANSEN, Lene. **The evolution of international security studies**. Cambridge, UK; New York: Cambridge University Press, 2009.

BUZAN, Barry; WÆVER, Ole. **Macrosecuritisation and security constellations: reconsidering scale in securitisation theory**. Review of international studies, v. 35, n. 02, p. 253–276, 2009.

_____. **Regions and powers: the structure of international security**. New York: Cambridge University Press, 2003. v. 91.

BUZAN, Barry; WÆVER, Ole; DE WILDE, Jaap.**Security: a new framework for analysis**. Boulder: Lynne Rienner Publishers, 1998.

CAMPBELL, David. **Writing security: United States foreign policy and the politics of identity**. Minneapolis: University of Minnesota Press, 1992.

CAMPBELL, David et al. Performing security: The imaginative geographies of current US strategy. Political Geography, v. 26, n. 4, p. 405–422, Maio 2007.

CAVELTY, Myriam Dunn. **Cyber-security and threat politics: US efforts to secure the information age**. [S.l.]: Routledge, 2007a.

_____. **Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate**. Journal of Information Technology & Politics, v. 4, n. 1, p. 19–36, 2007b.

CHRISTOFOLETTI, Rogério. **Privacidade e Regulamentação do Marco Civil da Internet: registros e preocupações.** Revista ECO-Pós, v. 18, n. 3, p. 213–229, 2015.

COGBURN, Derrick L. The Multiple Logics of Post-Snowden Restructuring of Internet Governance.MUSIANI, F. et al. (Org.). . **The Turn to Infrastructure in Internet Governance**.New York: Palgrave Macmillan US, 2016. p. 25–46.

COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE (CEPAL). **Estado de la Banda Ancha en América Latina y el Caribe, 2012**. . Santiago de Chile: Naciones Unidas, 2012.

DE ANDRADE, Vera Regina Pereira. **Por que a Criminologia (e qual Criminologia) e importante no Ensino Jurídico?** Unisul de Fato e de Direito: revista jurídica da Universidade do Sul de Santa Catarina, v. 3, n. 6, p. 179–183, 2013.

DE MONTE, Lambertus; OCHSENFURT, Andreas; DE SCOTIA, Thomas. Certificado oficial de aprovação do tratado Malleus Maleficarum. **O Martelo das feiticeiras: malleus maleficarum**. Tradução Paulo Fróes. Rio de Janeiro: Rosa dos Tempos, 2002. p. 518–524.

DENARDIS, Laura. **Hidden levers of Internet control: An infrastructure-based theory of Internet governance**. Information, Communication & Society, v. 15, n. 5, p. 720–738, Jun 2012.

_____. **Internet points of control as global governance**. , Internet Governance Papers., nº 2. Canada: The Centre for International Governance Innovation, 2013.

DENARDIS, Laura; MUSIANI, Francesca. Governance by Infrastructure.MUSIANI, F. et al. (Org.). . **The Turn to Infrastructure in Internet Governance**. New York: Palgrave Macmillan US, 2016. p. 3–21.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

_____. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico: Journal of Law [EJJL], v. 12, n. 2, p. 91–108, 2011.

EISSA, Gabriel Sergio et al. El ciberespacio y sus implicancias en la defensa nacional. In: VI CONGRESO DE RELACIONES INTERNACIONALES, 2012, La Plata. Anais... La Plata: [s.n.], 2012. Disponível em:

<http://sedici.unlp.edu.ar/bitstream/handle/10915/40210/Documento_completo.pdf?sequence=1>. Acesso em: 15 jun 2015.

FAIRCLOUGH, Norman. **Analysing discourse: textual analysis for social research**.London; New York: Routledge, 2003.

FINLEY, Laura; ESPOSITO, Luigi.**"Digital Blackwater": The National Security Administration, Telecommunications Companies and State-Corporate Crime**. State Crime Journal, v. 3, n. 2, p. 182–199, Out 2014.

FOUCAULT, Michel. **A arqueologia do saber**. Tradução Luiz Felipe Baeta Neves. 3ª ed. Rio de Janeiro: Forense Universitária, 1987.

_____. **A evolução da noção de "indivíduo perigoso" na psiquiatria legal do século XIX**. Ditos e escritos, v. 5, p. 1–25, 2004.

_____. **El gobierno de sí y de los otros: curso en el College de France (1982-1983)**. Tradução Horacio Pons. Buenos Aires: Fondo de Cultura Económica, 2009.

_____. **El poder psiquiátrico: curso en el Collège de France (1973-1974)**. Buenos Aires: Fondo de Cultura Económica, 2005.

_____. **Microfísica do poder, trad**. Las ediciones de La Piqueta, Madrid, 1979.

_____. **Nascimento da Biopolítica: curso dado no Collège de France (1977-1978)**. Tradução Eduardo Brandão; Claudia Berliner. 1ª ed. São Paulo: Martins Fontes, 2008.

_____. **Vigilar y castigar: nacimiento de la prisión**. 1a Reimp. ed. Buenos Aires: Siglo Veintiuno Editores S.A., 1983.

FUCHS, Christian. **Power in the Age of Social Media**. Heathwood Journal of Critical Theory, v. 1, n. 1, p. 1–29, Set 2015a.

_____. Social media surveillance. COLEMAN, S.; FREELON, D. (Org.). . **Handbook of digital politics**. Cheltenham, UK; Northampton, MA, USA: Edward Elgar Publishing, 2015b. p. 395–414.

_____. **The political economy of privacy on Facebook**. Television & New Media, v. 13, n. 2, p. 139–159, 2012.

FUCHS, Christian; TROTTIER, Daniel. **Towards a theoretical model of social media surveillance in contemporary society**. Communications, v. 40, n. 1, 1 Jan 2015.Disponível em: <http://www.degruyter.com/view/j/comm.2015.40.issue-1/commun-2014-0029/commun-2014-0029.xml>. Acesso em: 30 nov 2015.

GÓMEZ, Santiago Miguel. **El alcance de las palabras**. Buenos Aires: [s.n.], 2016. Disponível em: <http://observatorio-riqueza.org/wp-content/uploads/sites/15/2016/09/Ensayo_-El-alcance-de-las-palabras-Observatorio.pdf>. Acesso em: 30 out 2016.

_____. ¿Poder de qué? De hacer nombrar. **La Criminología Mediática**, 2012. Disponível em: <http://lacriminologiamediatica.blogspot.com.br/2012/10/poder-de-que-de-hacer-nombrar.html>. Acesso em: 20 jul 2015.

GREENWALD, Glenn. **Sem Lugar Para Se Esconder - Edward Snowden, A Nsa e A Espionagem do Governo Americano**. Tradução Fernanda Abreu. Rio de Janeiro: Sextante, 2014. (Primeira Pessoa).

HANSEN, Lene; NISSENBAUM, Helen. **Digital disaster, cyber security, and the Copenhagen School**. International Studies Quarterly, v. 53, n. 4, p. 1155–1175, 2009.

HARDING, Luke. **Os arquivos Snowden: a história secreta do homem mais procurado do mundo**. Tradução Alice Klesck; Bruno Correia. Rio de Janeiro: LeYa, 2014.

HUYSMANS, Jef. Agency and the politics of protection.Implications for security studies. HUYSMANS, J.;

DOBSON, A.; PROKHOVNIK, R. (Org.). . **The Politics of protection: sites of insecurity and political agency**. Routledge advances in international relations and global politics. London: Routledge, 2009. p. 1–18.

IGREJA CATÓLICA. **Código de direito canónico: promulgado por S.S. o Papa João Paulo II**. Tradução António Leite. Lisboa; Braga: Conferência Episcopal Portuguesa; Editorial Apostolado da Oração, 1995.

INOCÊNCIO VIII. Bula Summis desiderantes affectibus. **O Martelo das feiticeiras: malleus maleficarum**. Tradução Paulo Fróes. Rio de Janeiro: Rosa dos Tempos, 2002. p. 43–46.

KRAMER, Heinrich; SPRENGER, Jacob. **O Martelo das feiticeiras: malleus maleficarum**. Tradução Paulo Fróes. Rio de Janeiro: Rosa dos Tempos, 2002.

KUROSE, James F; ROSS, Keith W. **Computer Networking: A Top-Down Approach Featuring the Internet, 3/E**. 6. ed. New Jersey: Pearson Education India, 2005.

LACAZE, Laura. Convergencia digital y dependencia. In: II CONGRESO DE PENSAMIENTO ECONÓMICO LATINOAMERICANO, 27 Out 2016a, Cochabamba, Bolivia. Anais... Cochabamba, Bolivia: [s.n.], 27 Out 2016.

LAFER, Celso. **A reconstrução dos direitos humanos: a contribuição de Hannah Arendt**. Estudos Avançados, v. 11, n. 30, p. 55–65, Ago 1997.

LEFÉBURE, Antoine. **El caso Snowden: así espía Estados Unidos al mundo**. 1. ed. Buenos Aires: Capital Intelectual, 2014.

LIBICKI, Martin C. **Information War, Information Peace.** Journal of International Affairs, 411, v. 51, n. 2, p. 411, 1998.

LILES, Samuel. Cyber warfare: As a form of low–intensity conflict and insurgency. In: CONFERENCE ON CYBER CONFLICT PROCEEDINGS, 2010, Estonia. Anais... Estonia: CCD COE Publications, 2010. p. 47–58. Disponível em:

<https://ccdcoe.org/sites/default/files/multimedia/pdf/Liles%20-%20Cyber%20warfare%20%20As%20a%20form%20of%20low-intensity%20conflict%20and%20insurgency.pdf>. Acesso em: 3 maio 2015.

LYON, David. **Surveillance studies: an overview**. Repr ed. Cambridge: Polity Press, 2007.

MACHADO, Joana de Moraes Souza. **A Expansão do Conceito de Privacidade e a Evolução na Tecnologia de Informação com o Surgimento dos Bancos de Dados**. Revista da AJURIS, v. 41, n. 134, 2014.

MCDONALD, M. **Securitization and the Construction of Security**.European Journal of International Relations, v. 14, n. 4, p. 563–587, 1 Dez 2008.

KATZ, Raúl. **El ecosistema y la economía digital en América Latina**. Madrid; Barcelona: Fundación Telefónica; Ariel, 2015.

NYE, Joseph S Jr. **Cyber power.** Cambridge, 2010. Disponível em: <http://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf>. Acesso em: 23 maio 2015.

OLSSON, Christian. Military interventions and the concept of the political: bringing the political back into the interactions between external forces and local societies. BIGO, D.; TSOUKALA, A. (Org.). . **Terror, insecurity and liberty: illiberal practices of liberal regimes after 9/11**. Routledge studies in liberty and security. London; New York: Routledge, 2008. . POITRAS, Laura. **Citizenfour**. . [S.l: s.n.]. Disponível em: <https://citizenfourfilm.com/>. Acesso em: 30 out 2016. , 2014

PILATI, José Isaac; VIEIRA CANCELIER DE OLIVO, Mikhail. **Um novo olhar sobre o Direito à privacidade: Caso Snowden e Pós-modernidade jurídica**. Seqüência: Estudos Jurídicos e Políticos, v. 35, n. 69, p. 281, 17 Dez 2014.
ROSA, Daniel Aidar Da. **A demonomania harmônica: Jean Bodin, a bruxaria e a república**. 2013. Dissertação de Mestrado (Programa de Pós-Graduação em História Social da faculdade de

Filosofia, Letras e Ciências Humanas) – Universidade de São Paulo, 2013.

SAINT-PIERRE, Héctor Luis. 11 de Setembro: do terror à injustificada arbitrariedade e o terrorismo de Estado. Revista de Sociologia e Política, v. 23, n. 53, p. 9–26, Mar 2015.

_____. **“ Defesa” ou“ Segurança”? Reflexões em torno de Conceitos e Ideologias.** Contexto Internacional, v. 33, n. 2, 2011.

_____. **A política armada: fundamentos da guerra revolucionária.** São Paulo: Editora UNESP, 2000.

SILVERMAN, David. **Interpreting qualitative data: methods for analyzing talk, text, and interaction**.3rd ed ed. London; Thousand Oaks, Calif: SAGE Publications, 2006.

SCHMIDT, Eric; COHEN, Jared. **A nova era digital**. Tradução Ana Beatriz Rodrigues; Rogério Durst. 1. ed. Rio de Janeiro: Intrínseca, 2013.

SCHMITT, Carl. **El concepto de lo político: texto de 1932 con un prólogo y tres corolarios**. Tradução Rafael Agapito. Madrid: Alianza Editorial, 1998.

TSOUKALA, Anastassia. Defining the terrorist threat in the post-September 11 era.TSOUKALA, A.; BIGO, D. (Org.). . **Terror, insecurity and liberty: illiberal practices of liberal regimes after 9/11**. Routledge studies in liberty and security. London; New York: Routledge, 2008. p. 49–99.

TSOUKALA, Anastassia; BIGO, Didier. Understanding (in)security. BIGO, D.; TSOUKALA, A. (Org.).. **Terror, insecurity and liberty: illiberal practices of liberal regimes after 9/11**. Routledge studies in liberty and security. London; New York: Routledge, 2008. p. 1–9.

WÆVER, Ole. Securitization and Desecuritization. LIPSCHUTZ, R. D. (Org.). . **On Security**. Columbia: Columbia University Press, 1995. p. 46–87.

_____. **Security, the Speech Act**. manuscrito inédito: [s.n.], 1988. Disponível em: <http://www.academia.edu/2237994/Security_the_Speech_Act_-_working_paper_1989>. Acesso em: 5 mar 2016.

WALT, Stephen M. **The renaissance of security studies**. International Studies Quarterly, v. 35, n. 2, p. 211–239, 1991.

ZAFFARONI, Eugenio Raúl. **A questão criminal.** Tradução Sergio Lamarão. 1a.ed. Rio de Janeiro: Revan, 2013a.

_____. **El Enemigo en el Derecho Penal**. Buenos Aires: Ediar, 2006.

_____. **Friedrich Spee. El padre de la criminología crítica**. manuscrito inédito ed. [S.l: s.n.], 2016.

_____. **La cuestión criminal**. 5. ed ed. Buenos Aires: Planeta, 2013b.

_____. **La palabra de los muertos: conferencias de criminología cautelar**. 1. reimpr ed. Buenos Aires: Ediar, 2011a.

_____. **Nos cuidamos del ladrón y no nos damos cuenta de la violencia que crece en nuestra familia**. 29 Dez 2011b. Disponível em: <http://www.clarin.com/rn/ideas/Zaffaroni-_-Nos_cuidamos_del_ladron_y_no_nos_damos_cuenta_de_la_violencia_que_crece_en_nuestra_familia_0_617938445.html>. Acesso em: 24 jul 2015.

ŽIŽEK, Slavoj.**Edward Snowden, Chelsea Manning and Julian Assange: our new heroes.** The Guardian, Londres, 3 Set 2013. Disponível em: <http://www.theguardian.com/commentisfree/2013/sep/03/snowden-manning-assange-new-heroes>. Acesso em: 21 jul 2015.

REFERÊNCIAS JORNALÍSTICAS

ASSANGE, Julian; VIANA, Natalia. **EUA espionaram ministros de Dilma e o avião presidencial**. Carta Capital, 4 Jul 2015. Disponível em: <http://www.cartacapital.com.br/revista/857/os-alvos-do-tio-sam-9756.html>. Acesso em: 26 set 2016.

BALL, James. **NSA monitored calls of 35 world leaders after US official handed over contacts**. The Guardian, 25 Out 2013.US news Disponível em: <https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls>. Acesso em: 27 set 2016.

CURRIER, Cora. **Despite Anti-Profiling Rules, the FBI Uses Race and Religion When Deciding Who to Target.** The Intercept, New York, 31 Jan 2017. Disponível em: <https://theintercept.com/2017/01/31/despite-anti-profiling-rules-the-fbi-uses-race-and-religion-when-deciding-who-to-target/>. Acesso em: 18 fev 2017.

ELLIOTT, Justin. Claim on “Attacks Thwarted” by NSA Spreads Despite Lack of Evidence. **Propublica**, New York, 23 Out 2013. Disponível em: <https://www.propublica.org/article/claim-on-attacks-thwarted-by-nsa-spreads-despite-lack-of-evidence>. Acesso em: 12 dez 2016.

EMARKETER. Number of social network users worldwide from 2010 to 2020 (in billions). **Statista**, Jun 2016. Disponível em: <http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>. Acesso em: 16 set 2016.

GORMAN, Siobhan; VALENTINO-DEVRIES, Jennifer. **New Details Show Broader NSA Surveillance Reach**. Wall Street Journal, 21 Ago 2013.USDisponível em: <http://www.wsj.com/articles/SB10001424127887324108204579022874091732470>. Acesso em: 29 set 2016.

GREENWALD, Glenn. **NSA collecting phone records of millions of Verizon customers daily**. The Guardian, 6 Jun 2013. US news Disponível em: <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>. Acesso em: 17 nov 2015.

_____. **The Intercept is broadening access to the Snowden archive. Here's why.** The Intercept, New York, 16 Maio 2016. Disponível em: <https://theintercept.com/2016/05/16/the-intercept-is-broadening-access-to-the-snowden-archive-heres-why/>. Acesso em: 20 set 2016.

GREENWALD, Glenn; BALL, James; BORGER, Julian.**Revealed: how US and UK spy agencies defeat internet privacy and security**. The Guardian, 6 Set 2013. US news Disponível em: <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>. Acesso em: 23 set 2016.

GREENWALD, Glenn; MACASKILL, Ewen. **Boundless Informant: the NSA's secret tool to track global surveillance data**. The Guardian, 11 Jun 2013. US newsDisponível em: <https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining>. Acesso em: 23 set 2016.

GREENWALD, Glenn; MACASKILL, Ewen; POITRAS, Laura. **Edward Snowden: the whistleblower behind the NSA surveillance revelations.** The Guardian, 11 Jun 2013. US news Disponível em: <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance>. Acesso em: 1 out 2016.

LACAZE, Laura. Estados Unidos: el FBI va a la Justicia contra Apple. **Agencia Paco Urondo**, Ciudad Autónoma de Buenos Aires, 2 Mar 2016b.Disponível em: <http://agenciapacourondo.com.ar/sociedad/18755-estados-unidos-el-fbi-va-a-la-justicia-contra-apple>. Acesso em: 12 mar 2016.

LARSON, Nicole Perlroth, Jeff; SHANE, Scott. **N.S.A. Able to Foil Basic Safeguards of Privacy on Web**. The New York Times, 5 Set 2013. Disponível em: <http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html>. Acesso em: 23 set 2016.MARQUIS-BOIRE, Morgan; GREENWALD, Glenn; LEE, Micah. **XKEYSCORE: NSA's Google for the World's Private Communications**. The

Intercept, 1 Jul 2015. Disponível em: <https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/>.

POITRAS, Laura; ROSENBACH, Marcel; STARK, Holger. **“Follow the Money”: NSA Monitors Financial World. Part 1**.SPIEGEL ONLINE, Hamburg, 16 Set 2013.Disponível em: <http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html>. Acesso em: 29 set 2016

RICHTER, Felix. The Smartphone Platform War Is Over. **Statista**, 22 Ago 2016. Disponível em: <https://www.statista.com/chart/4112/smartphone-platform-market-share/>. Acesso em: 9 fev 2016.

SPIEGEL.**“Follow the Money”: NSA Spies on International Payments**. Spiegel Online, 15 Set 2013. InternationalDisponível em: <http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html>. Acesso em: 26 out 2015.

SPIELBERG, Steven. **Sentencia previa**. . [S.l: s.n.]. , 2002

STATISTA. Worldwide desktop market share of leading search engines from January 2010 to July 2016.2016.Disponível em: <https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/>. Acesso em: 30 set 2016.

STONE, Oliver. **Snowden**. . [S.l: s.n.]. Disponível em: <https://snohttps://snowdenfilm.com/wdenfilm.com/>. Acesso em: 15 jan 2017. , 2016

TELEGEOGRAPHY. **Executive Summary**. . Washington, D.C.: TeleGeography, 2016.

THE CONSTITUTION PROJECT. **Principles for Government Data Mining: Preserving Civil Liberties in the Information Age**. . Washington, D.C.: The Constitution Project, 7 Dez 2010. Disponível em: <http://www.constitutionproject.org/documents/principles-for-

government-data-mining-preserving-civil-liberties-in-the-information-age/>.

THE INTERCEPT. **How we prepared the nsa`s sensitive internal reports for release.** The Intercept, New York, 16 Maio 2016. Disponível em: <https://theintercept.com/2016/05/16/how-we-prepared-the-nsas-sensitive-internal-reports-for-release/> . Acesso em: 20 set 2016.

TOOMEY, Patrick; YACHOT, Noa. Why Today's Landmark Court Victory Against Mass Surveillance Matters. **American Civil Liberties Union**, 7 Maio 2015. Disponível em: <https://www.aclu.org/blog/speak-freely/why-todays-landmark-court-victory-against-mass-surveillance-matters>. Acesso em: 27 jan 2016.

WIKILEAKS. **Bugging Brazil**. Disponível em: <https://wikileaks.org/nsa-brazil/>. Acesso em: 26 set 2016a.

_____. **Espionnage Élysée**. Disponível em: <https://wikileaks.org/nsa-france/>. Acesso em: 26 set 2016b.

_____. **NSA Helped CIA Outmanoeuvre Europe on Torture**. Disponível em: <https://wikileaks.org/nsa-germany/>. Acesso em: 26 set 2016c.

_____. **NSA Targets World Leaders for US Geopolitical Interests: United Nations**. Disponível em: <https://wikileaks.org/nsa-201602/>. Acesso em: 26 set 2016.

_____. **Target Tokyo**. Disponível em: <https://wikileaks.org/nsa-japan/>. Acesso em: 26 set 2016d.

_____. **What is WikiLeaks**. Disponível em: <https://wikileaks.org/What-is-Wikileaks.html>. Acesso em: 26 set 2016e.

DOCUMENTOS

ADOBE SYSTEMS INCORPORATED. **What is PDF?** Disponível em: <https://acrobat.adobe.com/us/en/why-adobe/about-adobe-pdf.html>. Acesso em: 20 dez. 2016.

AGÊNCIA FEDERAL DE INVESTIGAÇÃO (FBI). **FBI Director Comments on San Bernardino Matter**. Declarações do Diretor do FBI. Washington D. C.: FBI National Press Office, 21 Fev 2016. Disponível em: <https://www.fbi.gov/news/pressrel/press-releases/fbi-director-comments-on-san-bernardino-matter>.

_____. **Guidance on the use of race, ethnicity, gender, national origin, religion, sexual orientation, or genden identity in assessments and predicated investigations.** 3 Mar 2016. Disponível em: <https://assets.documentcloud.org/documents/3423235/DIOG-Profiling-Rules-2016.pdf>. Acesso em: 25 fev 2017.

ALEXANDER, Keith. Clear and Present Danger: Cyber-Crime; Cyber-Espionage; Cyber-Terror; and Cyber-War. In: ASPEN SECURITY FORUM, 18 Jul 2013a, Press department. Disponível em: <https://www.nsa.gov/public_info/_files/speeches_testimonies/GEN_A_Aspen_Security_Forum_Transcript_18_Jul_2013.pdf>. Acesso em: 6 abr 2016.

_____. General Keith Alexander Speaks at AFCEA's Conference. In: AFCEA'S CONFERENCE, 28 Jun 2013b, Press department. Disponível em: <https://www.nsa.gov/public_info/_files/speeches_testimonies/Transcript_of_GEN_Alexanders_AFCEA_Keynote_Speech_27_June_2013.pdf>. Acesso em: 6 abr 2016.

_____. Statement for the Record of LT GEN Keith B. Alexander Director, National Security Agency before the Committee on the Judiciary United States Senate. In: COMMITTEE ON THE JUDICIARY UNITED STATES SENATE, 26 Jul 2006, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/testimonies/26july06-dirnsa.shtml>. Acesso em: 20 abr 2016.

_____. Statement for the Record Lieutenant General Keith Alexander Commander Joint Functional Component Command for Network Warfare Before the House Armed Services Committee Terrorism, Unconventional Threats, and Capabilities Subcommittee. In: HOUSE ARMED SERVICES COMMITTEE TERRORISM, UNCONVENTIONAL THREATS, AND CAPABILITIES SUBCOMMITTEE, 5 Maio 2009a, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/testimonies/alexander-statement-5may09.shtml>. Acesso em: 11 abr 2016.

_____. The Director of the National Security Agency (NSA) and Chief of the Central Security Service (CSS) briefed on “Securing Our Government Networks”. In: RSA SECURITY CONFERENCE, 22 Abr 2009b, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/21apr09-dir.shtm>. Acesso em: 12 abr 2016.

BOLÍVIA, Estado Plurinacional De. **Bolivia denuncia “secuestro” de su Presidente y violación de Convención de Viena**. Institucional. Disponível em: <http://comunicacion.presidencia.gob.bo/noticias/noticia.php?id=975>. Acesso em: 9 mar 2016.

BRASIL, República Federativa De. **Doutrina Militar de Defesa**. , nº Doutrina Militar de Defesa. Brasília: Secretaria de Política, Estratégia e Assuntos Internacionais do Ministério da Defesa, 2007. Disponível em: <http://www.arqanalagoa.ufscar.br/pdf/doutrina_militar_de_defesa.pdf>. Acesso em: 20 dez 2015.

_____. 12965. , de23 junho 2014. **Marco Civil da Internet**. , 23 Jun 2014.

_____. Visita oficial aos Estados Unidos será adiada. **Blog do Planalto - Presidencia da República**, 17 Set 2013. Disponível em: <http://blog.planalto.gov.br/visita-oficial-aos-estados-unidos-sera-adiada/>. Acesso em: 16 nov 2015.

BUSH, Jorge W. Address Before a Joint Session of the Congress on the United States Response to the Terrorist Attacks of September 11 (25/09/2001). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2001)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2005a. p. 1140–1143. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2001-book2/pdf/PPP-2001-book2.pdf>.

_____. Remarks at Boston Latin School in Boston, Massachusetts (08/01/2002). **George W. Bush (book I — january 1 to june 30, 2002)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2005b. p. 30–33. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2002-book1/pdf/PPP-2002-book1.pdf>.

_____. Remarks at the Federal Bureau of Investigation Academy in Quantico Virginia (10/09/2003). **George W. Bush (book II — july 1 to december 31, 2003)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2006. p. 1133–1139. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2.pdf>.

_____. Remarks at the National Hispanic Prayer Breakfast (30/06/2006). **George W. Bush (book I — january 1 to june 30, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010a. p. 1225–1230. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book1/pdf/PPP-2006-book1.pdf>.

_____. Remarks at the Port of Charleston, South Carolina (05/02/2004). **George W. Bush (book I — january 1 to june 30, 2004)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007a. p. 184–189. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2004-book1/pdf/PPP-2004-book1.pdf>.

_____. Remarks in Hershey, Pennsylvania (19/04/2004). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2004)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007b. p. 603–611. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2004-book1/pdf/PPP-2004-book1.pdf>.

_____. Remarks in Miami 27/08/2004. **George W. Bush (book II — july 1 to december 31, 2004)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007c. p. 1756–1763. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2004-book2/pdf/PPP-2004-book2.pdf>.

_____. Remarks in Nashville, Tennessee (01/02/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010b. p. 154–168. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book1/pdf/PPP-2006-book1.pdf>.

_____. Remarks on Intelligence Reform Legislation (09/07/2008). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to June 30, 2008)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2012. p. 1007.Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2001-book2/pdf/PPP-2008-book1.pdf>.

_____. Remarks on Signing the USA PATRIOT ACT of 2001 (26/10/2001). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2001)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2005c. p. 1036–1037. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2001-book2/pdf/PPP-2001-book2.pdf>.

_____. Remarks on the Anniversary of the United States Department of Homeland Security (02/03/2004). ESTADOS

UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2004)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007d. p. 291–295. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2004-book1/pdf/PPP-2004-book1.pdf>.

_____. Remarks to Department of Homeland Security Employees (28/03/2003). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . George W. Bush (book I — january 1 to june 30, 2003). Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2006b. p. 226–229. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2003-book1/pdf/PPP-2003-book1.pdf>.

_____. Remarks on the War on Terror and a Question-and-Answer Session in Louisville, Kentucky (11/01/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010c. p. 41–58. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book1/pdf/PPP-2006-book1.pdf>.

_____. Remarks to Reporters Following a Visit With United States Troops and an Exchange With Reporters in San Antonio, Texas (01/01/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010d. p. 1–3. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book1/pdf/PPP-2006-book1.pdf>.

_____. Remarks to the City Club of Cleveland and a Question-and-Answer Session in Cleveland, Ohio (20/03/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010e. p. 504–520. Disponível em:

<https://www.gpo.gov/fdsys/pkg/PPP-2006-book1/pdf/PPP-2006-book1.pdf>.

_____. Remarks to the Veterans of Foreign Wars National Convention in Salt Lake City, Utah (22/08/2005). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2005)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007e. p. 1336–1341. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2005-book2/pdf/PPP-2005-book2.pdf>.

_____. The President's News Conference (19/12/2005). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2005)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007f. p. 1875–1888. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2005-book2/pdf/PPP-2005-book2.pdf>.

_____. The President's Radio Address (27/10/2001). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2001).** Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2005d. p. 1312–1314. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2001-book2/pdf/PPP-2001-book2.pdf>.

_____. The President's Radio Address (17/04/2004). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2004)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007g. p. 600–601. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2004-book1/pdf/PPP-2004-book1.pdf>.

CENTRE FOR THE PROTECTION OF NATIONAL INFRAESTRUCTURE (CPNI). **My digital footprint: a brief guide**. 2015. Disponível em: <https://www.cpni.gov.uk/Documents/Publications/2015/Digital%2

0Footprint/09_My%20Digital%20Footprint%20-%20a%20brief%20guide%20FINAL.pdf>.

CLINTON, Hillary. Conference on Internet Freedom. In: FOKKER TERMINAL, 8 Dez 2011a, Press department. Disponível em: <http://www.state.gov/secretary/20092013clinton/rm/2011/12/178511.htm>. Acesso em: 4 abr 2016.

_____. Internet Rights and Wrongs: Choices & Challenges in a Networked World. 15 Fev 2011b, Disponível em: <http://www.state.gov/secretary/20092013clinton/rm/2011/02/156619.htm>. Acesso em: 5 abr 2016.

CLINTON, Hillary; PANETTA, Leon.**A Conversation with Secretaries Hillary Clinton and Leon Panetta**.Washington D.C, 16 Ago 2011.Disponível em: <http://www.state.gov/secretary/20092013clinton/rm/2011/08/170611.htm>. Acesso em: 11 abr 2016.

EMMERSON, Ben. **Promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo**. Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, nº A/69/397. New York: Nações Unidas, 23 Set 2014.

ESTADOS UNIDOS DA AMÉRICA (EUA). **A Warfighting Domain**. Washington D.C., 26 Set 2006. Disponível em: <http://www.au.af.mil/info-ops/usaf/cyberspace_taskforce_sep06.pdf>. Acesso em: 14 jul 2015.

_____. **Cyber Strategy**. Institucional. Disponível em: <http://www.defense.gov/home/features/2015/0415_cyber-strategy/>. Acesso em: 23 jul 2015.

_____. **Department of Defense Cyberspace Policy Report. A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934**. . Washington, D.C.: Department of Defense, Nov 2011a.

Disponível em: <https://fas.org/irp/eprint/dod-cyber.pdf>. Acesso em: 12 dez 2016.

_____. **Department of defense strategy for operating in Cyberspace**. . Washington D. C.: Department of Defense, 2011b.

_____. **Fact Sheet: Retroactive liability protection is critical to our National Security**. Disponível em: <https://www.justice.gov/archive/ll/docs/fisa-factsheet-070808.pdf>. Acesso em: 16 jan 2017a.

_____. **Fact sheet: Retroactive Liability Protection: Providing OurIntelligence Officials The Tools They Need To Keep Our Nation Safe**. Disponível em: <https://www.justice.gov/archive/ll/docs/fisawhfactsheet.pdf>. Acesso em: 16 jan 2017b.

_____. 110–261., de 10 julho 2008 c. **Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008**.Washington D.C., 10 Jul 2008, p. 44. Disponível em: <https://www.congress.gov/110/plaws/publ261/PLAW-110publ261.pdf>. Acesso em: 11 abr 2016.

_____. 29 outubro 2001 a. **Homeland Security Presidential Directive–1—Organization and Operation of the Homeland Security Council**. , 29 Out 2001. Disponível em: <https://georgewbush-whitehouse.archives.gov/news/releases/2001/10/20011030-1.html>. Acesso em: 30 set 2016.

_____. PPD-28. , de17 janeiro 2014. **Presidential Policy Directive - Signals Intelligence Activities.** Washington D.C., 17 Jan 2014. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201400031/pdf/DCPD-201400031.pdf>. Acesso em: 11 abr 2016.

_____. 110–55.,de 5 agosto 2007. **Protect America Act of 2007**. **Aug. 3, considered and passed Senate. Aug. 4, considered and passed House.**, , 5 Ago 2007. Disponível em: <https://www.congress.gov/110/plaws/publ55/PLAW-110publ55.pdf>.

_____. **The National Security Strategy of the United States of America.** Whashington, D. C., 17 Set 2002. Disponível em: <https://www.state.gov/documents/organization/63562.pdf>. Acesso em: 20 abr 2016.

_____. **The national strategy to secure cyberspace**. Washington, D.C., 2003. Disponível em: <https://georgewbush-whitehouse.archives.gov/pcipb/cyberspace_strategy.pdf>. Acesso em: 20 abr 2016.

_____. **Unclassified report on the President's surveillance program.**, no 2009–0013–AS. Washington, DC: [s.n.], 7 Out 2009.

_____. 107–56. , de26 outubro 2001 b. **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001**. Washington D.C., 26 Out 2001, p. 132. Disponível em: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf>. Acesso em: 2 jun 2015.

GOVERNMENT COMMUNICATIONS HEADQUARTERS (GCHQ). BULLRUN. 28 Dez 2014, Disponível em: <https://search.edwardsnowden.com/docs/BULLRUN2014-12-28nsadocs>. Acesso em: 27 set 2016.

HAYDEN, Michael. Statement For The Record Before The Governmental Affairs Subcommittee On International Security, Proliferation, And Federal Services Hearing On Critical Skills For National Security And The Homeland Security Federal Workforce Act. In: THE GOVERNMENTAL AFFAIRS SUBCOMMITTEE ON INTERNATIONAL SECURITY, PROLIFERATION, AND FEDERAL SERVICES HEARING ON CRITICAL SKILLS FOR NATIONAL SECURITY AND THE HOMELAND SECURITY FEDERAL WORKFORCE ACT, 12 Mar 2002, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/testimonies/12mar02.shtml>. Acesso em: 6 abr 2016.

_____. What american intelligence and especialy the NSA have been doing to defend the nation. In: THE NATIONAL PRESS

CLUB, 23 Jan 2006, Disponível em: <https://fas.org/irp/news/2006/01/hayden012306.html>. Acesso em: 12 dez 2016.

KERRY, John. **Interview With Charlie Rose and Norah O'Donnell of CBS**. Washington, D.C., 28 Maio 2014. Disponível em: <https://2009-2017.state.gov/secretary/remarks/2014/05/226578.htm>.

_____. **Interview With Elise Labott of CNN**. Washington D.C., 24 Jun 2013. Disponível em: <http://www.state.gov/secretary/remarks/2013/06/211089.htm>. Acesso em: 12 abr 2016.

NATIONAL SECURITY AGENCY (NSA). Boundless Informant.Describing mission capabilities from Metadata records.13 Jul 2012a, Disponível em: <https://assets.documentcloud.org/documents/710559/doc01187820130608104742.pdf>. Acesso em: 20 set 2016.

_____. **Boundless Informant - Frequently Asked Questions**. 6 Set 2012b. Disponível em: <https://assets.documentcloud.org/documents/710558/doc01187620130608104422.pdf>. Acesso em: 20 set 2016.

_____. Email Address vs User Activity. 24 Jun 2009a, Disponível em: <https://search.edwardsnowden.com/docs/EmailAddressvsUserActivity2015-07-01nsadocs>. Acesso em: 26 set 2016.

_____. **For Media Mining, the future is now!**1 Ago 2006.Disponível em: <https://assets.documentcloud.org/documents/2072019/sidtoday-future-is-now-final.pdf>. Acesso em: 20 set 2016.

_____. Intro to the VPN Exploitation Process. 13 Set 2010a, Disponível em: <https://edwardsnowden.com/2015/01/07/intro-to-the-vpn-exploitation-process/>. Acesso em: 26 set 2015.

_____. **Microsoft Skydrive Collection Now Part of PRISM Standard Stored Communications Collection**. 8 Mar 2013a.

Disponível em: <https://search.edwardsnowden.com/docs/SSOHIGHLIGHT%E2%80%93MicrosoftSkydriveCollectionNowPartofPRISMStandardStoredCommunicationsCollection2014-05-13nsadocs>. Acesso em: 27 set 2016.

_____. New Collection Posture. 2011, Disponível em: <https://edwardsnowden.com/2014/05/13/new-collection-posture/>. Acesso em: 30 out 2016.

_____. **New FAA702 Certification in the Works – Cyber Threat**.23 Mar 2012c.Disponível em: <https://edwardsnowden.com/docs/docs/pg_0002.pdf>. Acesso em: 29 set 2016.

_____. FY2013 Foreign Partner Review. 1 Jan 2013f, Data de publicação. Disponível em: <http://edwardsnowden.com/wp-content/uploads/2014/06/fy13.pdf>. Acesso em: 27 set 2016.

_____. NSA: How Network Mapping is Helping to Target the Credit Card Authorization Networks. 2010b, Disponível em: <https://edwardsnowden.com/2015/01/30/nsa-how-network-mapping-is-helping-to-target-the-credit-card-authorization-networks/>. Acesso em: 29 set 2016.

_____. **NSA Press statement in response to allegations about NSA operations. Washington, D. C., 30 Jul 2013. Disponível em:** <https://www.nsa.gov/news-features/press-room/statements/30-July-2013.shtml>. Acesso em: 20 set 2016.

_____. NSA Strategic Partnerships. 13 Maio 2014a, Data de publicação. Disponível em: <https://search.edwardsnowden.com/docs/NSAStrategicPartnerships2014-05-13nsadocs>. Acesso em: 27 set 2016.

_____. **PRISM/US-984XN. Overview or the SIGAD used most in NSA reporting overview**. Abr 2013c. Disponível em: <https://assets.documentcloud.org/documents/813847/prism.pdf>.

_____. Tier B allies. 13 Maio 2014b, Data de publicação. Disponível em: <http://edwardsnowden.com/wp-content/uploads/2014/06/tierb.pdf>. Acesso em: 27 set 2016.

_____. **Silent Success: SIGINT Synergy Helps Shape US Foreign Policy**. SIDToday, 30 Ago 2010c. Disponível em: <https://search.edwardsnowden.com/docs/SilentSuccessSIGINTSynergyHelpsShapeUSForeignPolicy2013-08-02nsadocs>. Acesso em: 26 set 2016.

_____. Special Source Operations: Corporate Partner Access. 1 Nov 2013d, Disponível em: <https://search.edwardsnowden.com/docs/SpecialSourceOperationsCorporatePartnerAccess2013-11-01nsadocs>. Acesso em: 27 set 2016.

_____. SSO Collection Optimization overview. 2012d, Disponível em: <https://search.edwardsnowden.com/docs/SSOCollectionOptimizationoverview2013-10-14nsadocs>. Acesso em: 26 set 2016.

_____. **SSO dictionary – FAIRVIEW**. Data de publicação, 15 Ago 2015a. Disponível em: <https://search.edwardsnowden.com/docs/SSOdictionary%E2%80%93FAIRVIEW2015-08-15nsadocs>. Acesso em: 29 set 2016.

_____. **SSO Expands PRISM Skype Targeting Capability**. 3 Abr 2013e.Disponível em: <https://search.edwardsnowden.com/docs/SSOExpandsPRISMSkypeTargetingCapability2014-05-13nsadocs>. Acesso em: 27 set 2016.

_____. **SSO FAIRVIEW Overview**. Disponível em: <https://edwardsnowden.com/docs/docs/fair.pdf>. Acesso em: 29 set 2016b.

_____. Targets visiting specific websites. 8 Jan 2007, Data de classificação. Disponível em: <https://search.edwardsnowden.com/docs/Targetsvisitingspecificwebsites2015-07-01nsadocs>. Acesso em: 26 set 2016.

_____. XKEYSCORE. 25 Fev 2008, Disponível em: <https://search.edwardsnowden.com/docs/XKeyScore2013-07-31nsadocs>. Acesso em: 26 set 2016.

_____. XKEYSCORE: Finding and Querying Document Metadata. Abr 2009b, Disponível em: <https://search.edwardsnowden.com/docs/FindingandQueryingonDocumentMetadata2015-07-01nsadocs>. Acesso em: 26 set 2016.

OBAMA, Barak. Address Before a Joint Session of the Congress on the State of the Union. 20 Jan 2015a, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201500036/pdf/DCPD-201500036.pdf>. Acesso em: 20 dez 2016.

_____. Address to the Nation by the President. 6 Dez 2015b, Press department. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201500874/pdf/DCPD-201500874.pdf> . Acesso em: 11 abr 2016.

_____. Remarks by the President at the National Defense University. 23 Maio 2013a, Press department. Disponível em: <https://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university>. Acesso em: 11 abr 2016.

_____. Remarks by the President in a Press Conference. 9 Ago 2013b, Press department. Disponível em: <https://www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference>. Acesso em: 11 abr 2016.

_____. Remarks on United States Signals Intelligence and Electronic Surveillance Programs. In: DEPARTMENT OF JUSTICE, 17 Jan 2014, Press department. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201400030/pdf/DCPD-201400030.pdf>. Acesso em: 4 abr 2016.

_____. Remarks on Improving Homeland Security (07/01/2010).**Barack Obama (book I — january 1 to june 30,**

2010). Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2013c. p. 8–10. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2010-book1/pdf/PPP-2010-book1.pdf>.

_____. Remarks to Federal Bureau of Investigation Employees (28/04/2009). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). **. Barack Obama (book I — january 1 to june 30, 2009).** Public papers of the presidents of the United States. Washington D. C.: United States Government Publishing Office, 2010. p. 565–566. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2009-book1/pdf/PPP-2009-book1.pdf>. Acesso em: 21 maio 2016.

_____. The President's News Conference With Chancellor Angela Merkel of Germany in Berlin, Germany. 19 Jun 2013d, United States Government Printing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201300438/pdf/DCPD-201300438.pdf>. Acesso em: 12 dez 2016.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI). Facts on the Collection of Intelligence pursuant to Section 702 of the Foreign Intelligence Surveillance Act. **Office of the Director of National Intelligence**, Washington, D.C., 8 Jun 2013. Disponível em: <https://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf>. Acesso em: 15 set 2016.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **El derecho a la privacidad en la era digital**. Relatório do Escritório Alto Comissário das Nações Unidas para os Direitos Humanos. Nova Iorque: Nações Unidas, 30 Jun 2014.

_____. 1 novembro 2013 a. **El derecho a la privacidad en la era digital**. , 1 Nov 2013. Disponível em: <http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45&Lang=S>. Acesso em: 23 mar 2016.

_____. 18 dezembro 2013 b. **El derecho a la privacidad en la era digital**. , 18 Dez 2013. Disponível em:

<http://www.un.org/es/comun/docs/?symbol=A/RES/68/167>. Acesso em: 16 nov 2015.

_____. 16 dezembro 1966. **Pacto Internacional de Derechos Civiles y Políticos**. , 16 Dez 1966. Disponível em: <http://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx>. Acesso em: 12 dez 2016.

PARLAMENTO EUROPEU. **LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens**. Relatório sobre procedimentos, resultados e documentos respaldatórios. Bruxelas: Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos do Parlamento Europeu, 16 Out 2014a. Disponível em: <http://www.polcms.europarl.europa.eu/cmsdata/upload/7d8972f0-e532-4b12-89a5-e97b39eec3be/att_20141016ATT91322-206135629551064330.pdf>.

_____. **Relatório sobre o programa de vigilância da Agência Nacional de Segurança dos EUA (NSA), os organismos de vigilância em diversos Estados-Membros e o seu impacto nos direitos fundamentais dos cidadãos da UE e na cooperação transatlântica no domínio da justiça e dos assuntos internos (2013/2188(INI))**. Relatório da Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos. [S.l.]: Parlamento Europeo, 21 Fev 2014b.

POWELL, Colin. Remarks at the Development, Democracy and Security Bretton Woods Committee Conference.30 Set 2004, Disponível em: <http://2001-2009.state.gov/secretary/former/powell/remarks/36649.htm>. Acesso em: 12 dez 2016.

_____. The U.S.-Middle East Partnership Initiative: Building Hope for the Years Ahead. 12 Dez 2002, Disponível em: <http://2001-2009.state.gov/secretary/former/powell/remarks/2002/15920.htm>. Acesso em: 12 dez 2016.

RICE, Condolezza. Centennial Annual Meeting of the American Society of International Law. In: CENTENNIAL ANNUAL

MEETING OF THE AMERICAN SOCIETY OF INTERNATIONAL LAW, 29 Mar 2006, Press department. Disponível em: <https://2001-2009.state.gov/secretary/rm/2006/63855.htm>. Acesso em: 4 abr 2016.

_____. **Interview on Fox News Sunday With Chris Wallace**. Washington D.C., 18 Dez 2005a. Disponível em: <http://2001-2009.state.gov/secretary/former/powell/remarks/33476.htm>. Acesso em: 5 abr 2016.

_____. **Interview With Morris Jones of Sinclair Broadcast Group**. Washington D.C., 8 Dez 2006b. Disponível em: <http://2001-2009.state.gov/secretary/rm/2006/71981.htm>. Acesso em: 4 abr 2016.

_____. **Interview With the New York Post Editorial Board**. Washington D.C., 25 Set 2006c. Disponível em: <http://2001-2009.state.gov/secretary/rm/2006/73107.htm>. Acesso em: 4 abr 2016.

_____. Opening Remarks Before the Senate Foreign Relations Committee. In: FAIRMONT HOTEL, 8 Fev 2007, Press department. Disponível em: <http://2001-2009.state.gov/secretary/rm/2007/feb/80271.htm>. Acesso em: 12 dez 2016.

_____. Remarks at Sophia University. 19 Mar 2005b, Press department. Disponível em: <http://2001-2009.state.gov/r/pa/ei/pix/2005/43647.htm>. Acesso em: 12 dez 2016.

_____. Remarks at the Institut d'Etudes Politiques de Paris. In: INSTITUT D'ETUDES POLITIQUES DE PARIS, 8 Fev 2005c, Press department. Disponível em: < https://2001-2009.state.gov/secretary/rm/2005/41973.htm >.

_____. Remarks On Transformational Diplomacy. In: GEORGETOWN UNIVERSITY, 12 Fev 2008, Press department. Disponível em: <https://2001-2009.state.gov/secretary/rm/2008/02/100703.htm>. Acesso em: 12 dez 2016.

ROGERS, Michael. Remarks by Admiral Michael S. Rogers at the New America Foundation Conference on Cybersecurity. In: NEW AMERICA FOUNDATION CONFERENCE ON CYBERSECURITY, 23 Fev 2015a, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/022315-new-america-foundation.shtml>. Acesso em: 6 abr 2016.

_____. Special Keynote Address by ADM Michael S. Rogers, Commander, U.S. Cyber Command, Director, National Security Agency, Chief, Central Security Service. In: FORDHAM UNIVERSITY'S FIFTH INTERNATIONAL CONFERENCE ON CYBER SECURITY (ICCS 2015), 8 Jan 2015b, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/fordham-transcript.shtml>. Acesso em: 6 abr 2016.

_____. Testimony of Admiral Michael S. Rogers, USN Director, National Security Agency Chief, Central Security Service before The Senate Select Committee on intelligence. In: SENATE SELECT COMMITTEE ON INTELLIGENCE, 24 Set 2015c, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/testimonies/nsa-sfr-ssci-open-hearing-22sept15.shtml>. Acesso em: 6 abr 2016.

ROUSSEFF, Dilma. **Discurso da Presidente da República Dilma Rousseff, na abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas**. . Nova Iorque: Assambleia-Geral da Organização das Nações Unidas (ONU), 2013.

APÊNDICE

Listado de documentos analisados. Acompanha a versão impressa da presente dissertação um CD-Rom contendo todos os documentos completos.

Documentos doutrinários

ESTADOS UNIDOS DA AMÉRICA (EUA). **A Warfighting Domain**. Washington D.C., 26 Set 2006a. Disponível em: <http://www.au.af.mil/info-ops/usaf/cyberspace_taskforce_sep06.pdf>. Acesso em: 14 jul 2015.

_____. **Cyber Strategy**. Institucional. Disponível em: <http://www.defense.gov/home/features/2015/0415_cyber-strategy/>. Acesso em: 23 jul 2015a.

_____. **Department of Defense Dictionary of Military and Associated Terms**. Joint Publication 1-02. Washington D. C.: Department of Defense, 31 Jan 2011a. Disponível em: <http://ra.defense.gov/Portals/56/Documents/rtm/jp1_02.pdf>. Acesso em: 11 set 2015.

_____. **Department of defense strategy for operating in Cyberspace**. . Washington D. C.: Department of Defense, 2011b.

_____. NSA21: Facing Threats to the Nation and Future Challenges with Innovation, Integration, and a Focus on Talent. **nsa.gov**, 8 Fev 2016. Disponível em: <about:reader?url=https%3A%2F%2Fwww.nsa.gov%2Fpublic_info%2Fspeeches_testimonies%2F08feb16.shtml>. Acesso em: 6 abr 2016.

_____. **The department of Defense Cyber Strategy**. . [S.l: s.n.], 2015b. Disponível em: <http://www.defense.gov/home/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>. Acesso em: 16 jun 2015.

_____. **The national military strategy for cyberspace operations**. . Washington D. C.: Department of Defense, 2006b.

_____. **The National Military Strategy of the United States of America**. . Washington D. C.: Department of Defense, 2004.

_____. **The National Security Strategy of the United States of America**. Whashington, D. C., 17 Set 2002. Disponível em: <https://www.state.gov/documents/organization/63562.pdf>. Acesso em: 20 abr 2016.

_____. **The national strategy to secure cyberspace**. Washington, D.C., 2003. Disponível em: <https://georgewbush-whitehouse.archives.gov/pcipb/cyberspace_strategy.pdf>. Acesso em: 20 abr 2016.

Textos normativos

ESTADOS UNIDOS DA AMÉRICA (EUA). Executive order. , de 1 abril 2015. **Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities**. Washington D.C., 1 Abr 2015, p. 44. Disponível em: <https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m>. Acesso em: 11 abr 2016.

_____. **Department of Defense Cyberspace Policy Report. A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934**. . Washington, D.C.: Department of Defense, Nov 2011. Disponível em: <https://fas.org/irp/eprint/dod-cyber.pdf>. Acesso em: 12 dez 2016.

_____. **Fact Sheet: Retroactive liability protection is critical to our National Security**. Disponível em: <https://www.justice.gov/archive/ll/docs/fisa-factsheet-070808.pdf>. Acesso em: 16 jan 2017a.

_____. **Fact sheet: Retroactive Liability Protection: Providing Our Intelligence Officials The Tools They Need To**

Keep Our Nation Safe. Disponível em: <https://www.justice.gov/archive/ll/docs/fisawhfactsheet.pdf>. Acesso em: 16 jan 2017b.

_____. 95–511. , de 16 outubro 1978. **Foreign Intelligence Surveillance Act of 1978**. Washington D.C., 16 Out 1978. Disponível em: <http://fas.org/irp/agency/doj/fisa/hspci1978.pdf>. Acesso em: 22 mar 2016.

_____. 110–261. , de 10 julho 2008 c. **Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008**. Washington D.C., 10 Jul 2008, p. 44. Disponível em: <https://www.congress.gov/110/plaws/publ261/PLAW-110publ261.pdf>. Acesso em: 11 abr 2016.

_____. 29 outubro 2001 a. **Homeland Security Presidential Directive–1—Organization and Operation of the Homeland Security Council**. , 29 Out 2001. Disponível em: <https://georgewbush-whitehouse.archives.gov/news/releases/2001/10/20011030-1.html>. Acesso em: 30 set 2016.

_____. PPD-28. , de 17 janeiro 2014. **Presidential Policy Directive - Signals Intelligence Activities**. Washington D.C., 17 Jan 2014. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201400031/pdf/DCPD-201400031.pdf>. Acesso em: 11 abr 2016.

_____. 110–55. , de 5 agosto 2007. **Protect America Act of 2007**. **Aug. 3, considered and passed Senate. Aug. 4, considered and passed House.**, , 5 Ago 2007. Disponível em: <https://www.congress.gov/110/plaws/publ55/PLAW-110publ55.pdf>. Acesso em: 21 nov 2016.

_____. 107–56. , de 26 outubro 2001 b. **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001**. Washington D.C., 26 Out 2001, p. 132. Disponível em: <frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf>. Acesso em: 2 jun 2015.

Manifestações públicas

ALEXANDER, Keith. Clear and Present Danger: Cyber-Crime; Cyber-Espionage; Cyber-Terror; and Cyber-War. In: ASPEN SECURITY FORUM, 18 Jul 2013a, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/gen-a-aspen-security-forum-transcript-18july2013.shtml>. Acesso em: 6 abr 2016.

_____. General Keith Alexander Speaks at AFCEA's Conference. In: AFCEA'S CONFERENCE, 28 Jun 2013b, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/transcript-gen-a-afcea-keynote-27june2013.shtml>. Acesso em: 6 abr 2016.

_____. Keynote Address by General Keith Alexander, Director, National Security Agency. In: BLACK HAT USA 2013, 31 Jul 2013c, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/transcript-of-gen-alexander-black-hat-speech-31july2013.shtml>. Acesso em: 6 abr 2016.

_____. Statement for the Record Lieutenant General Keith Alexander Commander Joint Functional Component Command for Network Warfare Before the House Armed Services Committee Terrorism, Unconventional Threats, and Capabilities Subcommittee. In: HOUSE ARMED SERVICES COMMITTEE TERRORISM, UNCONVENTIONAL THREATS, AND CAPABILITIES SUBCOMMITTEE, 5 Maio 2009a, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/testimonies/alexander-statement-5may09.shtml>. Acesso em: 11 abr 2016.

_____. Statement for the Record of LT GEN Keith B. Alexander Director, National Security Agency before the Committee on the Judiciary United States Senate. In: COMMITTEE ON THE JUDICIARY UNITED STATES SENATE, 26 Jul 2006, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/testimonies/26july06-dirnsa.shtml>. Acesso em: 20 abr 2016.

_____. The Director of the National Security Agency (NSA) and Chief of the Central Security Service (CSS) briefed on “Securing Our Government Networks”. In: RSA SECURITY CONFERENCE, 22 Abr 2009b, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/21apr09-dir.shtm>. Acesso em: 12 abr 2016.

_____. U.S. cybersecurity policy and the role of U.S. CYBERCOM. In: CSIS CYBERSECURITY POLICY DEBATE SERIES, 6 Mar 2010, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/100603-alenander-transcript.shtml>. Acesso em: 6 abr 2016.

BUSH, Jorge W. Address Before a Joint Session of the Congress on the State of the Union (31/01/2006). **George W. Bush (book I — january 1 to june 30, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010a. p. 146–155. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book1/pdf/PPP-2006-book1.pdf>.

_____. Address Before a Joint Session of the Congress on the United States Response to the Terrorist Attacks of September 11 (25/09/2001). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2001)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2005a. p. 1140–1144. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2001-book2/pdf/PPP-2001-book2.pdf>.

_____. Interview With Brit Hume of FOX News (07/01/2009). **George W. Bush (book II — july 1, 2008 to january 20, 2009)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2012a. p. 1531–1542. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2008-book2/pdf/PPP-2008-book2.pdf>.

_____. Remarks at a Breakfast for Congressional Candidate Richard G. Renzi in Scottsdale, Arizona (04/10/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010b. p. 1765–1773. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book2/pdf/PPP-2006-book2.pdf>.

_____. Remarks at a Breakfast for Congressional Candidate Richard W. Pombo in Stockton, California (03/10/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010c. p. 1750–1757. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book2/pdf/PPP-2006-book2.pdf>.

_____. Remarks at a Reception for Congressional Candidate Don Sherwood and the Pennsylvania Victory Committee in La Plume, Pennsylvania (19/10/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010d. p. 1872–1878. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book2/pdf/PPP-2006-book2.pdf>.

_____. Remarks at a Reception for Congressional Candidate Michael A. "'Mac'" Collins in Macon, Georgia (10/10/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010e. p. 1807–1813. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book2/pdf/PPP-2006-book2.pdf>.

_____. Remarks at a Reception for Congressional Candidates Peter Roskam and David McSweeney and the Illinois Congressional Victory Committee in Chicago, Illinois

(12/10/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010f. p. 1872–1878. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book2/pdf/PPP-2006-book2.pdf>.

_____. Remarks at the Federal Bureau of Investigation Academy in Quantico Virginia (10/09/2003). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2003)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2006a. p. 1133–1139. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2.pdf>.

_____. Remarks at the National Hispanic Prayer Breakfast (30/06/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010g. p. 1100–1103. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book1/pdf/PPP-2006-book1.pdf>.

_____. Remarks at the Port of Charleston, South Carolina (05/02/2004). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2004)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007a. p. 184–189. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2004-book1/pdf/PPP-2004-book1.pdf>.

_____. Remarks Following a Visit to the National Security Agency at Fort Meade, Maryland (19/09/2007). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2007)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2011a. p. 1210–1211. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2007-book2/pdf/PPP-2007-book2.pdf>.

_____. Remarks Following a Visit to the National Security Agency at Fort Meade, Maryland (25/01/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010h. p. 124–126. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book1/pdf/PPP-2006-book1.pdf>.

_____. Remarks in Hershey, Pennsylvania (19/04/2004). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2004)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007b. p. 603–611. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2004-book1/pdf/PPP-2004-book1.pdf>.

_____. Remarks in Miami (27/08/2004). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2004)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007c. p. 1756–1763. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2004-book2/pdf/PPP-2004-book2.pdf>.

_____. Remarks in Nashville, Tennessee (01/02/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010i. p. 154–168. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book1/pdf/PPP-2006-book1.pdf>.

_____. Remarks in Panama City, Florida (10/08/2004). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2004)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007d. p. 1589–1595. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2004-book2/pdf/PPP-2004-book2.pdf>.

_____. Remarks on Intelligence Reform Legislation (09/07/2008). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to June 30, 2008)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2012b. p. 1007. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2001-book2/pdf/PPP-2008-book1.pdf>.

_____. Remarks on Signing the FISA Amendments Act of 2008 (10/07/2008). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1, 2008 to january 20, 2009)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2012c. p. 1007–1009. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2008-book2/pdf/PPP-2008-book2.pdf>.

_____. Remarks on Signing the USA PATRIOT ACT of 2001 (26/10/2001). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2001)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2005b. p. 1306–1307. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2001-book2/pdf/PPP-2001-book2.pdf>.

_____. Remarks on the Anniversary of the United States Department of Homeland Security (02/03/2004). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2004)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007e. p. 291–295. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2004-book1/pdf/PPP-2004-book1.pdf>.

_____. Remarks on the PATRIOT Act in Baltimore, Maryland (20/07/2005). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2005)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007f. p. 1249–1256. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2005-book2/pdf/PPP-2005-book2.pdf>.

_____. Remarks on the PATRIOT Act in Columbus, Ohio (09/06/2005). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2005)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007g. p. 958–962. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2005-book2/pdf/PPP-2005-book2.pdf>.

_____. Remarks on the PATRIOT Act in McLean, Virginia (10/06/2005). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2005)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007h. p. 964–967. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2005-book2/pdf/PPP-2005-book2.pdf>.

_____. Remarks on the War on Terror and a Question-and-Answer Session in Louisville, Kentucky (11/01/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010j. p. 41–58. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book1/pdf/PPP-2006-book1.pdf>.

_____. Remarks on the War on Terror and a Question-and-Answer Session in Manhattan, Kansas (23/01/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010k. p. 101–123. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book1/pdf/PPP-2006-book1.pdf>.

_____. Remarks to Department of Homeland Security Employees (28/03/2003). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2003)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2006b. p. 226–229. Disponível em:

<https://www.gpo.gov/fdsys/pkg/PPP-2003-book1/pdf/PPP-2003-book1.pdf>.

_____. Remarks to Federal Bureau of Investigation Employees (25/09/2001). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2001)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2005c. p. 1160–1162. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2001-book2/pdf/PPP-2001-book2.pdf>.

_____. Remarks to Reporters Following a Visit With United States Troops and an Exchange With Reporters in San Antonio, Texas (01/01/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010l. p. 1–3. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book1/pdf/PPP-2006-book1.pdf>.

_____. Remarks to the City Club of Cleveland and a Question-and-Answer Session in Cleveland, Ohio (20/03/2006). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2006)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010m. p. 504–520. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2006-book1/pdf/PPP-2006-book1.pdf>.

_____. Remarks to the Veterans of Foreign Wars National Convention in Salt Lake City, Utah (22/08/2005). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2005)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007i. p. 1336–1341. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2005-book2/pdf/PPP-2005-book2.pdf>.

_____. The President's News Conference (19/12/2005). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2005)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007j. p. 1875–1888. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2005-book2/pdf/PPP-2005-book2.pdf>.

_____. The President's Radio Address (17/04/2004). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2004)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007k. p. 600–601. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2004-book1/pdf/PPP-2004-book1.pdf>.

_____. The President's Radio Address (20/03/2004). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book I — january 1 to june 30, 2004)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2007l. p. 414–416. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2004-book1/pdf/PPP-2004-book1.pdf>.

_____. The President's Radio Address (21/07/2007). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2007)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2011b. p. 1039–1040. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2007-book2/pdf/PPP-2007-book2.pdf>.

_____. The President's Radio Address (23/08/2003). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2003)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2006c. p. 1053–1054. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2.pdf>.

_____. The President's Radio Address (27/10/2001). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **George W. Bush (book II — july 1 to december 31, 2001)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2005d. p. 1312–1314. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2001-book2/pdf/PPP-2001-book2.pdf>.

CLINTON, Hillary. **America's Pacific Century: The Future of Geopolitics Will Be Decided in Asia, Not in Afghanistan or Iraq, and the United States Should Be Right at the Center of the Action**. Foreign Policy, n. 189, p. 56–63, 2011a.

_____. Conference on Internet Freedom. In: FOKKER TERMINAL, 12 Ago 2011b, Press department. Disponível em: <http://2009-2017.state.gov/secretary/20092013clinton/rm/2011/12/178511.htm>. Acesso em: 4 abr 2016.

_____. Digital Town Hall at TecMilenio University. In: DIGITAL TOWN HALL, 26 Mar 2009, Press department. Disponível em: <https://2009-2017.state.gov/secretary/20092013clinton/rm/2009a/03/120955.htm>. Acesso em: 11 abr 2016.

_____. Internet Rights and Wrongs: Choices & Challenges in a Networked World. 15 Fev 2011c, Disponível em: <http://2009-2017.state.gov/secretary/20092013clinton/rm/2011/02/156619.htm>. Acesso em: 5 abr 2016.

_____. Remarks at the Australia-United States Ministerial. 11 Ago 2010a, Disponível em: <http://2009-2017.state.gov/secretary/20092013clinton/rm/2010/11/150663.htm>. Acesso em: 4 abr 2016.

_____. Remarks on Internet Freedom. In: THE NEWSEUM, 21 Jan 2010b, Disponível em: <https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm>. Acesso em: 11 abr 2016.

_____. Remarks With Australian Foreign Minister Robert Carr, Australian Defense Minister Stephen Smith, and Secretary of Defense Leon Panetta. 14 Nov 2012, Press department. Disponível em: <https://2009-2017.state.gov/secretary/20092013clinton/rm/2012/11/200507.htm>. Acesso em: 11 abr 2016.

_____. Remarks With Secretary of Defense Robert Gates, Australian Foreign Minister Stephen Smith, and Australian Defense Minister Joel Fitzgibbon. 4 Set 2009, Press department. Disponível em: <http://m.state.gov/md121555.htm>. Acesso em: 11 abr 2016.

CLINTON, Hillary; GATES, Robert; CARTWRIGHT, James. Press Briefing With White House Press Secretary Robert Gibbs, Secretary of Defense Robert Gates, and Vice Chairman of the Joint Chiefs of Staff General James Cartwright. 16 Dez 2010, Press department. Disponível em: <https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/12/153041.htm>. Acesso em: 11 abr 2016.

CLINTON, Hillary; PANETTA, Leon. **A Conversation with Secretaries Hillary Clinton and Leon Panetta**. Washington D.C, 16 Ago 2011. Disponível em: <http://2009-2017.state.gov/secretary/20092013clinton/rm/2011/08/170611.htm>. Acesso em: 11 abr 2016.

ESTADOS UNIDOS DA AMÉRICA (EUA). Homeland Security Presidential Directive–1—Organization and Operation of the Homeland Security Council (29/10/2001). **George W. Bush (book II — july 1 to december 31, 2001)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2005. p. 1320–1322. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2001-book2/pdf/PPP-2001-book2.pdf>.

HAYDEN, Michael. Statement For The Record Before The Governmental Affairs Subcommittee On International Security, Proliferation, And Federal Services Hearing On Critical Skills For National Security And The Homeland Security Federal Workforce

Act. In: THE GOVERNMENTAL AFFAIRS SUBCOMMITTEE ON INTERNATIONAL SECURITY, PROLIFERATION, AND FEDERAL SERVICES HEARING ON CRITICAL SKILLS FOR NATIONAL SECURITY AND THE HOMELAND SECURITY FEDERAL WORKFORCE ACT, 3 Dez 2002a, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/testimonies/12mar02.shtml>. Acesso em: 6 abr 2016.

_____. Statement for the Record by Lieutenant General Michael V. Hayden, USAF, Director, National Security Agency/Chief, Central. 17 Out 2002b, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/testimonies/17oct02-dirnsa.shtml>. Acesso em: 6 abr 2016.

KERRY, John. **Interview With Andres Oppenheimer of CNN Espanol and The Miami Herald**. Washington D.C., 12 Set 2013a. Disponível em: <http://2009-2017.state.gov/secretary/remarks/2013/12/218810.htm>. Acesso em: 12 abr 2016.

_____. **Interview With Bild Newspaper**. Washington D.C., 11 Jul 2013b. Disponível em: <http://2009-2017.state.gov/secretary/remarks/2013/11/217389.htm>. Acesso em: 12 abr 2016.

_____. **Interview With Charlie Rose and Norah O'Donnell of CBS**. Washington, D.C., 28 Maio 2014a. Disponível em: <https://2009-2017.state.gov/secretary/remarks/2014/05/226578.htm>.

_____. **Interview With Chuck Todd of MSNBC's The Daily Rundown**. Washington D.C., 28 Maio 2014b. Disponível em: <https://2009-2017.state.gov/secretary/remarks/2014/05/226598.htm>. Acesso em: 11 abr 2016.

_____. **Interview With Elise Labott of CNN**. Washington D.C., 24 Jun 2013c. Disponível em: <http://2009-

2017.state.gov/secretary/remarks/2013/06/211089.htm>. Acesso em: 12 abr 2016.

_____. **Interview With Nikole Killion of Hearst Television**. Washington D.C., 18 Mar 2014c. Disponível em: <https://2009-2017.state.gov/secretary/remarks/2014/03/223667.htm>. Acesso em: 11 abr 2016.

_____. **Interview With Wang Guan of CCTV**. Washington D.C., 30 Jun 2014d. Disponível em: <https://2009-2017.state.gov/secretary/remarks/2014/06/228904.htm>. Acesso em: 12 abr 2016.

_____. Joint Press Availability With Secretary of Defense Chuck Hagel, Australian Foreign Minister Julie Bishop, and Australian Defence Minister David Johnston. 20 Nov 2013, Press department. Disponível em: <https://2009-2017.state.gov/secretary/remarks/2013/11/217817.htm>. Acesso em: 11 abr 2016.

_____. Remarks to the Freedom Online Coalition Conference. In: FREEDOM ONLINE COALITION CONFERENCE, 28 Abr 2014e, Press department. Disponível em: <http://2009-2017.state.gov/secretary/remarks/2014/04/225290.htm>. Acesso em: 12 abr 2016.

KERRY, John; HAGUE, William. Remarks With British Foreign Secretary William Hague After Their Meeting. 6 Dez 2013, Disponível em: <https://2009-2017.state.gov/secretary/remarks/2013/06/210583.htm>. Acesso em: 11 abr 2016.

KERRY, John; STEINMEIER, Frank-Walter. Remarks With German Foreign Minister Frank-Walter Steinmeier After Their Meeting. In: BERLIN TEGEL AIRPORT, 31 Jan 2014a, Press department. Disponível em: <http://2009-2017.state.gov/secretary/remarks/2014/01/221085.htm>. Acesso em: 12 abr 2016.

_____. Remarks With German Foreign Minister Frank-Walter Steinmeier After Their Working Lunch. In: BENJAMIN FRANKLIN ROOM, 27 Fev 2014b, Press department. Disponível em: <http://2009-2017.state.gov/secretary/remarks/2014/02/222657.htm>. Acesso em: 1 mar 2017.

NATIONAL SECURITY AGENCY (NSA). NSA Press Statement in response to allegations about NSA operations. 30 Jul 2013a, Press department. Disponível em: <https://www.nsa.gov/news-features/press-room/statements/30-July-2013.shtml>. Acesso em: 6 abr 2016.

_____. Statement in response to press allegations. 13 Mar 2014, Press department. Disponível em: <https://www.nsa.gov/news-features/press-room/statements/2014-03-14-press-allegations-response.shtml>. Acesso em: 6 abr 2016.

_____. Statement to the Press: NSA's Activities: Valid Foreign Intelligence Targets Are the Focus. **nsa.gov**, 31 Out 2013b. Disponível em: <https://www.nsa.gov/news-features/press-room/public-announcements/2013/NSA-Activities-Valid-FI-Targets.shtml>. Acesso em: 6 abr 2016.

NATIONAL SECURITY AGENCY (NSA); OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI). Joint ODNI-NSA Statement in Response to Reports Mischaracterizing NSA Collection of Online Communications Under FISA Section 702. **nsa.gov**, Washington, D.C., 21 Ago 2013. Disponível em: <https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_21_Joint_Statement_ODNI_NSA.pdf>. Acesso em: 6 abr 2016.

OBAMA, Barack. Address Before a Joint Session of the Congress on the State of the Union. 20 Jan 2015a, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201500036/pdf/DCPD-201500036.pdf>. Acesso em: 20 dez 2016.

_____. Address Before a Joint Session of the Congress on the State of the Union. 28 Jan 2014a, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201400050/pdf/DCPD-201400050.pdf>. Acesso em: 20 dez 2015.

_____. Address to the Nation by the President. 12 Jun 2015b, Press department. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201500874/pdf/DCPD-201500874.pdf>. Acesso em: 11 abr 2016.

_____. Commencement Address at the United States Air Force Academy in Colorado Springs, Colorado. 6 Fev 2016a, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201600373/pdf/DCPD-201600373.pdf>. Acesso em: 19 nov 2016.

_____. **Interview of the President by Jay Leno, The Tonight Show**. California, 8 Jun 2013a. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201300551/pdf/DCPD-201300551.pdf>. Acesso em: 11 abr 2016.

_____. Remarks at the Central Intelligence Agency. ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **Barack Obama (book I — january 1 to june 30, 2011)**. Public papers of the presidents of the United States. Langley, Virginia: United States Government Printing Office, 2011. p. 567–569. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2011-book1/pdf/PPP-2011-book1.pdf>.

_____. Remarks at the Veterans of Foreign Wars Convention in Phoenix, Arizona. In: ETERANS OF FOREIGN WARS CONVENTION, 17 Set 2009, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-200900650/pdf/DCPD-200900650.pdf>. Acesso em: 11 abr 2016.

_____. Remarks by the President at the National Defense University. In: NATIONAL DEFENSE UNIVERSITY, 23 Maio 2013b, Press department. Disponível em:

<https://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university>. Acesso em: 11 abr 2016.

_____. Remarks During a Question -and -Answer Session at the South by Southwest Interactive Festival in. 5 Nov 2016b, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201600138/pdf/DCPD-201600138.pdf>. Acesso em: 20 dez 2016.

_____. Remarks Following a Meeting With President Xi Jinping of China and an Exchange With Reporters. 6 Jul 2013c, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201300404/pdf/DCPD-201300404.pdf>. Acesso em: 20 dez 2016.

_____. Remarks on Health Insurance Reform and an Exchange With Reporters in San Jose, California. 7 Jul 2013d, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201300397/pdf/DCPD-201300397.pdf>. Acesso em: 11 abr 2016.

_____. Remarks on Securing the Nation's Information and Communications Infrastructure (29/05/2009). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **Barack Obama (book I — january 1 to june 30, 2009)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010a. p. 731–735. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2009-book1/pdf/PPP-2009-book1.pdf>.

_____. Remarks on United States Signals Intelligence and Electronic Surveillance Programs. In: DEPARTMENT OF JUSTICE, 17 Jan 2014b, Press department. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201400030/pdf/DCPD-201400030.pdf>. Acesso em: 4 abr 2016.

_____. Remarks Prior to a Meeting With Senior Officials at the Federal Bureau of Investigation and an Exchange With Reporters

(28/04/2009). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **Barack Obama (book I — january 1 to june 30, 2009)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Publishing Office, 2010b. p. 564. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2009-book1/pdf/PPP-2009-book1.pdf>. Acesso em: 21 maio 2016.

_____. Remarks to Federal Bureau of Investigation Employees (28/04/2009). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **Barack Obama (book I — january 1 to june 30, 2009)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Publishing Office, 2010c. p. 565–566. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2009-book1/pdf/PPP-2009-book1.pdf>. Acesso em: 21 maio 2016.

_____. Statement by the President on the Cybersecurity Framework. 2 Dez 2014c, Press department. Disponível em: <https://www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework>. Acesso em: 11 abr 2016.

_____. Statement by the President on the Section 215 Bulk Metadata Program. 27 Mar 2014d, US Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201400213/pdf/DCPD-201400213.pdf>. Acesso em: 11 abr 2016.

_____. Statement on Congressional Passage of the USA FREEDOM Act. 6 Fev 2015c, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201500412/pdf/DCPD-201500412.pdf>. Acesso em: 11 abr 2016.

_____. Statement on Signing the Intelligence Authorization Act for Fiscal Year 2010. 10 Jul 2010d, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201600138/pdf/DCPD-201600138.pdf>. Acesso em: 20 dez 2016.

_____. Statement on the European Union-United States Agreement on the Terrorist Finance Tracking Program. ESTADOS

UNIDOS DA AMÉRICA (EUA) (Org.). . **Barack Obama (book II — july 1 to december 31, 2010)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2013e. p. 1043–1044. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2010-book2/pdf/PPP-2010-book2.pdf>.

_____. Statement on the White House Organization for Homeland Security and Counterterrorism (26/05/2009). ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **Barack Obama (book I — january 1 to june 30, 2009)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2010e. p. 717–718. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2009-book1/pdf/PPP-2009-book1.pdf>.

_____. The President's News Conference. 8 Set 2013f, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201300562/pdf/DCPD-201300562.pdf>. Acesso em: 11 abr 2016.

_____. The President's News Conference. 20 Dez 2013g, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201300865/pdf/DCPD-201300865.pdf>. Acesso em: 11 abr 2016.

OBAMA, Barack; HARPER, Stephen. Joint Declaration by President Barack Obama and Prime Minister Stephen J. Harper of Canada: Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness. ESTADOS UNIDOS DA AMÉRICA (EUA) (Org.). . **Barack Obama (book I — january 1 to june 30, 2011)**. Public papers of the presidents of the United States. Washington D. C.: United States Government Printing Office, 2011. p. 84–87. Disponível em: <https://www.gpo.gov/fdsys/pkg/PPP-2011-book1/pdf/PPP-2011-book1.pdf>.

OBAMA, Barack; HOLLANDE, François. The President's News Conference With President François Hollande of France. 2 Nov 2014, U.S. Government Publishing Office. Disponível em:

<https://www.gpo.gov/fdsys/pkg/DCPD-201400082/pdf/DCPD-201400082.pdf>. Acesso em: 20 dez 2016.

OBAMA, Barack; MERKEL, Angela. The President's News Conference With Chancellor Angela Merkel of Germany. 5 Fev 2014, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201400324/pdf/DCPD-201400324.pdf>. Acesso em: 20 dez 2015.

_____. The President's News Conference With Chancellor Angela Merkel of Germany. 2 Set 2015, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201500089/pdf/DCPD-201500089.pdfhttps://www.gpo.gov/fdsys/pkg/DCPD-201500089/pdf/DCPD-201500089.pdf>.

_____. The President's News Conference With Chancellor Angela Merkel of Germany in Berlin, Germany. 19 Jul 2013, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201300438/pdf/DCPD-201300438.pdf>. Acesso em: 20 dez 2016.

_____. The President's News Conference With Chancellor Angela Merkel of Germany in Hannover, Germany. 24 Abr 2016, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201600260/pdf/DCPD-201600260.pdf>. Acesso em: 20 dez 2016.

OBAMA, Barack; REINFELDT, John Fredrik. The President's News Conference With Prime Minister John Fredrik Reinfeldt of Sweden in Stockholm, Sweden. 9 Abr 2013, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201300599/pdf/DCPD-201300599.pdf>. Acesso em: 20 dez 2016.

OBAMA, Barack; ROUSSEFF, Dilma. The President's News Conference With President Dilma Rousseff of Brazil. 30 Jun 2015, U.S. Government Publishing Office. Disponível em:

<https://www.gpo.gov/fdsys/pkg/DCPD-201500412/pdf/DCPD-201500412.pdf>. Acesso em: 11 abr 2016.

OBAMA, Barack; RUTTE, Mark. The President's News Conference With Prime Minister Mark Rutte of the Netherlands in The Hague, Netherlands. 25 Maio 2014, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201400197/pdf/DCPD-201400197.pdf>. Acesso em: 20 dez 2016.

OBAMA, Barack; SALL, Macky. The President's News Conference With President Macky Sall of Senegal. 20 Dez 2013, U.S. Government Publishing Office. Disponível em: <https://www.gpo.gov/fdsys/pkg/DCPD-201300463/pdf/DCPD-201300463.pdf>. Acesso em: 20 dez 2016.

OBAMA, Barack; SINGH, Manmohan. U.S.-India Joint Statement. 27 Set 2013, The White House Office of the Press Secretary. Disponível em: <https://obamawhitehouse.archives.gov/the-press-office/2013/09/27/us-india-joint-statement>. Acesso em: 20 dez 2016.

POWELL, Colin. Remarks at the Development, Democracy and Security Bretton Woods Committee Conference. 30 Set 2004, Disponível em: <http://2001-2009.state.gov/secretary/former/powell/remarks/36649.htm>. Acesso em: 12 dez 2016.

_____. The U.S.-Middle East Partnership Initiative: Building Hope for the Years Ahead. 12 Dez 2002, Disponível em: <http://2001-2009.state.gov/secretary/former/powell/remarks/2002/15920.htm>. Acesso em: 12 dez 2016.

RICE, Condolezza. Building Partnership Capacity and development of the Interagency Process. 15 Abr 2008a, Press department. Disponível em: <https://2001-2009.state.gov/secretary/rm/2008/04/103589.htm>. Acesso em: 20 dez 2015.

_____. Centennial Annual Meeting of the American Society of International Law. In: CENTENNIAL ANNUAL MEETING OF THE AMERICAN SOCIETY OF INTERNATIONAL LAW, 29 Mar 2006a, Press department. Disponível em: <https://2001-2009.state.gov/secretary/rm/2006/63855.htm>. Acesso em: 4 abr 2016.

_____. **Interview on CNN with Wolf Blitzer**. Washington D.C., 19 Dez 2005a. Disponível em: <http://2001-2009.state.gov/secretary/former/powell/remarks/31280.htm>. Acesso em: 4 abr 2016.

_____. **Interview on CNN With Zain Verjee**. Washington D.C., 17 Dez 2008b. Disponível em: <http://2001-2009.state.gov/secretary/rm/2006/74860.htm>. Acesso em: 4 abr 2006.

_____. **Interview on Fox News Sunday With Chris Wallace**. Washington D.C., 18 Dez 2005b. Disponível em: <http://2001-2009.state.gov/secretary/former/powell/remarks/33476.htm>. Acesso em: 5 abr 2016.

_____. **Interview on NBC Today Show With Katie Couric**. Washington D.C., 16 Dez 2005c. Disponível em: <http://2001-2009.state.gov/g/rls/rm/2003/16914.htm>. Acesso em: 4 abr 2016.

_____. **Interview on NBC with Andrea Mitchell**. Washington D.C., 16 Dez 2005d. Disponível em: <http://2001-2009.state.gov/secretary/rm/2005/58287.htm>.

_____. **Interview on NBC's Meet the Press With Tim Russert**. Washington D.C., 8 Jun 2006b. Disponível em: <http://2001-2009.state.gov/secretary/rm/2006/70014.htm>. Acesso em: 4 abr 2016.

_____. **Interview With Morris Jones of Sinclair Broadcast Group**. Washington D.C., 12 Ago 2006c. Disponível em:

<http://2001-2009.state.gov/secretary/rm/2006/71981.htm>. Acesso em: 4 abr 2016.

_____. **Interview With Paul Smith of The Paul Smith Show**. Washington D.C., 10 Dez 2006d. Disponível em: <http://2001-2009.state.gov/secretary/rm/2006/73907.htm>. Acesso em: 4 abr 2016.

_____. **Interview With the New York Post Editorial Board**. Washington D.C., 25 Set 2006e. Disponível em: <http://2001-2009.state.gov/secretary/rm/2006/73107.htm>. Acesso em: 4 abr 2016.

_____. Opening Remarks and Q&A Session at Chicago Council on Foreign Relations. In: CHICAGO COUNCIL ON FOREIGN RELATIONS, 19 Abr 2006f, Press department. Disponível em: <https://2001-2009.state.gov/secretary/rm/2006/64797.htm>.

_____. Opening Remarks Before the Senate Foreign Relations Committee. In: FAIRMONT HOTEL, 2 Ago 2007a, Press department. Disponível em: <http://2001-2009.state.gov/secretary/rm/2007/feb/80271.htm>. Acesso em: 12 dez 2016.

_____. Remarks at Sophia University. 19 Mar 2005e, Press department. Disponível em: <https://2001-2009.state.gov/secretary/rm/2005/43655.htm>. Acesso em: 12 dez 2016.

_____. Remarks at the Institut d'Etudes Politiques de Paris. In: INSTITUT D'ETUDES POLITIQUES DE PARIS, 2 Ago 2005f, Press department. Disponível em: <https://2001-2009.state.gov/secretary/rm/2005/41973.htm>.

_____. Remarks On Transformational Diplomacy. 2 Ago 2007b, Press department. Disponível em: <https://2001-2009.state.gov/secretary/rm/2007/feb/80989.htm>. Acesso em: 12 dez 2016.

_____. Remarks On Transformational Diplomacy. In: GEORGETOWN UNIVERSITY, 2 Dez 2008c, Press department. Disponível em: <https://2001-2009.state.gov/secretary/rm/2008/02/100703.htm>. Acesso em: 12 dez 2016.

_____. Remarks With Egyptian Foreign Minister Aboul Gheit. 19 Abr 2006g, Press department. Disponível em: <https://2001-2009.state.gov/secretary/rm/2007/mar/82166.htm>. Acesso em: 20 dez 2015.

ROGERS, Michael. Cyber war: The Role of Cyber in the 21st Century Warfare. In: REAGAN NATIONAL DEFENSE FORUM, 15 Nov 2014a, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/reagan.shtml>. Acesso em: 6 abr 2016.

_____. Hearing of the House (Select) Intelligence Committee Subject: “Cybersecurity Threats: The Way Forward”. In: HEARING OF THE HOUSE (SELECT) INTELLIGENCE COMMITTEE: “CYBERSECURITYTHREATS: THE WAY FORWARD,” 20 Nov 2014b, Press department. Disponível em: <https://www.nsa.gov/public_info/_files/speeches_testimonies/ADM.ROGERS.Hill.20.Nov.pdf>. Acesso em: 6 abr 2016.

_____. Remarks by Admiral Michael S. Rogers at the New America Foundation Conference on Cybersecurity. In: NEW AMERICA FOUNDATION CONFERENCE ON CYBERSECURITY, 23 Fev 2015a, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/022315-new-america-foundation.shtml>. Acesso em: 6 abr 2016.

_____. Sharing Cyber Threat Information to Protect Business and America. In: U.S. CHAMBER OF COMMERCE, 20 2014c, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/28oct14-dirnsa.shtml>. Acesso em: 6 abr 2016.

_____. Special Keynote Address by ADM Michael S. Rogers, Commander, U.S. Cyber Command, Director, National Security Agency, Chief, Central Security Service. In: FORDHAM UNIVERSITY'S FIFTH INTERNATIONAL CONFERENCE ON CYBER SECURITY (ICCS 2015), 1 Ago 2015b, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/fordham-transcript.shtml>. Acesso em: 6 abr 2016.

_____. Testimony of Admiral Michael S. Rogers, USN Director, National Security Agency Chief, Central Security Service before The Senate Select Committee on intelligence. In: SENATE SELECT COMMITTEE ON INTELLIGENCE, 24 Set 2015c, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/testimonies/nsa-sfr-ssci-open-hearing-22sept15.shtml>. Acesso em: 6 abr 2016.

_____. U.S. Cyber Command Commander and National Security Agency Director Admiral Michael Rogers. In: FREEMAN SPOGLI INSTITUTE FOR INTERNATIONAL STUDIES, 11 Mar 2014d, Press department. Disponível em: <https://www.nsa.gov/news-features/speeches-testimonies/speeches/cyber-maryland.shtml>. Acesso em: 6 abr 2016.

_____. U.S. Cyber Command Commander and National Security Agency Director Admiral Michael Rogers. In: CYBERMARYLAND 2014 CONFERENCE, 29 Out 2014e, Baltimore, Maryland. Anais... Baltimore, Maryland: Federal News Service, 29 Out 2014. Disponível em: <https://www.nsa.gov/public_info/_files/speeches_testimonies/CyberMaryland.pdf>. Acesso em: 6 abr 2016.