UNIVERSIDADE FEDERAL DE MINAS GERAIS
FACULDADE DE FILOSOFIA E CIÊNCIAS HUMANAS
BACHARELADO EM ANTROPOLOGIA – ANTROPOLOGIA SOCIAL

GUSTAVO RAMOS RODRIGUES

A LIBERDADE É A CHAVE:
UMA ETNOGRAFIA MULTISSITUADA DAS GUERRAS CRIPTOGRÁFICAS NOS ESTADOS UNIDOS

BELO HORIZONTE
2018

UNIVERSIDADE FEDERAL DE MINAS GERAIS
FACULDADE DE FILOSOFIA E CIÊNCIAS HUMANAS
BACHARELADO EM ANTROPOLOGIA – ANTROPOLOGIA SOCIAL

GUSTAVO RAMOS RODRIGUES

A LIBERDADE É A CHAVE: UMA ETNOGRAFIA MULTISSITUADA DAS GUERRAS CRIPTOGRÁFICAS NOS ESTADOS UNIDOS

Monografia de conclusão de curso apresentada como requisito parcial para a obtenção do título de bacharel em Antropologia com habilitação em Antropologia Social pela Faculdade de Filosofia e Ciências Humanas da Universidade Federal de Minas Gerais

Orientadora: Érica Renata de Souza

BELO HORIZONTE
2018

GUSTAVO RAMOS RODRIGUES

A LIBERDADE É A CHAVE:
UMA ETNOGRAFIA MULTISSITUADA DAS GUERRAS CRIPTOGRÁFICAS NOS ESTADOS UNIDOS

Monografia de conclusão de curso apresentada como requisito parcial para a obtenção do título de bacharel em Antropologia com habilitação em Antropologia Social pela Faculdade de Filosofia e Ciências Humanas da Universidade Federal de Minas Gerais

Data: 12/12/2018

Nota: 100

Conceito: A

BANCA EXAMINADORA

Profa. Dra. Érica Renata de Souza – Orientadora

Universidade Federal de Minas Gerais

Prof. Dr. Marco Antônio Sousa Alves – Avaliador

Universidade Federal de Minas Gerais

No final do século XX, neste nosso tempo, um tempo mítico, somos todos quimeras, híbridos – teóricos e fabricados – de máquina e organismo; somos, em suma, ciborgues. O ciborgue é nossa ontologia; ele determina nossa política. O ciborgue é uma imagem condensada tanto da imaginação quanto da realidade material: esses dois centros, conjugados, estruturam qualquer possibilidade de transformação histórica.

Donna Haraway

AGRADECIMENTOS

A Odélia por sua força, coragem e competência que me serão eterno exemplo. Por sua paciência, dedicação e amor incondicionais. Por ter acreditado em mim no fim de 2013 e por tudo mais que jamais conseguirei expressar independente do número de linhas do agradecimento.

A Léon e Julia por seus exemplos, por seu apoio e zelo.

A Fábio pelo apoio durante a escrita, pela paciência e por um amor de carinho, respeito e cuidado.

A Érica pelas aulas e por ter me acolhido e acompanhado generosamente durante toda a graduação.

A Marco pelas eventuais trocas e ensinamentos a respeito dos temas deste trabalho e pela gentileza de aceitar participar da banca.

A Karenina pelas aulas e por seu suporte que me manteve no curso num momento difícil.

A Yurij pelas aulas, pela paciência, pelos diálogos e pelos comentários sobre este trabalho.

A Carol e Marlon pelos anos de amizade e por permanecerem comigo, apesar do tempo e da distância.

A Ana pelos anos de amizade, pelo apoio, pelas trocas, discussões e risadas.

A Lucas e Davi, por serem amigos fofos e inspiradores que me apresentaram o universo de políticas da internet.

Às amigas e amigos do GNet e do IRIS, em especial Paloma, Victor, Mari e Pedro, pelos roles, piadas ruins, ensinamentos sobre direito e trocas sobre governança da internet.

Às amigas e amigos do InCiTe, em especial Victor, Brunah e Carol, pelos aprendizados e por compartilharem as dores e delícias da pesquisa em ciência e tecnologia.

A Nath e Ju pela inspiração, pelo apoio e pelo companheirismo nas matérias boas e ruins.

A Isadora, Lara, Flora, Caio e Luan, pelas noites de conversas, risos e pitangas choradas.

A Maria, Florencia, Iago e Luis Felipe pelas amizades e pelos aprendizados conjuntos em antropologia e antropologia da ciência.

A Ítalo e Daniel por me ensinarem muito mais do que eu poderia retribuir.

A Márcia por salvar minha vida com sua competência e sensibilidade.

A Ângela pela competência e pelo auxílio durante toda a graduação.

A Diego por comentários gentis que influenciaram bastante o produto final deste texto.

RESUMO

O presente trabalho investiga conflitos relativos ao acesso público à tecnologias de encriptação forte nos Estados Unidos ao longo das últimas três décadas, as chamadas guerras criptográficas (*crypto wars*). Buscou-se mapear os principais atores envolvidos, seus interesses, argumentos e ações relativas aos conflitos em questão. O recorte do trabalho consistiu nos seguintes contextos: i) as disputas em torno da implementação do chip *Clipper*, o qual tornaria os celulares dos usuários vulneráveis à decifragem de suas comunicações por parte do governo federal, entre os anos de 1993 e 1996; ii) a contenda entre a empresa Apple e a Agência Federal de Investigação (FBI) em 2016 acerca do desbloqueio do iPhone de um dos terroristas responsáveis pelo atentado de San Bernardino ao fim de 2015. O contexto prévio ao caso *Clipper* e desdobramentos relevantes ocorridos entre os dois conflitos também foram incluídos na descritiva a fim de tornar inteligíveis as conexões, transformações, continuidades e descontinuidades entre os dois casos analisados. O método adotado para a pesquisa foi a etnografia multissituada, a qual se empreendeu a partir de *snowballing* documental que ensejou a formação de um extenso corpus de documentos técnicos, jurídicos, jornalísticos e de declarações públicas dos atores envolvidos. Os dados foram analisados à luz de um arcabouço teórico híbrido cujo eixo comum foi a influência do pós-estruturalismo francês e a tematização dos processos de subjetivação no neoliberalismo, bem como contribuições dos estudos de securitização e de vigilância. Dentre as conclusões alcançadas estão: i) a corroboração da hipótese de Rider segundo a qual os fatores definidores das posturas e ações dos principais atores envolvidos no debate eram o interesse estatal na expansão da vigilância e o interesse mercadológico em garantir um ambiente não-regulado; ii) o principal discurso responsável pela suposta derrota do setor estatal nos conflitos foi estruturado em torno de uma versão neoliberal da categoria liberdade em que liberdade política é associada a liberdade de mercado; iii) na ausência de um impacto econômico negativo visível, o setor privado esteve perfeitamente confortável em fornecer sistemas inseguros aos usuários para garantir acesso estatal irregular; iv) a publicização dessas práticas após as revelações de Edward Snowden tornou a privacidade economicamente explorável e reintroduziu um motivador econômico para que as guerras criptográficas fossem retomadas.

Palavras-chave: *crypto wars*; vigilância; tecnopolítica; neoliberalismo; privacidade.

ABSTRACT

This research investigates conflicts concerning public access to strong encryption technologies in the United States over the last three decades, the so-called crypto wars. The goal was to map the main actors involved, their interests, arguments and actions related to the conflicts in question. The analytical cut of the work consisted of the following contexts: i) disputes over the implementation of the Clipper chip, which would make the users' cell phones vulnerable to the deciphering of their communications by the federal government, between 1993 and 1996; (ii) the dispute between Apple and the Federal Bureau of Investigation (FBI) in 2016 over the unlocking of the iPhone from one of the terrorists responsible for the San Bernardino bombing at the end of 2015. The background to the Clipper case and relevant developments between the two conflicts were also included in the descriptive in order to make the connections, transformations, continuities, and discontinuities between the two cases analyzed intelligible. The method adopted for the research was the multisited ethnography, which was undertaken from documentary snowballing that led to the formation of an extensive corpus of technical, legal, journalistic and public statements documents of the actors involved. The data were analyzed in the light of a hybrid theoretical framework whose common axis was the influence of French poststructuralism and the thematization of the processes of subjectivation in neoliberalism, as well as contributions from securitization and surveillance studies. Among the conclusions reached are: i) corroboration of Rider's hypothesis according to which the defining factors of the positions and actions of the main actors involved in the debate were the state interest in the expansion of vigilance and the market interest in guaranteeing a non-regulated environment; ii) the main discourse responsible for the alleged defeat of the state sector in the conflicts was structured around a neoliberal version of the category of freedom in which political freedom is associated with market freedom; iii) in the absence of a visible negative economic impact, the private sector has been perfectly comfortable in providing unsecured systems to users to ensure irregular state access; iv) publicizing these practices after the revelations of Edward Snowden made privacy economically exploitable and reintroduced an economic motivator for cryptographic wars to be retaken.

Keywords: Crypto Wars; Surveillance; Privacy; Technopolitics; Neoliberal governmentality

SUMÁRIO

INTRODUÇÃO – EM BUSCA DE UMA FICÇÃO PERSUASIVA

0.1 A antropologia diante do espelho

A inspiração para o desenvolvimento do presente trabalho está associada a dois movimentos políticos e epistemológicos que emergiram e ganharam grande notoriedade na antropologia ao longo das últimas cinco décadas. Esses movimentos não correspondem exatamente a duas escolas de pensamento ou dois *corpora* discretos de produção acadêmica. Trata-se antes de dois conjuntos de linhas paralelas e heterogêneas de ação e pensamento. Algumas dessas linhas convergem aqui e separam-se acolá, outras assumem caminhos opostos e jamais sequer interagem, transformando-se em linguagens mutuamente ininteligíveis. Outras interagem continuamente, mas em franco conflito que permeia artigos, reuniões departamentais e palestras. O ponto comum a ambos os movimentos, a meu ver, consiste em colocar a própria antropologia sob exame.

Um deles é o que Gabriela Coleman (2012, p. 4), etnógrafa do hacktivismo, classifica, a meu ver acertadamente, como uma "virada crítica na antropologia". O termo indica a ascensão de uma série de debates que marcaram a antropologia, sobretudo a estadunidense, ao longo da segunda metade do século XX. Me refiro aqui à leva de discussões iniciada já no final da década de 1960 com o declínio do estruturalismo e a publicação dos diários pessoais de Malinowski, passando pela ascensão da antropologia simbólica e pelo reaparecimento dos marxismos e feminismos antropológicos ao longo da década de 1970 e culminando com as devastadoras críticas da antropologia pós-moderna dos anos 1980.

Materializada em variados graus e com ênfases distintas nas produções de figuras como Talal Asad, Catherine Lutz, Sandra Morgen, Laura Nader, Eric Wolf, Gayatri Spivak, George Marcus, Lila Abu-Lughod, James Clifford e Edward Said, as críticas em questão tinham seu denominador comum no questionamento de categorias basilares do dispositivo conceitual da disciplina: observação-participante, cultura, alteridade, nativo, interlocutor, etc. Dentre as principais contribuições teóricas do movimento estavam a explicitação analítica dos mecanismos de produção da autoridade etnográfica, a denúncia dos efeitos coloniais da forma como a noção de cultura era empregada pela disciplina e a identificação das conexões entre esses pontos e a omissão histórica da antropologia em relação a temas como colonialismo, capitalismo, poder e classe.

Os efeitos epistemológicos desse momento de efervescência crítica foram de uma capilaridade imensa. As fronteiras disciplinares às quais a antropologia (ainda) é tão apegada foram se tornando mais porosas conforme um universo de debates, teorias, e métodos previamente marginalizados pelo cânone da disciplina ganhava uma nova legitimidade acadêmica. Podia-se experimentar e até mesmo reinventar a etnografia malinowskiana, como diversos autores fariam durante esses anos e os anos subsequentes.

Laura Nader (1972) colocou em questão o impacto das relações de poder entre etnógrafo e etnografados, provocando a antropologia a olhar para cima e para os poderosos. George Marcus (1995) descreveu a etnografia multissituada e mostrou sua potência para conectar práticas locais a processos macroteóricos a partir de articulação entre observação-participante e fontes variadas por meio das quais se poderia seguir interações entre atores dispersos no tempo e no espaço. Susan Star (1999) demonstrou a proficuidade do exercício de direcionamento do olhar etnográfico para as infraestruturas, sobretudo na medida em que seria possível politizar sua arquitetura a partir da desnaturalização de sua invisibilidade cotidiana. Peirano (2014), por sua vez, sintetizou a porosidade das fronteiras que separam o momento etnográfico do resto do cotidiana do etnógrafo na contundente declaração: "etnografia não é método".

Assim, na década atual, Coleman (2010) pode ofertar uma disciplina optativa denominada *Anthropology of hackers* na New York University e eu posso tematizar conflitos sociotécnicos envolvendo criptografia em minha monografia de conclusão de curso. Isso se deve, em boa medida, ao trabalho teórico, metodológico e político levado a cabo pelas autoras e autores supracitados. Seria impreciso, contudo, deixar de fazer referência ao outro movimento que mencionei em meu parágrafo inicial, uma vez que este tem peso igual no desenvolvimento desta pesquisa.

Se a virada crítica na antropologia tem um de seus núcleos na problematização da categoria cultura, pode-se dizer que o outro movimento – o qual ainda tenho certa dificuldade de nomear – se desenvolve a partir de uma problematização da relação entre a cultura e seu correlato: a natureza. Essa empreitada, levada a cabo simultaneamente por esforços dos estudos sociais da ciência e tecnologia, da etnologia indígena e dos estudos de gênero, encontra-se corporificada em figuras como Bruno Latour, Donna Haraway, Marilyn Strathern, Roy Wagner, Annemarie Mol, Eduardo Viveiros de Castro, Sandra Harding, Isabele Stengers, Jasbir Puar, Karen Barad, Paul B. Preciado, dentre outros. O espírito geral

deste tipo de movimentação está associado ao que tem sido chamado de uma "virada material" (ALAIMO e HEKMAN, 2008, p. 6) na teoria feminista e de virada ontológica na antropologia.

Na antropologia, a questão emerge de um dos binários fundamentais da disciplina: natureza e cultura. A etnologia estudaria e compararia as culturas, tendo como pano de fundo comum a todas elas o partilhamento de uma mesma natureza humana. A cultura seria da ordem do múltiplo, do construído, do variável, do particular, da crença, da política e da representação. A natureza seria da ordem do um, do dado, do invariável, do universal, do fato, da técnica e do objeto. Em síntese: a cultura é ideal e a natureza é materialidade. O conhecimento científico, por sua vez, seria um canal de acesso a essa materialidade pré-existente. O método científico seria um mecanismo de remoção do véu da cultura, o qual permitiria acessar a natureza tal como ela é.

Os problemas desse modelo foram tópico de múltiplas discussões na segunda metade do século XX. Diálogos entre as etnologias ameríndia e melanésia se pautaram cada vez mais pelo reconhecimento da pobreza analítica do binário natureza x cultura para a compreensão dos universos ameríndio e melanésio. A antropologia foi confrontada com o fato da díade natureza x cultura ser um produto específico da cultura euroamericana, um instrumento conceitual cujo emprego irrefletido aparecia como obstáculo para a compreensão das realidades de outros povos. Isso não significou a negar a natureza, mas passá-la do um ao múltiplo ao reconhecer uma multiplicidade de mundos possíveis que não podem simplesmente ser reduzidos a representações da natureza.

Paralelamente, o programa forte da sociologia do conhecimento desafiou a ideia de que ao sociólogo do conhecimento competiria somente explicar os erros científicos, enquanto os acertos seriam tratados quase como o simples resultado da boa aplicação do método. As consequências dessa proposição foram radicalizadas pela Teoria do Ator-Rede, a qual buscou demonstrar ativamente como os fatos científicos são produzidos e mantidos estáveis por redes fractais conformadas pelas interações entre atores humanos e não-humanos. O projeto nesse caso também não foi de negação da facticidade da ciência, mas de complexificar as relações entre técnica e política, entre objetividade e experiência vivida.

A versão mais potente deste argumento geral foi enunciada, a meu ver, por Donna Haraway (2000, p. 36) no que foi indubitavelmente o texto mais importante de minha graduação:

> A ironia tem a ver com contradições que não se resolvem – ainda que dialeticamente – em totalidades mais amplas: ela tem a ver com a tensão de manter juntas coisas incompatíveis porque todas são necessárias e verdadeiras. A ironia tem a ver com o humor e o jogo sério. [...] No centro de minha fé irônica, de minha blasfêmia, está a imagem do ciborgue. Um ciborgue é um organismo cibernético, um híbrido de máquina e organismo, uma criatura de realidade social e também uma criatura de ficção. Realidade social significa relações sociais vividas, significa nossa construção política mais importante, significa uma ficção capaz de mudar o mundo. Os movimentos internacionais de mulheres têm construído aquilo que se pode chamar de "experiência das mulheres". Essa experiência é tanto uma ficção quanto um fato do tipo mais crucial, mais político. A libertação depende da construção da consciência da opressão, depende de sua imaginativa apreensão e, portanto, da consciência e da apreensão da possibilidade. O ciborgue é uma matéria de ficção e também de experiência vivida – uma experiência que muda aquilo que conta como experiência feminina no final do século XX. Trata-se de uma luta de vida e morte, mas a fronteira entre a ficção científica e a realidade social é uma ilusão ótica. A ficção científica contemporânea está cheia de ciborgues – criaturas que são simultaneamente animal e máquina, que habitam mundos que são, de forma ambígua, tanto naturais quanto fabricados. A medicina moderna também está cheia de ciborgues, de junções entre organismo e máquina, cada qual concebido como um dispositivo codificado, em uma intimidade e com um poder que nunca, antes, existiu na história da sexualidade.

Nos estudos de gênero, a década de 1980 foi marcada por uma problematização de sua própria versão do binário natureza x cultura: o binário sexo x gênero. A denúncia histórica do caráter socialmente construído da dominação masculina estava apoiada na naturalização do sexo, o que tinha por efeito implícito reificar uma identidade política fixa comum às mulheres. A naturalização dessa identidade poderia mascarar outras matrizes de dominação, como as baseadas em raça e classe, bem como tornar invisíveis as complexas interações entre práticas médicas, jurídicas, midiáticas e outras cujo efeito é a estabilização do sexo. Se algumas versões da teoria *queer*[1] haviam transformado o gênero e o sexo em efeitos de atos discursivos, Haraway simetrizou o discurso e a materialidade em sua análise.

Sendo ela própria um híbrido (sua graduação foi tripla: filosofia, zoologia e literatura), a biofilósofa emprega, com declarada ironia, o ciborgue como a perfeita imagem de seu

[1] Esta é a conhecida crítica de Preciado (2014) a Judith Butler. É necessário observar, todavia, que a filósofa refinou sua análise ao longo dos anos, oferecendo maior atenção à materialidade do corpo em textos mais recentes. A esse respeito, ver a entrevista dada por Butler a Prins e Meijer (2002).

argumento. Sendo simultaneamente real e ficcional, natural e produzido, sujeito e objeto, , o ciborgue é uma imagem e um fato que torna perfeitamente visível o ponto fundamental. As experiências comuns de sujeitos políticos são fatos tão reais e tão produzidos, materiais e discursivos, assim como o fatos fatos da seleção natural e da reprodução. A ciência é produzida por sujeitos dotados de corpos situados no tempo e no espaço em interação com as tecnologias de visualização específicas, o que não significa que o conhecimento científico seja subjetivo e falso, mas que ele a própria oposição é simples demais para descrevê-lo.

0.2 Arquitetura desta ficção

Considerei necessário falar sobre os dois movimentos em questão por dois motivos. O primeiro deles diz respeito à imensa influência de ambos os *corpora* de produção acadêmica em minha formação acadêmica e pessoal. O convite de Laura Nader a empreender uma antropologia que olhasse para cima e não somente para baixo, para os poderosos e não somente para os marginalizados, foi uma referência importante na definição do tema desta pesquisa. As reflexões de James Clifford (1998) e Marilyn Strathern (2013) a respeito da dimensão literária-ficcional do texto etnográfico e das diferentes possibilidades de mobilização dos contextos etnográficos para a produção de eficácia epistemológica também me influenciaram significamente. Tenho, por conseguinte, preocupações literárias e científicas que atravessam este texto.

Isso não significa abrir mão do ideal de objetividade, como tem sido demonstrado pelas contribuições de figuras como Donna Haraway (op cit.), Bruno Latour (1994), Susan Star (op. cit.) e Annemarie Mol (1999; 2002). Assim, outra das posições que informa esse texto é a de rejeitar tanto o grande divisor moderno entre matéria e espírito quanto as tentativas de corrigi-lo através da redução da coisa à palavra. Explicito o caráter ficcional deste trabalho para torná-lo mais objetivo, não menos. Meu objetivo é persuadir eventuais leitoras e leitores de que o apresentado aqui constitui construção literária e representação factual, posicionamento político e comentário técnico, humor e jogo sério.

Para fazê-lo, é necessário que tal empreitada seja traduzível numa linguagem acadêmica formal, empreendimento para o qual me volto nas próximas linhas. O presente trabalho consiste numa etnografia multissituada das chamadas guerras criptográficas nos Estados Unidos. O termo “guerras criptográficas “ (*crypto wars*) é popular entre ativistas,

pesquisadores e jornalistas de tecnologia da informação para designar uma série de conflitos relativos à regulação do acesso público à certas tecnologias de encriptação nos fins do século XX. Uma vez que esses conflitos existem em fluxos de interações entre atores[2] heterogêneos (ONGs, instituições policiais, empresas, *experts*, etc) e dispersos no tempo e no espaço, foi necessário estabelecer um recorte mais específico.

O recorte inicial foi o de duas grandes disputas de grande expressão pública que marcaram tais conflitos nos Estados Unidos: os debates públicos em torno do chip *Clipper* durante a década de 1990 e a contenda entre a empresa Apple e a Agência Federal de Investigação (FBI) em 2016. As conexões entre os dois casos foram se tornando mais etnograficamente relevantes no decorrer da pesquisa, o que levou à inclusão do período entre os casos no escopo da análise.

O objetivo geral da investigação foi cartografar as racionalidades que informaram os atores nos conflitos em questão, com ênfase nas relações entre enunciados e práticas dos atores envolvidos. Os objetivos específicos foram: i) identificar os principais atores envolvidos em ambos os conflitos; ii) mapear seus principais interesses e como esses se convergiam ou divergiam contextualmente; iii) caracterizar os argumentos mobilizados para a realização desses interesses; iv) relacionar tais argumentos com as práticas nas quais os atores se engajaram ao longo dos conflitos, em especial na medida em que tais práticas foram exercidas por meio de escolhas técnicas; v) visibilizar os efeitos objetivos das escolhas técnicas nas interações entre os atores.

As fontes etnográficas foram levantadas a partir do método de *snowballing* (SCHULZE, 2017, p. 56), o que resultou no extenso corpus documental que compõe as referências deste trabalho, o qual consiste em matérias jornalísticas, transcrições de audiências públicas, documentos judiciais do caso Apple v. FBI, vídeos contendo declarações de atores envolvidos, textos científicos publicados pelos atores envolvidos, *white papers* de segurança descrevendo o funcionamento da encriptação do iPhone e comunicados oficiais dos atores.

[2] Embora algumas das contribuições de Bruno Latour sejam inspirações teórico-metodológicas para o presente trabalho, o que se faz aqui não é um mapeamento de controvérsias sociotécnicas no sentido estrito e associado à Teoria do Ator-Rede do termo. Como escolha metodológica, utilizo aqui o termo ator para me referir a atores que Latour caracterizaria como humanos: *experts*, instituições, empresas, etc. Como previamente comentado, isso não significa ignorar que os campos de ação desses atores sejam conformados pelo impacto de elementos não-humanos.

Além disso, enquanto desenvolvia esta pesquisa passei a fazer parte de uma comunidade envolvida com discussões de Governança da Internet na qual debates referentes à encriptação não são incomuns. Ao frequentar eventos como a *Cryptorave* brasileira e o Fórum da Internet no Brasil, tive a oportunidade de me familiarizar com aspectos técnicos da discussão, dialogar com outras pessoas sobre esses temas e receber indicações de referências com as quais não tinha familiaridade. Não obstante a ausência de referências pontuais e explícitas a essas experiências ao longo do texto, seus efeitos atravessam a perspectiva etnográfica que o envolve inteiramente. Nesse sentido, me apoio nas reflexões de Peirano sobre a dificuldade em separar o momento etnográfico do momento não-etnográfico quando a antropologia nos treina a produzir esse tipo de reflexão sobre nossos encontros.

Se os movimentos teóricos e epistêmicos mencionados na seção anterior forneceram bases teórico-metodológicas implícitas no trabalho, o arcabouço teórico ao qual recorro explicitamente aparece no primeiro capítulo intitulado "Ovelhas, ciborgues e homossexuais". Nesse capítulo, busco reconstituir algumas das principais contribuições da fase genealógica da obra do filósofo francês Michel Foucault a respeito dos temas: punição soberana, poder disciplinar, poder pastoral, razão de Estado, polícia, dispositivo da sexualidade, liberalismo e neoliberalismo. Embora a descrição do trabalho de Foucault não seja de modo algum exaustiva, optei por dedicar ao pensador em questão a maioria das páginas do capítulo.

Essa escolha se deu em função de dois elementos específicos. Em primeiro lugar, a vasta maioria dos autores dos quais fiz uso encontra-se em diálogo explícito com algum aspecto da obra de Foucault, seja para complementá-lo, criticá-lo ou mesmo repudiar suas análises. Em segundo lugar, ambos os movimentos supra descritos incorporam premissas foucaultianas: seja pela centralidade que a tópica das relações entre técnica e política ganha em sua obra, seja pela importância de sua analítica do poder para um entendimento dos mecanismos pelos quais o indivíduo é produzido e feito obedecer na modernidade, inclusive por meio da vigilância. Em adição, acredito que haja um potencial grande para análises ricas ao se relacionar a discussão de Foucault sobre racionalidades governamentais liberais e neoliberais com contextos empíricos concretos atravessados por tais racionalidades. Na seção final do capítulo "Sonhos de andróides", utilizo uma leva de autores mais recentes para oferecer complementos e contrapontos à análise empreendida por Foucault a respeito das relações entre poder pastoral, mercado e governo no neoliberalismo.

O capítulo "O paradoxo das folhas de chá" corresponde à análise e discussão do caso *Clipper*. Para esse fim, apresento alguns elementos das políticas de encriptação e das políticas criminais identificáveis na sociedade estadunidense, sobretudo na segunda metade do século XX. Essa contextualização visa situar o contexto no qual o governo Clinton tentou passar o projeto *Clipper*, iniciativa que deflagrou as guerras criptográficas dos anos 1990. Apresento também o funcionamento técnico do *Clipper* para tornar visíveis as intencionalidades materializadas no sistema e os efeitos políticos que sua infraestrutura teria para o debate. Reconstituo os principais atores e discursos que marcaram os conflitos entre 1993 e 1996, bem como desdobramentos subsequentes ao longo da segunda metade da década. Esse capítulo se apoia primariamente em estudos científicos sobre o conflito, mas os complementa com dados de fontes jornalísticas e documentais.

Finalmente, o capítulo final, "Em Nome da América", apresenta inicialmente alguns processos que influenciaram a trajetória das tecnologias de encriptação nos EUA entre 2000 e 2013. As revelações de Edward Snowden sobre os programas de vigilância massiva dos EUA e seus impactos são rememorados para que então se introduza a descrição do caso Apple v. FBI. Foi sobre o caso em questão que investi a maior parte do trabalho empírico realizado aqui. Um grande número de referências do corpus documental supracitado é mobilizado para se mostrar as estratégias, ações e argumentos adotados pelos atores envolvidos no caso em questão. Concluo o capítulo em questão com uma ponderação sobre as continuidades e descontinuidades das guerras criptográficas entre os anos 1990 e a contenda em questão.

0.3 Decifrar a tecnicidade

Para familiarizar eventuais leitoras e leitores com o jargão técnico da criptografia, tento introduzir nas próximas páginas os principais termos que serão acionados com frequência ao longo deste trabalho:

Encriptação ou **cifragem** consiste no processo de transformação de texto inteligível em ininteligível através da aplicação de algum algoritmo[3] aos dados que se deseja cifrar. A menos que haja uma vulnerabilidade no sistema, informação cifrada só pode ser acessada por

[3] Em termos extremamente gerais e didáticos, um algoritmo pode ser definido como uma sequência finita de instruções bem definidas, usualmente para a execução de um objetivo. Um algoritmo não está necessariamente ligado a um programa de computador. Receitas culinárias e instruções para procedimentos burocráticos são exemplos de algoritmos que permeiam a vida cotidiana.

meio da reversão dos procedimentos utilizados na encriptação - processo conhecido como decriptação ou **decifragem**. Para os fins deste trabalho, os termos "dados", "informação" e "texto" serão utilizados de forma intercambiável, a fim de designar qualquer conteúdo comunicado ou e/ou armazenado na forma de algum tipo de escrita.

A cifragem usualmente é explicada a partir de exemplos em que uma parte A tenta se comunicar com uma parte B por um canal inseguro no qual as comunicações estão sujeitas a interceptação por um *eavesdropper*("bisbilhoteiro"). Imaginemos, portanto, que a jovem **A**lice deseja se comunicar com seu amigo **B**ob através de um canal sujeito a interceptação por parte da *eavesdropper* Eve. Neste exemplo, Eve seria uma **adversária**, termo de segurança da informação que denota uma entidade interessada em violar um certo objetivo de segurança. Essa entidade nem sempre é um indivíduo, pode ser uma empresa, um Estado, um grupo criminoso, etc.

Para garantir a confidencialidade de sua mensagem, Alice resolve cifrá-la. Suponhamos que a mensagem seja a palavra "antropologia". Essa informação original não cifrada ("antropologia") é chamada de texto plano. Alice aplica a seu texto plano o procedimento de substituir cada letra por outra letrada situada um número x de posições depois dela na ordem alfabética. Assim, se o valor de x for 1, Alice substituirá cada letra pela seguinte, de modo que seu texto plano ("antropologia") seja cifrado como "bouspqpmphjb". Se esse valor for 2, "antropologia" se transformará em "cpvtqrqnqikc" e assim sucessivamente.

Para os fins desse exemplo, imaginaremos que Alice havia acordado previamente com Bob o uso do número 7 como valor de x, portanto seu texto cifrado será "huayvwvsvnph" e que a mensagem cifrada foi entregue com sucesso a Bob, mas Eve conseguiu uma cópia dela.

Bob sabe quais procedimentos foram utilizados para cifrar o texto, ou seja, Bob sabe qual foi o algoritmo de cifragem utilizado. Em nosso exemplo, Alice fez uso de um dos mais simples existentes: a cifra de César[4]. Imaginemos que Eve também consegue descobrir o algoritmo utilizado após estudar o texto e perceber um certo padrão. Agora tanto Bob quanto Eve são capazes de deduzir facilmente a sequência de procedimentos necessária para reverter o procedimento de cifragem utilizado, ou seja, são capazes de deduzir o algoritmo de

[4] O nome advém do imperador romano Júlio César que, em tese, faria uso desse algoritmo para assegurar a confidencialidade de suas comunicações. Para uma discussão mais aprofundada sobre o uso de encriptação na antiguidade, ver Singh (2000).

decifragem. Basta substituir substituir cada letra do texto cifrado por outra situada um número *x* de posições antes dela na ordem alfabética.

Mas há uma diferença crucial entre Eve e Bob. Enquanto ela sabe somente o algoritmo utilizado, ele tem acesso a uma informação adicional: Bob sabe que o valor de *x* é 7, pois esse valor foi acordado previamente entre ele e Alice. Em outras palavras, Bob tem acesso à **chave de decifragem**, o dado que efetivamente possibilita a ele decifrar a mensagem em tempo hábil. Ao aplicar essa chave de decifragem (7) ao algoritmo de decifragem descrito acima, Bob transforma o texto cifrado ("huayvwvsvnph") em texto plano ("antropologia") novamente, ganhando assim acesso à informação que Alice deseja comunicar.

Nota-se, portanto, a importância do gerenciamento de chaves para qualquer sistema criptográfico. Em criptografia, uma chave é um dado utilizado como parâmetro na execução de um algoritmo de cifragem e/ou decifragem para controlar o resultado concreto de sua operação. Se a mesma chave for utilizada para a cifragem e decifragem do texto, como em nosso exemplo (em que a chave é o número 7), trata-se de um sistema de **encriptação simétrica**. Sistemas criptográficos baseados nesse tipo de encriptação apresentam, contudo, alguns problemas importantes quanto ao gerenciamento de chaves.

O mais básico deles deriva do fato da mesma chave ser utilizada para cifrar e decifrar o texto, pois um adversário que consiga essa chave normalmente não vai avisar às partes da comunicação que a obteve. Isso coloca um dilema: trocar ou não trocar a chave periodicamente? Se a mesma chave for mantida, há o risco de algum adversário que a tenha obtido interceptar todas as comunicações. Se a chave for trocada, como uma parte comunica a chave nova à outra parte? Enviar uma mensagem pelo sistema que potencialmente já foi comprometido?

Essa questão afetou usuários de sistemas criptográficos durante séculos, dentre eles lideranças militares e chefes de Estado. A solução mais utilizada envolvia algo que se chamava "centro de distribuição de chaves" ou "repositório de gerenciamento de chaves", o que fundamentalmente consistia na introdução de um "terceiro de confiança" no sistema. Esse terceiro ficaria responsável por gerar uma chave nova para cada sessão de comunicações cifradas. Essa solução era insatisfatória, todavia, pois a introdução de uma parte adicional implica num novo foco potencial de vulnerabilidades exploráveis por adversários, o que reduz intrinsecamente a segurança do sistema.

Foi a esse problema que os pesquisadores Whitfield Diffie e Martin Hellman buscaram solucionar com suas pesquisas na virada da década de 1960 para 1970, as quais culminaram na publicação do artigo "*New directions in cryptography*" no periódico IEEE Transactions on Information Theory em 1976. A novidade introduzida por eles consistiria num método de distribuição de chaves que permitiria a criação de sistemas cifrados nos quais o terceiro de confiança seria desnecessário. Seu método, em linhas gerais, teria o seguinte funcionamento:

Cada usuário teria duas chaves. Tudo que uma delas cifrasse, a outra decifraria, mas nenhuma delas seria capaz de realizar os dois procedimentos. A chave de cifragem poderia ser divulgada amplamente sem comprometer a segurança do sistema e por esse motivo seria conhecida como chave pública. A chave de decifragem deveria ser mantida somente com o usuário e por isso seria chamada de chave privada. Se Alice quisesse enviar uma mensagem para Bob, ela utilizaria a chave pública de Bob para cifrar a mensagem e o rapaz faria uso de sua própria chave privada para decifrá-la. Para responder, Bob similarmente cifraria a mensagem com a chave pública de Alice e ela decifraria a mensagem com sua própria chave privada. Esse método passou a ser conhecido como encriptação de Diffie-Hellman, **encriptação assimétrica**[5] ou encriptação de chave pública.

A encriptação é comumente metaforizada como o trancamento da informação, de modo que somente aqueles que detenham acesso à chave possam acessá-la. Essa metáfora aparece, por exemplo, no conceito de ***backdoor***[6], o qual denota uma vulnerabilidade num sistema que permite contornar os mecanismos convencionais de segurança. A metáfora do trancamento evidencia a importância do gerenciamento de chaves em qualquer sistema criptográfico: o acesso à chave de decifragem, e nenhum outro, deve ser o elemento definidor do acesso ao texto plano. Em sistemas contemporâneos e de maior complexidade, este raciocínio é usualmente expresso no chamado princípio de Kerckhoffs[7]: deve-se assumir que um adversário conhece a totalidade do sistema, exceto a chave de decifragem.

[5] Uma vez que a finalidade desta seção é apresentar didaticamente o jargão técnico da criptografia, apresentei o desenvolvimento da encriptação assimétrica de forma extraordinariamente simplificada. Para uma narrativa mais sofisticada, ver Levy (2001).

[6] O termo, que normalmente não é traduzido, metaforiza uma situação na qual alguém utiliza uma porta dos fundos destrancada para acessar um espaço cujo acesso autorizado deveria ocorrer por porta dianteira.

[7] Esta lei ou princípio é de fato o produto de interpretações derivadas de um conjunto de condições estabelecidas pelo engenheiro holandês August Kerckhoffs como sendo "desejáveis à criptografia militar, no século XIX". (REZENDE, 2009, p. 1)

Para retomar nosso exemplo, Eve e Bob conhecem igualmente os algoritmos de cifragem e decifragem do sistema, mas somente ele tem acesso à chave. Isso não necessariamente significa que Eve desistirá de obter acesso não-autorizado ao texto plano. Ela poderá, como alternativa, tentar obter esse acesso por meio de **criptoanálise** - termo que designa o repertório de práticas e saberes relativos à obtenção de acesso não-autorizado a texto plano sem que se conheça inicialmente a chave ou senha necessária para a decifragem.

Eve poderia, por exemplo, aplicar um dos ataques criptoanalíticos mais simples existentes: o **ataque de força bruta** ou busca exaustiva de chave. Esse ataque consiste simplesmente em tentativa e erro: o adversário testa sistematicamente todas as chaves ou senhas possíveis até obter a correta. Ela tentaria decifrar a mensagem usando o número 1 como chave, depois o número 2 e assim sucessivamente até suceder em sua sétima tentativa, o que não demoraria muito tempo devido à fraqueza do sistema utilizado. Em tese, o ataque de força bruta pode ser utilizado para quebrar qualquer criptosistema existente. Na prática, contudo, o tempo e os recursos computacionais necessários para quebrar sistemas contemporâneos frequentemente tornam o uso desse método inviável ou ineficaz.

Isso porque muitos dos sistemas contemporâneos utilizam **encriptação forte**. Um criptosistema é considerado forte ou, para ser mais tecnicamente preciso, computacionalmente seguro se ele não puder ser quebrado em tempo hábil com os recursos computacionais disponíveis no presente ou em um futuro próximo. As noções de "tempo hábil" e de "recursos computacionais disponíveis no presente ou em um futuro próximo" estão sujeitas a interpretação. Em muitos casos, no entanto, não é raro que o tempo estimado para a quebra de um criptosistema forte seja de alguns milhares de anos, mesmo o atacante dispondo dos recursos computacionais de uma potência militar.

À luz dessa imperfeita exposição, posso finalmente aterrissar na definição de **criptografia** como sendo o campo de saberes e práticas referentes aos princípios, métodos e técnicas relativos a sistemas voltados à cifragem, gerenciamento de chaves e decifragem da informação. Escolhi apresentar tal definição tardiamente no texto como estratégia para justificar algumas das escolhas terminológicas que orientam a produção desta análise, sobretudo a escolha de distinguir terminologicamente a cifragem (processo) da criptografia (campo).

Destaco essa escolha porque esses termos não raramente são empregados como sinônimos devido à centralidade do processo de encriptação para o campo da criptografia. Na

língua inglesa, o debate público faz muito mais referências ao termo *encryption* e suas variações que ao termo *cryptography* (criptografia). Fala-se sobre *encrypted data* (dados cifrados), *encrypting information* (cifrar a informação), *strong encryption* (encriptação/cifragem forte) e *encryption algorithm* (algoritmo de cifragem). No Brasil, por outro lado, essa palavra raramente é utilizada. Emprega-se quase que exclusivamente o termo criptografia para se referir tanto ao campo quanto ao processo. Assim sendo, seria normal traduzir os termos anglófonos supracitados por dados criptografados, criptografar a informação, criptografia forte e algoritmo criptográfico, respectivamente. Este último adjetivo é a razão de minha escolha em distinguir encriptação de criptografia neste trabalho, não obstante as convenções da língua portuguesa.

Isso porque, conforme previamente asseverado, o campo da criptografia comporta conceitualmente tanto o processo de cifragem, quanto o de decifragem. Tratar criptografia e cifragem/encriptação como sinônimos geraria ambiguidade na adjetivação "criptográfico", uma vez que "criptográfico" poderia ser tanto algo relativo à encriptação, quanto algo potencialmente relativo a ambos os processos (encriptação e decifragem). Por esse motivo, estarei utilizando as locuções adjetivas "de encriptação" ou "de cifragem" no tocante ao processo e o adjetivo "criptográfico" no que se refere ao campo e/ou quando não me referir a um dos dois procedimentos especificamente.

CAPÍTULO 1 – OVELHAS, CIBORGUES E HOMOSSEXUAIS

1.1 Esvaziar o trono

O filósofo francês Michel Foucault se debruçou extensamente sobre as relações entre poder, corpo, subjetividade e verdade ao longo de sua vasta obra. Seus estudos sobre temas como loucura, sexualidade, disciplina e punição, os quais eram objeto de marginalização epistemológica nas em boa parte das ciências humanas, ofereceram um potente incentivo para a proliferação dos debates relativos a tais questões. Além disso, a originalidade metodológica de suas análises consistemente produziu insights inovadores ao longo de toda sua carreira.

Um elemento comum a todas essas análises foi o receio com o qual o pensador tratou uma série de premissas ontológicas frequentemente adotadas sem maior reflexão pelas ciências sociais tradicionais. Me refiro aqui aos grandes divisores modernos (LATOUR, 1991; GOLDMAN e LIMA, 1999; CESARINO, 2015), esse conjunto de binarismos entre termos continuamente imaginados, produzidos e atualizados como substâncias opostas: natureza x cultura, política x técnica, sujeito x objeto, humano x não-humano, indivíduo x sociedade, subjetivo x objetivo, nós x eles, self x mundo, verdade x ideologia, etc.

Foucault, leitor de Nietzsche e Espinosa e interlocutor de Deleuze, desafia repetidamente a simplicidade desse raciocínio de matriz cartesiana à luz da complexidade das relações que configuram as realidades por ele investigadas. Ele aponta a co-produção da razão e da loucura, descreve a fabricação do corpo individual, demonstra a tecnologização do governo e observa a politização dos fatos biológicos. Sua obstinada recusa em aderir aos universais não seria um deslocamento epistemológico tão audacioso e, conjecturo, impactante não fosse o fato do filósofo tê-la estendido do nível endógeno ao nível exógeno da análise.

Um dos aspectos mais intrigantes da obra foucaultiana indubitavelmente concerne o tratamento dado pelo pensador às relações entre poder e Estado. É conhecida sua rejeição tanto à concepção jurídica que compreende o poder em termos de soberania e constituição quanto à concepção marxista que o localiza no controle dos meios produtivos. Tais concepções tenderiam a tratar o poder como um objeto alienável do qual alguém (o soberano

ou a classe dominante) seria detentor e cuja expressão visível seria negativa: sua capacidade interditiva e proibitiva. Tanto na perspectiva liberal quanto na marxista, o poder acaba por ser identificado com o Estado na medida em que a tomada do Estado significa a tomada do poder.

Foucault realiza dois deslocamentos notórios em relação a essa concepção negativista e Estadocêntrica do poder. A primeira consistiu na inclusão e ênfase na positividade do poder em suas análises, em localizar os efeitos produtivos e positivos do poder. O poder é concebido então como força produtiva, como algo que produz corpos e subjetividades, algo que incita prazeres e discursos. Esse ponto encontra-se atrelado a sua concepção de governo como a conduta da conduta: ação que produz efeitos transformadores do campo de ações realizáveis por outrem. Eis o primeiro deslocamento: situar as interações produtivas realizadas nas diversas instituições (psiquiátricas, penais, educacionais) no escopo das expressões do poder.

O segundo, e talvez o mais radical, deslocamento em sua elaboração conceitual do poder está ligado a sua rejeição à compreensão do poder como objeto. O poder não é algo que se tem ou se toma, é algo que se exerce: o poder acontece. Foucault, amante das multiplicidades, esvazia o trono. Ele toma o conjunto supracitado de interações heterogêneas não como expressões do poder, mas como o próprio poder. Nessa narrativa, o poder figura como uma situação, um jogo de forças conformado por estratégias, táticas e lutas e sempre passível de mutação. Por esse motivo, o que o pensador oferece não é uma teoria do poder, mas uma analítica do poder: descrições que decompõem as interações concretas nas quais o poder é exercido. O poder não está "por trás" das coisas, ele é constitutivo dessas coisas.

Esse entendimento do poder ajuda a tornar visíveis os motivos pelos quais o autor deu atenção especial às interações difusas pelas quais o poder se exerce em sua análise. Ao comentar a escolha dos mecanismos do poder como seu objeto de pesquisa, o filósofo reflete a respeito das diferenças entre seu foco de análise e os de outras correntes de pensamento em voga na época:

> Ninguém se preocupava com a forma como ele se exercia concretamente e em detalhe, com sua especificidade, suas técnicas e suas táticas. Contentava-se em denunciá-la no "outro", no adversário, de uma maneira ao mesmo tempo polêmica e global: o poder no socialismo soviético, era chamado por seus adversários de totalitarismo; no capitalismo ocidental, era denunciado pelos marxistas como

> dominação de classe; mas a mecânica do poder nunca era analisada." (FOUCAULT, 1979, p. 7)

Há uma divisão razoavelmente consensual entre estudiosos[8] do pensamento desse autor no tocante à possibilidade de classificação de sua obra em três períodos: i) arqueologia, período marcado por investigações a respeito da constituição de certos saberes; ii) genealogia, fase em que o pensador se debruça sobre as tecnologias do poder e as formas de subjetivação a elas associadas; 3) ética, quando o autor questiona as formas de constituição do sujeito à luz das práticas de cuidado e governo de si. As fronteiras entre tais fases não são de forma alguma impermeáveis e a divisão cumpre muito mais uma função metodológica que outra coisa.

As próximas páginas deste capítulo buscarão reconstituir alguns dos argumentos desenvolvidos pelo autor durante sua fase genealógica. Os principais livros e cursos utilizados serão *Vigiar e Punir*, *Em defesa da sociedade*, *História da sexualidade I*, *Segurança, Território, População* e *Nascimento da Biopolítica.* Também serão acionados outras obras e entrevistas na medida em que delas for possível extrair comentários úteis do autor acerca de questões desenvolvidas nesse período.

1.2 O castigo impoluto

No livro *Vigiar e Punir*, Foucault investigou as transformações que caracterizaram a emergência e consolidação das práticas e racionalidades punitivas modernas. Ao descrever o regime de poder que marcava o antigo regime, Foucault fala de sociedades de soberania. A soberania consiste primariamente numa relação do soberano com a terra, o que tem como consequência, por efeito, o exercício do poder sobre a totalidade do corpo social na forma dos súditos. Não há uma grande preocupação política em conduzir atividades, em governar condutas, mas principalmente com a repressão de revoltas. Trata-se de um poder que se exerce verticalmente e de cima para baixo. O soberano poderia ordenar a morte do súdito ou deixá-lo vivo, era disso que se tratava a soberania: fazer morrer ou deixar viver.

Além disso, sua tecnologia punitiva é uma "arte das sensações insuportáveis" (FOUCAULT, 2007, p. 14). O suplício público é uma espécie de ritual político pelo qual o

[8] Ver, por exemplo, Fonseca (1995), Ferreirinha e Raitz (2010), Santos (2010) e Souza (2013), dentre outros. Para uma problematização da divisão, ver Veiga-Neto (2003).

poder do soberano se efetua: emanando a partir da realidade material do corpo do monarca e incidindo sobre o corpo do condenado na forma de dor e tortura. Tal espetáculo beligerante é o exercício primário da soberania. Longe de ser mero aditivo ou adorno ao processo penal, as etapas de sofrimento infligido ao condenado são o que o constitui e o define. A morte final, nesse caso, é apenas o desfecho desse processo de fazer morrer "mil vezes" tão caro ao poder soberano em toda sua glória repressiva.

Ao longo do século XVIII, o espetáculo da punição vai desaparecendo. Isso estaria ligado a uma mudança mais ampla no que caracteriza a justiça. A arte de sofrer essencial à soberania vai sendo substituída por uma "economia de direitos suspensos" (Ibid.). A intensidade punitiva paulatinamente dá lugar à sua fatalidade invariável enquanto mecanismo pelo qual se assegura obediência. O corpo do condenado deixa de ser o alvo do poder em si mesmo e passa a ser um intermediário entre a justiça e o sujeito jurídico punido. A punição torna-se cada vez mais limpa, científica e eficaz. Talvez a maior expressão disso seja a adoção da guilhotina como tecnologia de supressão da vida.

> Quase sem tocar o corpo, a guilhotina suprime a vida, tal como a prisão suprime a liberdade, ou uma multa tira os bens. Ela aplica a lei não tanto a um corpo real e susceptível de dor quanto a um sujeito jurídico, detentor, dentre outros direitos, do de existir. (FOUCAULT, 2007, p. 16)

Foucault aponta outras mudanças diversas no sistema judiciário marcando tal regime: a introdução de diversos especialistas encarregados de avaliar não somente se houve crime, mas todo um detalhamento de suas circunstâncias, suas causas e possíveis medidas de reparação. Torna-se relevante distinguir, por exemplo, se as causas do ato criminoso são psicológicas, genéticas, ambientais ou morais, o que infletirá sobre as medidas aplicadas para normalização do criminoso. Nota-se aqui não mais meramente uma reafirmação de uma autoridade soberana, mas uma preocupação ativa em conhecer o corpo e a alma do condenado para governá-lo.

Todas essas mudanças sinalizam a sobreposição de um regime novo ao velho regime de soberania. O novo regime será qualificado pelo filósofo como disciplinar. Diferentemente do antigo, não será mais o corpo do soberano o núcleo a partir do qual o poder é exercido de forma espetacularizada, mas sim um conjunto de técnicas de aplicação tão difusa e contínua que sua capilaridade tornaria difícil visualizar seus efeitos. Uma tecnologia política do corpo destinada a tornar a repressão desnecessária, pois sua eficácia impediria que se produzissem

revoltados: uma articulação entre saber e poder destinada a fazer o corpo individual obedecer utilizando o mínimo de violência possível.

O dispositivo disciplinar pode ser definido como um conjunto heterogêneo de métodos e técnicas de produção de corpos dóceis e úteis. Dóceis porque sua autonomia é reduzida ao mínimo, úteis porque sua utilidade é ampliada ao máximo. É um dispositivo que individualiza para produzir uma massa uniforme por meio da supressão das diferenças. A subjetividade, individualizada, deveria ser construída sobre a pertença institucional do indivíduo. O corpo e a alma são adestrados, as paixões e impulsos são domados pela força de um poder racionalizador.

O corpo do soldado ilustra bem essa oposição: o soldado do início do século XVII é o camponês forte de ombros largos, alguém que intimida pelo tamanho do corpo e pode ser reconhecido de longe. O soldado do fim do século XVIII é potencialmente qualquer um: o soldado tornou-se um corpo e uma consciência que se fabrica, corpo-máquina passível de ser produzido. O exército é uma força muito maior, organizada e eficaz por sua organização e disciplina que a soma dos soldados individuais.

Confina-se a multidão num espaço institucional, reparte-se o espaço em tantas células, carteiras, macas ou quadrantes quanto há indivíduos, os quais são distribuídos em fileiras e têm seu vestuário uniformizado. O tempo e a atividade biológica são regulados: regra-se o tempo de entrada, de saída, de alimentação, hidratação e excreção. Regulam-se também os gestos de maneira a aplicar pequenas sanções normalizadoras aos indivíduos que cometem pequenas infrações: o poder esquadrinha o espaço e o corpo. Ambos são percorridos em detalhe: nada deve ser deixado sem vigilância e regulação.

A disciplina mobiliza técnicas heterogêneas e acionadas em formas distintas ou variáveis, porém que compõem uma tecnologia geral de redução da autonomia do indivíduo e facilitação da sua gestão por parte da instituição. Se o espaço concreto no qual esse dispositivo esteve mais próximo de seu emprego em totalidade foi a prisão moderna, certamente não deixamos de perceber a aplicação de suas técnicas em variados graus nos conventos, quartéis, fábricas, escolas, oficinas, hospitais, hospícios, etc.

> Se os detentos são condenados não há perigo de complô, de tentativa de evasão coletiva, projeto de novos crimes para o futuro, más influências recíprocas; se são doentes, não há perigo de contágio; loucos, não há risco de violências recíprocas; crianças, não há "cola", nem barulho, nem conversa, nem dissipação. Se são

> operários não há roubos, nem conluios, nada dessas distrações que atrasam o trabalho, tornam-no menos perfeito ou provocam acidentes. A multidão, massa compacta, local de múltiplas trocas, individualidades que se fundem, efeito coletivo, é abolida em proveito de uma coleção de individualidades separadas. Do ponto de vista do guardião, é substituída por uma multiplicidade enumerável e controlável; do ponto de vista dos detentos, por uma solidão sequestrada e olhada. (FOUCAULT, 2007, p. 166)

É interessante destacar o protagonismo de noções como norma e igualdade para o bom funcionamento da disciplina. A multiplicidade dá lugar a uma oposição binária entre a norma e o desvio, sendo este último rapidamente corrigido e readequado para seu enquadramento na norma. Na medida em que a noção de norma é produzida como parte de um discurso colonial, ela também se define a partir de suas exterioridades: o desvio precisa ser produzido enquanto desvio para que a norma se produza e reproduza enquanto norma. O registro incessante também é parte essencial deste dispositivo. As instituições disciplinares classificam, registram e armazenam informações sobre os corpos que docilizam. Elas produzem biografias ordenadas em torno da pertença institucional: o aluno é conversa demais? ele faz as atividades corretamente? comporta-se bem? Tudo isto é devidamente armazenado.

Finalmente, um elemento fundamental ao bom funcionamento da disciplina é o panoptismo. Doutrina de vigilância baseada na arquitetura de uma prisão ideal proposta pelo filósofo e jurista Jeremy Bentham, a ideia é a de uma torre central cercada por um anel periférico. No anel periférico, tantas subdivisões quanto prisioneiros: as celas. Janelas duplas permitiriam a entrada contínua de luz, por um lado, e a visibilidade contínua dos prisioneiros por parte de alguém situado na torre central, onde deveria localizar-se um inspetor. No lugar do corpo do rei como centro simbólico e materialização do poder em todo seu esplendor, o vigia permanece oculto na torre central. Os presos continuamente em evidência por uma arquitetura que não lhes permite ver, apenas serem vistos.

> Daí o efeito mais importante do Panóptico: induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder. Fazer com que a vigilância seja permanente em seus efeitos, mesmo se é descontínua em sua ação; que a perfeição do poder tenda a tornar inútil a atualidade de seu exercício; que esse aparelho arquitetural seja uma máquina de criar e sustentar uma relação de poder independente daquele que o exerce; enfim, que os detentos se encontrem presos numa situação de poder de que eles mesmos são os portadores. Para isso, é ao mesmo tempo excessivo e muito pouco que o prisioneiro

> seja observado sem cessar por um vigia: muito pouco, pois o essencial é que ele se saiba vigiado; excessivo, porque ele não tem necessidade de sê-lo efetivamente. Por isso Bentham colocou o princípio de que o poder devia ser visível e inverificável. Visível: sem cessar o detento terá diante dos olhos a alta silhueta da torre central de onde é espionado. Inverificável: o detento nunca deve saber se está sendo observado; mas deve ter certeza de que sempre pode sê-lo. (FOUCAULT, 2007, pp. 166-167)

A economia de visibilidade do panoptismo é diametralmente oposta àquela presente no regime de soberania, onde a punição alternava entre o suplício público e a masmorra. O suplício público, já supra descrito, constitui uma situação na qual o poder coloca a si e ao condenado em pleno foco da luz. A masmorra, por outro lado, se caracteriza pela introdução de um corte entre a luz e o condenado, o que resulta numa inacessibilidade mútua: o condenado não pode ver o dia, mas também não pode ser vigiado continuamente. A lógica de visibilidade trazida pelo panoptismo sofistica imensamente essa lógica ao introduzir uma dinâmica de poder inverificável e alvo vigiado.

1.3 A benevolência do pastor

Muitos dos elementos presentes no poder disciplinar são identificados por Foucault no poder pastoral, seu antecedente genealógico. As relações pastorais são localizadas por ele inicialmente no Egito faraônico, na Judéia e na Assíria. No Egito, a entrega do cajado de pastor era um dos rituais que marcava a coroação do faraó, o qual era concebido como um pastor dos homens: um ente que velava continuamente por eles, por sua alimentação, saúde e vitalidade. A tópica seria desenvolvida com maior profundidade pelos hebreus, inclusive por meio de frequentes comparações, sobretudo negativas, entre reis e pastores.

Foucault (1990a, p. 80) ressalta a peculiaridade histórica do poder pastoral ao contrastar esta forma de conceber as relações entre a autoridade pública e o povo com o modo como os gregos elaboravam conceitualmente as relações com suas divindades: como relações pautadas menos pelo cuidado incessante e mais por uma espécie de diplomacia cósmica. Nos textos hebraicos, por outro lado, o que coloca é uma atenção e uma benignidade "constante, individualizada e final", um cuidado incessante, específico e autorreferido.

> É uma questão de benignidade constante, individualizada e final. De benignidade constante, visto que o pastor proporciona alimentos a seu rebanho; diariamente,

> mitiga sua fome e sua sede. Ao deus grego competia proporcionar uma terra fecunda e colheitas abundantes. Não se esperava dele que sustentasse um rebanho dia após dia. E também de benignidade individualizada, pois o pastor vela para que todas as ovelhas, uma a uma, sejam alimentadas e salvas. Mais adiante os textos hebraicos, em particular, ressaltaram esse poder individualmente benigno: um comentário rabínico sobre o Êxodo explica por que Javé escolheu Moisés para pastor de seu povo: ele abandonara seu rebanho para ir em busca de uma única ovelha perdida." (FOUCAULT, 1990a, p. 80)

Para extrair as consequências da identificação da autoridade política com o pastor, é necessário explorar mais a fundo a caracterização exposta acima. Em primeiro lugar, a oposição entre uma atenção acidental decorrente de uma relação entre possuidor e terra, como nas divindades gregas, e uma atenção integral resultante de relações entre pastor e rebanho, como desenvolvida no cristianismo. Um efeito da constatação dessa diferença é a observação de que o poder pastoral é benevolente: seu foco é o zelo por aqueles sob seu cuidado, não a expansão de suas posses ou a derrocada beligerante dos inimigos.

Como esse zelo se traduz na prática? Em uma atenção contínua e mútua à individualidade de cada ovelha e ao bem-estar do rebanho como um todo. O assobio do pastor reúne as ovelhas e eleva sua existência de multiplicidade caótica de corpos em movimento a rebanho com um destino. Seu desaparecimento e/ou má conduta levam à dispersão do rebanho. Dessa responsabilidade mútua com indivíduo e massa emerge o que Foucault (2008a, p. 224) denominou "lado paradoxalmente distributivo do pastorado cristão": a ovelha que ameaça corromper o rebanho deve ser excluída, expulsa ou abandonada, mas a salvação de uma única ovelha deve suscitar tantos esforços por parte do pastor a ponto dele estar disposto a abandonar o rebanho para trazê-la de volta.

Outro aspecto significativo da diferença entre as práticas gregas e o pastorado cristão concerne o lugar da obediência nas relações entre a autoridade e os sujeitos a ela. A obediência grega (se é que tal categoria estava presente na Grécia) emanava do respeito à vontade da cidade ou constituia um meio para um fim específico: obedecer-se-ia o médico para obter a saúde, o pedagogo para obter o saber, e assim sucessivamente. O pastorado cristão realiza algo absolutamente diverso ao introduzir a obediência como um tipo de relação individualizada (entre cada ovelha e o pastor), infinita (não se encerra após a realização de um fim específico) e valorada como um fim em si própria.

A noção de exame, tão essencial ao funcionamento das instituições modernas (escola, hospital, etc), tem seu antecedente genealógico no exame de consciência helenístico (prática pitagórica, estoica e epicurista). Mas se o exame de consciência tinha por fim o domínio de si quando realizada pelos estóicos, por exemplo, o exame de consciência cristão visa a renúncia total de si. Examina-se e confessa-se continuamente com a finalidade de matar cada pensamento, desejo ou afeto que esteja em desacordo com a vontade do pastor. O pastor, por sua vez, prescreverá continuamente formas de conduzir a ovelha a um estado mais desejável e adequado – a direção contínua e total da consciência. Alves resume (2016, p. 83): " No fundo, as práticas cristãs parecem dar duas ordens básicas: obedecer e dizer!".

A apresentação dos temas do pastorado cristão pode sugerir uma série de reflexões simbólicas, mas estas se atrelam a práticas e problemas absolutamente concretos da vida monástica e da organização da igreja, como a recuperação do desviante que se afastou do cristianismo e o cotidiano da administração monasterial. Esta brevíssima contextualização deve tornar mais visíveis algumas das continuidades e as descontinuidades entre o poder pastoral e o poder disciplinar, o qual podemos retomar a partir deste ponto.

1.4 A polícia dos grãos

Entre o século XVI e os fins do século XVIII, a Europa passa por uma série de transformações ligadas a intensificação das formações urbanas, crescente circulação de mercadorias, reforma protestante e contra-reforma, etc. Trata-se também de uma Europa marcada pela estruturação de Estados configurados como "grandes monarquias administrativas cujo governo tem como como objetivo gerir grandes massas de indivíduos e fazer deles corpos dóceis" (CASTELFRANCHI, 2008, p. 111). O desenvolvimento e implementação massiva das técnicas disciplinares nesse contexto indicam um processo mais amplo e gradual de penetração de temas e problemas característicos do pastorado no âmbito das práticas de governo[9], sobretudo as questões do governo de si e do governo dos outros.

Os termos nos quais as relações entre a autoridade política e o que a ela compete se transformam gradualmente, a começar por seu problema primário. A preocupação central de

[9] Enfatizo muito mais as continuidades entre poder pastoral e razão de Estado as descontinuidades. Esse é um foco distinto daquele do próprio filósofo, que frequentemente preferia sublinhar as diferenças entre as duas formas de exercício do poder.

pensadores como Botero, Palazzo e Chemnitz na passagem do século XVI ao XVII não era o tema aquiniano sobre a garantia da conformidade do governo dos homens com certas leis transcendentes (naturais e/ou divinas). Também não se tratava mais da tópica maquiavelista: como o príncipe pode manter seu soberania sobre alguma província ou território. A questão que se colocava era a seguinte: num contexto de competição interestatal, como garantir a estabilidade da república e aumentar seu poderio, sua capacidade de subjugar outras?

Eis uma forma original de elaborar conceitualmente o problema de como a autoridade deve ser exercida. A ênfase não está no príncipe, mas nesta articulação presumida estável entre jurisdição, domínio e condição de vida: o Estado, a república. O questionamento também é colocado em termos inteiramente imanentes, racionais e pragmáticos. Não se trata de desenvolver um saber que permita identificar o que é justo ou o que é legítimo, somente o que é necessário para que a tranquilidade republicana seja preservada e as forças do Estado se expandam.

A pergunta original suscita uma resposta original na forma de efeitos que emergirão nos séculos seguintes. Dentre estes efeitos está a percepção da necessidade de conhecimento das forças do Estado[10], conhecimento este que será codificado em números. A partir dos arranjos normalizadores da disciplina, ainda que não somente, mas em boa medida, foi possível gerar o nível de regularidade necessário à produção de uma norma. No século XVIII, essa norma permitiria conectar os fatos dos corpos individuais e institucionais aos do corpo social. Nesse sentido específico, a constituição da estatística moderna foi um dos efeitos mais decisivos da doutrina de razão de Estado.

Externamente, essa doutrina teve por efeito o desenvolvimento de um dispositivo diplomático-militar voltado à interação interestatal. Suas operações visam o aumento do poderio do Estado, porém externamente de forma autorefreada, sem que disso decorresse um conflito que levasse os Estados à aniquilação. O surgimento da ideia moderna de Europa está vinculado, portanto, à noção de equilíbrio europeu, a qual tinha seus alicerces nas noções de igualdade entre Estados europeus, por um lado, e de desigualdade entre a Europa e todo o mundo, por outro (MBEMBE, 2017). Nesta formulação do tipo "*The West and the rest*", o "resto", isto é, os continentes asiático, australiano, americano e africano, foi teorizado como disponível à apropriação colonial, o que era legitimado e mesmo incentivado.

[10] Eis aqui outro elemento de pastoralização do Estado: necessidade de conhecer o rebanho (população) simultaneamente como indivíduo e como massa.

Internamente, o aparecimento da estatística moderna esteve relacionado à emergência de todo um campo de práticas de intervenção destinadas à alocação racional dos elementos que circulam no território, a fim de se obter resultados ótimos para os interesses do Estado. O modelo dessa racionalidade advém da economia, em seu sentido grego original: o ordenamento, a disposição, dos elementos que compõem o espaço doméstico. Governar bem na relação entre Estado e sociedade torna-se analógico ao modo como um pai deve governar a casa: trabalho administrativo. Trata-se de conduzir adequadamente sua própria ação, a alocação e o uso de seus bens, assim como as condutas de sua família.

Isso se traduz na instauração de todo um leque de iniciativas direcionadas a conduzir os mais diversos aspectos da existência social a um estado considerado desejável, feliz, ordenado e pacífico. A ação governamental passa a incidir, portanto, sobre um conjunto de processos concretos cuja transcorrência deve ser otimizada: a circulação de mercadorias, a criminalidade, as epidemias, etc. O conjunto de instituições e medidas destinadas a uma espécie de polimento metafórico da sociedade será denominado de polícia, termo então empregado com um sentido bastante distinto do atual, pois engloba, mas não se limita às forças de segurança pública.

O Estado de polícia atua para conduzir as massas à felicidade conforme o necessário para a maximização das forças da república. Necessidade, eis uma categoria fundamental à razão de Estado. Se ao pastor competia a condução do rebanho, ao Estado compete a condução da população. Como o rebanho, a população é concebida como um sujeito de necessidades - alimento, saúde, segurança, etc (CAMATI, 2014). E como o pastor quebra a perna da ovelha rebelde para o seu bem, o Estado viola o direito se assim for necessário para sua sobrevivência e para a sobrevivência do rebanho. É por esse motivo que Foucault não entende o golpe de Estado como uma ruptura com a razão de Estado, e sim, em certo sentido, como manifestação dela.

1.5 Discurso sobre o silêncio

Há um último ponto conectado a todas essas transformações que é necessário abordar para os fins do argumento geral desse trabalho, o qual diz respeito às teses avançadas por Foucault no primeiro volume de sua *História da sexualidade.* Na obra em questão, o filósofo empreendeu uma análise minuciosa do que ele denominou “hipótese repressiva”

(FOUCAULT, 1999b, p. 19) segundo a qual a história da sexualidade entre os séculos XVII e XVIII seria uma “a crônica de uma crescente repressão" (ibid, p. 11), um processo de contenção, interdição e silenciamento cada vez maior do sexo.

Foucault não se preocupa em denunciar uma suposta falsidade da hipótese repressiva, mas em situá-la no contexto mais amplo de máquinas produtivas. Ao “interrogar essa sociedade que fala prolixamente de seu próprio silêncio” (GABRIELE *et al.*, 2010), ele insere o aparato repressivo nas engrenagens de um dispositivo da sexualidade que se caracteriza, dentre outros, por uma incitação contínua aos discursos sobre o sexo. Na igreja, tem-se um detalhamento dos sonhos e pensamentos sexuais nas confissões. Na literatura, proliferação das descrições minuciosas, como em Sade. Nas instituições médicas e jurídicas, tipificação e investigação sobre as perversões: surgem o homossexual, a mulher histérica, o pervertido, etc.

Aqueles que falam sobre o sexo o fazem cientes do poder exercido nesses momentos e portanto o fazem com certo gozo, o que Foucault (1999, p. 11) chama de “benefício do locutor”. Em suma, fala-se e intervêm-se cada vez mais sobre o sexo, mas institucionalmente, regradamente, nos espaços apropriados e contextos adequados, os quais são cada vez mais urgentes e portanto devem ser multiplicados tendo em vista a relevância do tabu em questão. Constitui-se então todo um campo de saberes, rituais, situações, objetos de estudo, corpos e tipos de gente articulado em torno dos fatos do sexo e da sexualidade.

A dimensão repressiva do tratamento dado ao sexo na modernidade se insere no contexto de uma tática pela qual o dispositivo da sexualidade responde à urgência histórica de territorializar, cartografar, vigiar e regular o corpo e as condutas. Trata-se de construir, a partir do, em torno do sexo e através dele um jogo de identidades, saberes, códigos e arquiteturas para o qual não há externalidades. Conclui-se, portanto, que a configuração do dispositivo da sexualidade se insere no contexto mais amplo de policiamento do indivíduo e da massa que se observa gradualmente conforme o Estado de polícia se consolidava.

1.6 A autonomia da ovelha

Racionalização econômica e reconhecimento da imanência dos fenômenos, dois elementos já identificáveis no Estado de polícia que darão ensejo à consolidação da moderna

economia política como "burilamento interno da razão de Estado" (FOUCAULT, 2008b, p. 40), um saber que direcionaria cada vez mais a racionalidade governamental a partir de meados do século XVIII. E com a economia política aparece um novo princípio direcionador das práticas governamentais em âmbito interno: o princípio da autolimitação. A ideia de que as coisas devem ser, tanto quanto possível, deixadas transcorrer naturalmente.

Como compreender tal princípio? Em primeiro lugar, como uma espécie de inversão da racionalidade pastoral do Estado de polícia, o qual assumia, tendo por fim a maximização de suas forças, a premissa da necessidade de condução das condutas da população até o mínimo detalhe. A economia política denuncia essa racionalidade como sendo ineficaz para a realização dos próprios fins da razão de Estado: enriquecer o Estado e a população. Sua análise dos meios mais adequados ao enriquecimento levará a uma reflexão contínua sobre o custo das ações governamentais, bem como sobre seus efeitos ecológicos na sociedade.

Para a economia política, governar bem significa maximizar a eficiência e minimizar o custo. Isso implica, dentre outras coisas, na necessidade de instaurar mecanismos capazes de limitar o dispêndio pela própria ação estatal. O princípio de autolimitação da economia política não tinha sua raízes na legitimidade, mas na eficiência. Governar demais é governar mal, não por um critério de legalidade ou justiça, mas porque governar mal significa governar de forma estúpida e ineficaz. Quem governa demais é, antes de mais nada, um ignorante, alguém que falha em compreender a natureza, a verdade, a autorregulação dos fenômenos.

Esse crítica ao Estado de polícia, propagada principalmente por economistas fisiocratas como Quesnay e Turgot, fica bastante evidente em sua leitura do problema da população. Se para o Estado de polícia "nunca existe população suficiente porque sempre se precisa de mais mão de obra para produzir e aumentar as riquezas – e conseqüentemente o poder – do Estado" (SANTOS, 2010, p. 201), para os fisiocratas o problema deveria ser encarado de outra forma:

> Claro, é preciso bastante população para produzir muito, e principalmente bastante população agrícola. Mas não é preciso demais, e não deve ser demais, justamente para que os salários não sejam baixos demais, isto é, para que as pessoas tenham interesse em trabalhar e também para que possam, pelo consumo de que são capazes, sustentar os preços. Logo, não há valor absoluto da população, mas simplesmente um valor relativo. Há um número ótimo desejável de gente num território dado, e esse número desejável varia em função tanto dos recursos como do

> trabalho possível e do consumo necessário e suficiente para sustentar os preços e, de modo geral, a economia. (FOUCAULT, 2008a, p. 464)

Assim, o critério de validação da prática governamental passa a ser sua afinidade com a natureza imaginada dos fenômenos. Isso explica a redefinição da relação entre Estado e mercado: O mercado do século XVII era um "lugar de jurisdição" (FOUCAULT, 2008b: 45) produzido por intervenções voltadas ao combate do indesejável (escassez, etc), o mercado de meados do século XVIII tornou-se o “lugar de veridição” (Ibid.) das práticas governamentais. As leis de funcionamento do mercado, seus mecanismos de auto regulação e suas dinâmicas internas seriam dotadas de uma naturalidade independente das noções de justiça e legitimidade. Isso porque o mercado é tratado como o lugar da espontaneidade, das interações voluntárias entre sujeitos comportando-se como naturalmente o são: individuais e auto-interessados. O preço ditado pelo mercado sem a intervenção estatal seria, portanto, o preço natural, verdadeiro, dado somente pela dinâmica de oferta e demanda de um bem.

Para a economia política, o Estado deveria ser modesto e reconhecer, antes de mais nada, sua incapacidade de conhecer e realizar os interesses de todos. O Estado deveria aprender com o mercado e adaptar-se a suas leis. A autolimitação governamental permitiria que cada indivíduo buscasse seus próprios interesses e contribuisse com o enriquecimento coletivo no processo. Das ideias de autolimitação estatal como condição para o enriquecimento e de incapacidade do Estado em conhecer e realizar os interesses da população, deduz-se a competência do Estado: produzir e administrar as condições para a possibilidade de busca individual da felicidade, isto é, produzir e administrar liberdades (de expressão, de mercado, etc).

Candiotto (2014) observa a ausência de um conceito unívoco de liberdade em Foucault. A análise do poder disciplinar havia situado o sujeito de direitos iluminista como uma tipo de produto superestrutural da infraestrutura disciplinar de fabricação do indivíduo. Naquele momento, o filósofo analisara, ainda que tangencialmente, o liberalismo como ideologia, não como arte de governo. Suas considerações a respeito de uma arte liberal de governar reservam outro tratamento à categoria de liberdade, agora intimamente associada às ideias de interesse e de sujeito de interesses. Não estamos mais diante de um Estado de polícia que, como o pastor, conduz o rebanho de acordo com suas necessidades, e sim de um Estado gerenciador de liberdades cuja função é produzir as condições para que cada ovelha possa conduzir a si própria.

1.7 Viver perigosamente

Ocorre, no entanto, que a busca individual pela realização dos próprios interesses frequentemente gera problemas coletivos, o que o linguajar liberal codifica como externalidades negativas, obstáculos para a busca dos próprios interesses que não decorrem das próprias ações do sujeito. Por exemplo, liberdade de mercado irrestrita gera monopólio, o que resulta na extinção prática da liberdade de mercado. Por conseguinte, o Estado liberal encontra-se permanentemente confrontado com o problema de gerenciamento das liberdades e das externalidades.

Assim, me parece que a razão governamental liberal trata a noção de liberdade em dois sentidos complementares. Por um lado, a liberdade consistiria na capacidade objetiva do sujeito em realizar certa ação específica visando a realização de seus próprios interesses, sejam eles quais forem. Essa capacidade é sempre produto de um contexto específico, de uma situação. O segundo sentido se refere, por conseguinte, a uma 'situação de liberdade' cujo efeito seria conformar o campo de ação do sujeito de modo a produzir a capacidade que corresponde ao primeiro sentido. Nesse sentido, não faz sentido falar de sujeitos livres e da liberdade separadamente do contexto de governo. O que se tem são ações livres e liberdades adjetivadas (liberdade de imprensa, liberdade de cátedra, liberdade de mercado, etc).

Quando os efeitos produzidos pelo exercício de certas liberdades se traduzem em externalidades negativas para outras, o Estado liberal age. Essa ação pressupõe nos governados a experiência contínua de ameaça por externalidades negativas (dentre outros perigos) cujos efeitos possam se traduzir na redução de sua liberdade. Esse temor é o que legitima o contínuo jogo de negociação entre liberdade e segurança que caracteriza a experiência liberal. Assim Foucault (2008b, p. 90) afirma que o lema do liberalismo é "viver perigosamente", o que significa simplesmente que "que os indivíduos são postos perpetuamente em situação de perigo, ou antes, são condicionados a experimentar sua situação, sua vida, seu presente, seu futuro como portadores de perigo."

A circulação de enunciados relativos a diversos perigos (de degeneração, de crime, de epidemia, etc) é um traço importante da arte liberal de governar porque constitui o elemento discursivo de um movimento de expansão contínua dos mecanismos de vigilância. Foucault localiza no panoptismo benthaniano uma fórmula geral do governo liberal: nada tocar e tudo vigiar para que os olhos digam quando a mão é necessária. Tanto quanto um modelo de

arquitetura espacial das instituições, o panoptismo é uma filosofia política de governo. Mesmo quando a intervenção é necessária, o Estado liberal não intervém sobre o indivíduo – isso seria demasiadamente custoso e pouco eficaz –, e sim sobre o meio e seus elementos. Desenha-se então um regime geral de ação governamental cujo alicerce é a intervenção mínima e calculada sobre a imanência dos fenômenos. Esse regime articula uma prática de governar (*gouverner*) e a mentalidade (*mentalité)* que a direciona, e é denominado governamentalidade (*gouvernementalité*)[11][12].

A governamentalidade liberal não atua pela intervenção externa sobre um fenômeno indesejado (criminalidade, escassez, etc) com o objetivo de negá-lo em absoluto, de impedir sua ocorrência. Busca-se modulá-lo. Age-se por uma série de intervenções pontuais nas dinâmicas que conformam as frequências dos fenômenos. O objetivo passa a ser produzir um contexto, uma articulação entre os elementos envolvidos no fenômeno, que assegure a estabilidade de certas frequências em níveis considerados desejáveis. Essas articulações, denominadas pelo autor como dispositivos de segurança[13], são explicadas didaticamente por Castelfranchi (2008, p. 115):

> A biopolítica coloca para o governo uma nova questão: como fomentar ou dificultar processos, aumentar ou diminuir probabilidades, manipular e modular parâmetros e fluxos para que, em média, as coisas fiquem do jeito desejado. O meio social aparece como um campo de intervenção onde a população pode ser afetada. Por exemplo, diz Foucault, quanto maior é o amontoar-se da população num bairro, mais miasmas e enfermos haverá. Logo, quanto mais enfermos, mais mortos. Quanto mais mortos, mais cadáveres, e conseqüentemente, mais miasmas. Manipular a geometria das cidades e modular os fluxos de pessoas e mercadorias pode ser então uma forma de governo mais eficiente do que tentar controlar cada indivíduo.

[11] O termo *gouverne* também poderia ser traduzido por leme, dispositivo de controle de direções em embarcações e aeronaves. Na navegação à vela, o leme equivale ao timoneiro (do grego *kybernétes*, donde também se origina o termo cibernético). Esta última associação também alude ao fato de que a condução desse tipo de veículo não é feita por um movimento simples, mas envolve a observação da direção dos ventos, ondas e etc. Em suma, os efeitos que se deseja obter são alcançados por intervenções indiretas que visam produzir interações complexas das quais tais efeitos decorrerão.

[12] Foucault emprega o termo governamentalidade em pelo menos dois sentidos: um, mais geral, se refere ao fenômeno moderno de uma prática racional de conduta da conduta das pessoas, o que englobaria tanto a razão de Estado quanto a arte liberal de governar. O segundo sentido, mais específico, designa especificamente esta última arte e a relaciona expressamente com a economia política e com os dispositivos de segurança. Faço uso deste último sentido ao longo do texto (governamentalidade como governamentalidade liberal).

[13] O termo utilizado por Foucault é *securité*, o qual também poderia ser traduzido como seguridade, como em seguridade social.

Uma das consequências do desenvolvimento desse modelo, como ilustra a citação, é a inserção do *bios*, da vida enquanto natureza e enquanto biologia, no domínio das disputas políticas. Os fatos naturais do corpo social, agora crescentemente mapeados e delineados, são inseridos nos cálculos de governo: nascimento e morte são codificados como taxas de natalidade, mortalidade e reprodução. Os saberes demográfico e estatístico possibilitam a uma intervenção de tipo ecológico sobre esses fenômenos. O que era da ordem do transcendente, do ingovernável e do além-do-humano é deslocado para campo do imanente, do disputável e das estratégias.

A diferença entre razão de Estado e racionalidade liberal se expressa na diferença entre os dispositivos disciplinares e securitários. A disciplina visa aumentar infinitamente a granularidade da ação regulatória num espaço circunscrito, de modo que nenhuma conduta do indivíduo seja deixada sem condução: sua atuação é "centrípeta" (FOUCAULT, 2008a, p. 59), ela se aproxima continuamente do centro de sua ação (o corpo individual). Os dispositivos de segurança, por outro lado, tem atuação "centrífuga" (ibid.): se expandem continuamente para além do centro, o que só é possível devido ao caráter autorrefreado de suas intervenções. Se o Estado de polícia visa controlar tudo em seu território, a governamentalidade liberal intervém pontualmente sobre um campo cada vez maior de circuitos e articulações.

Por fim, algumas considerações a respeito da análise foucaultiana dos neoliberalismos. Utilizo o termo no plural porque Foucault se debruça sobre duas variedades de neoliberalismo: o ordoliberalismo alemão associado à Escola de Friburgo e o anarcoliberalismo estadunidense conectado à Escola de Chicago. O filósofo não entendia o neoliberalismo como uma total ruptura com o liberalismo dos séculos XVIII e XIX, mas como um rearranjo dessa racionalidade. Elementos comuns a ambos os neoliberalismos incluem a identificação do autoritarismo com o Estado planificador e a tentativa de redefinição do papel do Estado de acordo com os interesses que perfazem o mercado.

O ordoliberalismo alemão insere o mercado dentro da história. Ele não é tido como esfera da naturalidade dotada de uma lógica intrínseca, as interações que o compõem são, pelo contrário, niveladas com outras práticas sociais particulares e contextuais. A economia não é vista como determinante linear da sociedade. A alocação eficiente por via das interações no mercado e a livre concorrência não são dados, mas construídos. A mão invisível

não existe, portanto deve existir uma mão visível materializada na forma de regulação que garanta os ideais de bom funcionamento do mercado.

Em sua versão anarcoliberal, por outro lado, realiza-se uma operação inversa em que a lógica do mercado territorializa a sociedade. O Estado é uma empresa cujo produto é regulação favorável ao mercado e como qualquer empresa deve cortar quaisquer gastos não essenciais. O trabalhador é um empreendedor de si dotado de capital humano cuja boa aplicação fornecerá lucros (salários) maiores. As políticas de combate ao crime não devem almejar sua erradicação, somente "construir uma tabela adequada de castigos e desvantagens para os diferentes tipos de crime, de forma a modular as externalidades negativas de diversos tipos de conduta ilegal, que vão do excesso de velocidade ao homicídio" (CASTELFRANCHI, 2008, p. 123).

1.8 Sonhos de andróides

A análise foucaultiana da governamentalidade tem sido alvo de diversas polêmicas nas últimas décadas. Suas reflexões a respeito do tema tem sido acusadas de serem idealistas (WACQUANT, 2012; DUPONT e PEARCE, 2001), simpáticas ao neoliberalismo (HANSEN, 2015; HAN, 2014) e de incentivarem narrativas monolíticas e unilineares das transformações governamentais (BRADY, 2014; DUPONT e PEARCE, 2001) – embora essa crítica talvez seja dirigida mais a seus comentadores que ao próprio autor. Sem adentrar um debate relativo ao grau de pertinência dessas críticas, gostaria de explorar um aspecto tangencialmente tratado por todas elas: a ausência de uma análise mais sistemática sobre o emprego de técnicas de condução de conduta por parte do mercado.

A discussão do filósofo a respeito das governamentalidades liberais e neoliberais se fundamenta majoritariamente na análise de textos de economistas e outros teóricos. Esse material é interpretado à luz de uma perspectiva informada pela recusa da categoria ideologia. Isso significa que Foucault não se coloca na posição de avaliar a eficácia descritiva desses textos em relação aos fenômenos descritos. Em termos mais vulgares: Foucault não se propõe a discutir em que medida os textos de Quesnay, Ropke ou Becker oferecem representações acuradas da realidade – questão que possivelmente sequer faria sentido para o filósofo. O objeto de sua atenção está mais ligado aos efeitos desses textos no contexto de certas práticas e racionalidades governamentais.

Uma consequência desse tipo de análise foi a escassez de reflexões mais sistemáticas acerca do emprego de mecanismos de governo por parte do setor empresarial. Tanto a doutrina de polícia voltada ao total disciplinamento do indivíduo quanto a razão liberal e sua autolimitação materializada nos dispositivos securitários têm por pano de fundo a questão sobre como e quanto o Estado deve ou não agir (ainda que por meio de diversas instâncias difusas). Assim, por mais que Foucault reitere que seu tema é mais o governo que o Estado, sua discussão sobre governamentalidade se centra nas práticas governamentais do Estado.

Isso não deve ser interpretado exatamente como uma crítica ao autor, apenas como a constatação da existência de um espaço analítico cuja investigação engendra resultados profícuas. Felizmente, a reflexão sobre esse tipo de relação entre empresas e consumidores foi e vem sendo tematizada explicita ou implicitamente por diversas autoras e autores, dentre as quais merecem destaque Donna Haraway, Santiago Castro-Gomez, Paul B. Preciado, Antoinette Rouvroy, dentre outros. Recupero alguns de seus apontamentos para complementar a análise foucaultiana do neoliberalismo.

Dentre as transformações significativas sofridas pelo sistema capitalista no século XX estiveram a redução no ciclo de vida dos produtos, a popularização de uma economia de serviços e a valorização crescente dos bens simbólicos e da inovação (RIFKIN, 2011). Além disso, a corrida tecnológica ligada aos conflitos militares entre grandes potências levou a um desenvolvimento sem precedentes das tecnologias da informação. A partir da década de 1980, essas e outras tendências convergem para um contexto de globalização neoliberal ao modelo estadunidense, a qual se caracteriza pelo aprofundamento das desigualdades econômicas e por um processo de financeirização dos Estados (GIFFIN, 2007).

De modo geral, pode-se dizer que todas essas mudanças estiveram em relação circular com a expansão da esfera consumista, sendo tanto seu motor quanto sua consequência. A psicologia comportamental, a estatística e o marketing se articulam como saberes a partir dos quais se produz verdade, agora sobre consumidores continuamente fabricados por dispositivos de registro e feedback relativo a seus comportamentos. Santos (2001, p. 24) descreve o processo e sintetiza sua função: “A produção do consumidor, hoje, precede à produção dos bens e dos serviços. [...] Daí o império do marketing e da publicidade”. À tecnologia disciplinar associada primariamente ao Estado de polícia por Foucault, passa a se sobrepor um novo conjunto de mecanismos associado por Deleuze (1992) a uma sociedade de controle.

Como se caracteriza o exercício do poder nessa sociedade? Em primeiro lugar, trata-se de prisão em campo aberto, confinamento sem muros. As instituições disciplinares são mundos fechados em si, o escopo de atuação de seus mecanismos corresponde ao espaço do confinamento institucional. As novas técnicas, por outro lado, são tributárias da logística militar, da arte de assegurar a continuidade das redes de comunicação e a mobilidade estratégica. Elas jamais cessam de incidir sobre o sujeito conforme este se desloca entre diferentes espaços. Deleuze aponta que a sociedade disciplinar tinha na assinatura individual e no número de matrícula institucional seus dois pólos de representação do par indivíduo-massa. O novo regime, cuja linguagem é numérica, tende a articular um código pessoal intransferível e uma senha.

O uso da senha para o acesso a bens, serviços e espaços permite que as informações do ligadas ao código intransferível do indivíduo sejam atualizadas de forma móvel, automatizada e constante. Não é necessário monitorar uma cela, cama ou carteira, como na disciplina. A ação do próprio indivíduo (ao manipular um cartão de crédito ou telefone celular, por exemplo) atualiza seus registros nos bancos de dados. Não é coincidência que esses dois objetos estejam ligados ao consumo: consumir e ser conhecido tornam-se partes integrais do mesmo processo, a facilitação do controle torna-se condição para o acesso ao prazer.

As conexões entre o desenvolvimento destas novas formas de subjetivação e a evolução da ciência e da tecnologia são bastante profundas. Tanto no nível da produção do produto quanto no nível da produção do consumidor, os novos mecanismos de poder tornam-se cada vez mais atrelados à ordem tecnocientífica. A expressão desse tipo de transformação no campo das ciências biológicas foi colocada no centro da análise apresentada por Donna Haraway em *The Biological Enterprise - Sex, Mind & Profit from Human Engineering to Sociobiology* (1991). No texto, ela contrasta as produções de Robert Mearns Yerkes e Edward O. Wilson, conectando-as a momentos, projetos e racionalidades distintas no âmbito das ciências da vida. A comparação entre a psicofisiologia do primeiro e a sociobiologia do segundo ilustra tanto o modo como certas ideologias de contextos específicos eram incorporadas às premissas da produção científica quanto sua materialização em seus produtos.

Yerkes foi um dos grandes nomes da psicofisiologia e da primatologia estadunidenses na primeira metade do século XX. As relações entre fisiologia animal e condutas sociais eram

o objeto de seus estudos, sobretudo daqueles desenvolvidos entre 1924 e 1942 na Universidade de Yale e na Rockefeller Foundation. O objetivo de sua pesquisa era contribuir com a engenharia humana, um conjunto de práticas e saberes voltados à facilitação da administração racional de indivíduos. A administração científica dos corpos na época tinha por objetivos o "microcontrole de trabalhadores individuais, o estabelecimento de hierarquias cooperativas e a separação clara entre o trabalho manual e o controle funcional" (HARAWAY, 1991, p. 208 - 209, trad. minha).

O objeto material e discursivo sobre o qual os interesses da psicofisiologia incidiam era o organismo individual, cuja unidade era codificada na noção de personalidade. Para Yerkes, a personalidade emergia da interação entre estruturas psicológicas, impulsivas e hormonais e se traduziria numa unidade comportamental coerente dotada de propensão a desempenhar certas funções sociais no contexto das diferentes instituições (família, escola, fábrica, etc). A ideia de um todo diferenciado em partes discretas com funções bem definidas foi bastante popular nesse período, sendo utilizada por diferentes áreas de pesquisa como modelo para a compreensão de uma variedade de entes: empresas, sociedades, indivíduos, etc. Essas ideias passaram por uma variedade de aplicações, sobretudo durante a Primeira Guerra Mundial, quando Yerkes foi convidado para auxiliar no desenvolvimento de testes de inteligência aplicados a recrutas. Os resultados desses testes, os quais foram desenvolvidos juntamente com o cirurgião geral do exército como parte de um projeto de gerenciamento médico da sociedade, posteriormente receberam diversas aplicações, incluindo políticas de controle migratório.

Em todo caso, a psicofisiologia disciplinar de Yerkes entrou em declínio nos fins da década de 1930, decaindo notavelmente ao longo dos anos 1940. Um novo movimento denominado por Haraway (1991, p. 221) como "revolução das comunicações" ganhava popularidade rapidamente no período pós Segunda guerra mundial e durante a Guerra Fria, o qual estava amplamente conectado às preocupações e aos desenvolvimentos tecnológicos dessas guerras. O movimento é caracterizado pela autora nos seguintes termos: Uma revolução das comunicações significa uma reteorização dos objetos naturais como dispositivos tecnológicos propriamente entendidos em termos de mecanismos de produção, transferência e armazenamento de informação" (HARAWAY, 1991, p. 222).

As inspirações para esse movimento provinham de fontes diversas: teorias capitalistas do gerenciamento de investimentos, ciências da informação, termodinâmica e práticas

biopolíticas de controle populacional. Genética molecular, bioquímica e imunologia assumem um lugar de protagonismo anteriormente reservado à fisiologia dos organismos nesse estilo de pensamento. A ciência biológica se reconfigura: de uma ciência de organismos individuais passa a ser uma ciência de sistemas cibernéticos. "O novo livro da natureza é escrito não apenas com outros termos, adequados aos conceitos das teorias da comunicação, mas também na linguagem matemática dos sistemas computacionais" (SILVA, 2009, p. 57).

Nessa narrativa, a natureza imita o mercado. O individualismo atômico é a ideia basilar e o altruísmo figura como escândalo básico a ser explicado. A sociobiologia de Edward O. Wilson, desenvolvida no contexto da Guerra Fria, exemplifica isso ao tornar organismos e sociedades epifenômenos do real processo de seleção natural que ocorre no nível genético. O altruísmo de organismos é meramente uma expressão do egoísmo de genes e conjuntos de genes, os quais operam no sentido de maximizar sua replicação – o lucro no mercado da seleção natural. As noções de investimento, replicação, cópia e codificação assumem um lugar privilegiado nesse tipo de produção teórica. Esse modelo se torna hegemônico na biologia dos fins do século XX. Genes são como programas que jogam xadrez, diz Haraway (1991, p. 227) leitora de Dawkins. Por um lado, o gene não possui qualquer intencionalidade, é uma máquina sem alma. Por outro, sua forma de estar no mundo é a de um sujeito de interesses, um *homo economicus* voltado a vencer a competição da seleção natural e maximizar seus lucros no mercado genético.

Organismos são máquinas comportamentais que viabilizam a competição de genes e conjuntos de genes no mercado natural. Tais máquinas determinam a taxa de mudança do sistema em função de sua capacidade de monitorar e responder a variáveis ambientais. Órgãos sensoriais são dispositivos de entrada que possibilitam a tradução dessas variáveis em *inputs*. A vida mental corresponde a uma sequência de simulações possibilitada por cérebros, os quais figuram como aparelhos de processamento com sistemas operacionais. O sexo é uma audaciosa inovação que diversifica os investimentos e acelera a geração de mais inovação.

O debate de Haraway oferece uma complemento e um contraponto bastante ricos ao debate de Foucault sobre a racionalidade neoliberal como uma racionalidade que reconhece a não-naturalidade do mercado. Para a autora, o neoliberalismo reescreve a natureza à luz das mesmas dinâmicas de troca mercantil que se pretende reproduzir ao longo de todo o corpo social. O neoliberalismo não precisa naturalizar o mercado se a natureza for transformada em seu espelho.

Um dos elementos mais ricos da análise de Haraway é a constatação, anos antes da publicação do pequeno texto de Deleuze a respeito da sociedade de controle, que as ciências da comunicação, as biologias contemporâneas e as novas técnicas de subjugação se alicerçam na mesma operação fundamental, a qual resume o base da condução de condutas nessa sociedade. O problema essencial é

> a tradução do mundo em termos de um problema de codificação, isto é, a busca de uma linguagem comum na qual toda a resistência ao controle instrumental desaparece e toda a heterogeneidade pode ser submetida à desmontagem, à remontagem, ao investimento e à troca. (HARAWAY, 2000, p. 64, publicação original de 1985)

Os grandes divisores que outrora haviam operado a serviço da razão moderna se constituem agora um obstáculo para o aprofundamento do controle. Por esse motivo, Haraway identifica na interpenetração progressiva entre instâncias que o pensamento moderno produzira como substâncias imiscíveis o traço definidor dos novos mecanismos de conduta da conduta. Para que o controle se aprofunde, aumenta-se a porosidade das fronteiras entre trabalho e lazer, natureza e cultura, público e privado, norma e desvio, fato e ficção e assim sucessivamente. Não se deve esquecer que o ciborgue, imagem perfeita da hibridez, é uma arma de guerra permanentemente conectada ao aparato de controle por um chip.

A diluição das fronteiras também é perceptível no tratamento dado à diferença pelos novos mecanismos, o qual não raro é elogioso. Observa-se uma incitação crescente ao gozo e à livre expressão, o que assinala uma ruptura em relação à abordagem das relações entre norma e conduta na disciplina. Se a ordem disciplinar atuava para suprimir as condutas resultantes dos desejos individuais, o novo regime estimula a liberação de cada impulso e sua transformação em experiência. É a mudança observada por Preciado (2011, p. 22), ao analisar a globalização da pornografia como técnica de pene masturbação a partir de 1950:

> Isso é absolutamente diverso do que ocorria no séc. XIX, quando era necessário manter uma continuidade entre sexualidade e reprodução e por isso se patologizou e perseguiu medicamente e juridicamente todas as práticas não reprodutivas, em particular a masturbação, doença sexual por excelência do séc. XVII ao final do XIX. Note a mudança absolutamente radical que se verifica nos anos 50 quando se passa da repressão da masturbação a um incitamento pene-masturbatório planetário como parte de um sistema de comunicação e produção de capital. Durante o séc. XIX a masturbação era vista como uma perda de energia que deveria ser utilizada para trabalhar, enquanto nas configurações farmacopornográficas a masturbação é

> um processo de produção de subjetividade e de capital imprescindível para o capitalismo contemporâneo.

Por que tratar como desvio o que se pode tratar como demanda? A noção disciplinar de desvio favorecia a supressão de toda uma série de condutas excluídas do padrão normativo, o que resultava em homogeneidade e docilidade. Isso fazia sentido num momento em que a racionalidade governamental do Estado de polícia conectava o sucesso na economia de mercado ao aumento da escala de uma produção homogênea. Nos fins do século XX, por outro lado, a celeridade da inovação adquiriu um peso consideravelmente maior na competição, o que torna a diversidade positiva para o bom funcionamento da economia. Inovar é diferir, afinal de contas. Daí a meditação de Castro-Gomez (2005, p. 6, ênfases do autor):

> Poderíamos falar inclusive de uma *governamentalidade sem governo* para indicar o caráter espectral e nebuloso, às vezes imperceptível, mas por isso mesmo eficaz, que toma o poder em tempos de globalização. A sujeição ao sistema-mundo já não assegura mediante o controle sobre o tempo e sobre o corpo exercido por instituições como a fábrica ou o colégio, e sim pela produção de bens simbólicos e pela sedução irresistível que estes exercem sobre o imaginário do consumidor. O poder *libidinoso* da pós-modernidade pretende modelar a totalidade da psicologia dos indivíduos, de tal maneira que cada qual possa construir reflexivamente sua própria subjetividade sem necessidade de opor-se ao sistema. Pelo contrário, são os recursos oferecidos pelo próprio sistema os que permitem a construção diferencial do "Selbst". Para qualquer estilo de vida que se escolha, para qualquer projeto de auto-invenção, para qualquer exercício de escrever a própria biografia, sempre há uma oferta no mercado e um "sistema especialista" que garante sua confiabilidade. Mais que reprimir as diferenças, como fazia o poder disciplinar da modernidade, o poder libidinoso da pós-modernidade *as estimula e as produz*.

Esse tipo de análise é complementado pela argumentação de autoras como Denise Sant'anna (2002, p. 102) a respeito da passagem de uma "ordem jurídico-política" associada ao poder disciplinar do Estado de polícia a uma "ordem tecnocientífica-empresarial" ligada aos mecanismos de condução de condutas desenvolvidos e empregados por grandes empresas no contexto da globalização neoliberal, uma ordem, diz a autora, na qual a alegria é feita funcionar como palavra de ordem. O ponto fundamental desses diversos complementos às ponderações de Foucault a respeito do neoliberalismo reside, a meu ver, no que eles sinalizam a respeito das relações entre liberdade, sujeito e mercado.

O Estado de polícia arrogava para si a conduta da conduta do indivíduo e da população visando assegurar suas necessidades e garantir sua felicidade. O princípio de autolimitação governamental imposto pelo liberalismo modifica isso ao impor ao Estado o reconhecimento de sua incapacidade de conhecer os interesses de todas as ovelhas. Consequentemente, o Estado deveria refrear-se e permitir que cada ovelha pudesse perseguir seus próprios interesses. Em suma, trata-se de uma crítica em nome da liberdade.

Mas metaforizar o Estado como pastor e enfatizar sua ação regulatória como governo de ovelhas (sujeitos individuais e população) pode omitir as relações de conduta da conduta pelas quais alguns dos atores que o Estado regula tornam-se eles próprios pastores de outros. Isso pode passar a impressão de que todas as ovelhas são iguais e todas as liberdades são análogas. O que as autoras e autores trabalhados nesta seção fazem é trazer a tona as relações de conduta da conduta que permeiam as interações mercadológicas nos fins do século XX. Isso permite a constatação de um aspecto implícito da racionalidade governamental neoliberal, qual seja a relação de proporcionalidade inversa existente entre liberdade de mercado e autonomia do sujeito frente os mecanismos de controle empregados pelo mercado.

A autolimitação governamental codifica a expansão de um governo privado cuja ação é informada por uma descoberta tão radical quanto a descoberta de que se podia docilizar o corpo no século XVIII: pode-se modular o interesse. Docilizar os impulsos não é mais necessário ou eficiente, muito mais profícuo é inserir as engrenagens do poder na máquina de produção do desejo. Se a soberania responde à rebelião com o espetáculo punitivo e a disciplina impede a produção de revoltados, o controle é incita a revolta e a transforma em consumo. Se o sujeito fabricado pela disciplina está continuamente a dizer “sim, senhor”, aquele que o controle produz não cessa de afirmar “estou ciente e desejo continuar”.

CAPÍTULO 2 – O PARADOXO DAS FOLHAS DE CHÁ

2.1 Protocolos, tanques e aviões de combate

Conforme identificado por Donna Haraway, o exercício do poder na segunda metade do século XX passou a ter como operação fundamental a manipulação da informação. As máquinas características desse tipo de modelo, dissera Deleuze (1992, p. 4) são "máquinas de informática e computadores". Para compreender a importância da qual se reveste a encriptação nesse regime de poder, é conveniente investigar o papel desempenhado por esse recurso na emergência do próprio regime em questão. Com esse objetivo em mente, retorno rapidamente a um conflito que constituiu um marco na história da tecnologia da informação.

O conflito em questão foi a Primeira Guerra Mundial, quando comunicações telemáticas sem fio passaram a ser utilizadas sistematicamente para a transmissão ágil de mensagens de importância militar através de distâncias consideráveis, o que suscitou demanda por tecnologia capaz de garantir a segurança da informação (DIFFIE e LANDAU, 2007). Assim, observa Liu (2017, p. 316, trad. minha): "Todos os países envolvidos nos conflitos armados aprenderam ao fim da primeira guerra mundial que uma forma melhor e mais efetiva de assegurar comunicações era essencial de uma perspectiva de segurança nacional."

A apreensão e decifragem de mensagens militares tornou-se ainda mais importante durante a Segunda Guerra Mundial, quando os dois lados do conflito passaram a fazer uso intensivo de tecnologias produzidas no período de intervalo entre as guerras. Por exemplo, foi de grande importância para os aliados decifrar as mensagens transmitidas através da cifragem viabilizada pela máquina Enigma, então empregada pelos nazistas (SOUZA, 2016). A importância da encriptação continuou a crescer durante a Guerra Fria conforme os Estados Unidos e a União Soviética simultaneamente buscavam coletar o máximo de informação possível sobre as atividades do outro e ocultar suas próprias atividades.

A aplicação de um controle bastante estrito sobre produtos criptográficos foi considerada uma necessidade no período posterior à Segunda Guerra, o que levou à aprovação do *National Security Act* pelos Estados Unidos em 1947 (LIU, 2017). Essa lei tornava a Agência de Segurança Nacional (NSA) o principal ator na regulação da encriptação ao atribuir a ela, dentre outras, a responsabilidade de definir os produtos criptográficos que

poderiam ser exportados. Para Froomkin (1995), a NSA tratava tais produtos “como um tanque ou um avião de combate”.

Liu (2017) constata que as preocupações da agência não se limitavam à exportação desse tipo de produto, pois a NSA também atuava para inibir a difusão de encriptação forte em âmbito doméstico. Juntamente com a Agência Nacional de Padrões, a NSA desenvolveu a padrão de cifra para uso pelo setor privado nos EUA durante a década de 1970, o *Data Encryption Standard* (DES). Uma versão revisada desse protocolo, o algoritmo LUCIFER desenvolvido pela IBM, foi selecionada como padrão nacional em 1977. A NSA havia exigido, no entanto, que o tamanho de chave fosse reduzido de 100 bits para apenas 56, o que podia ser interpretado como "refletindo as preocupações dos EUA sobre a difusão de encriptação forte" (LIU, 2017, p. 319)[14].

Ao longo da década de 1970, contudo, alguns desenvolvimentos no campo criptográfico foram identificados como ameaças potenciais ao controle da agência sobre esse tipo de tecnologia. O LUCIFER/DES era alvo de críticas por suspeitas de um *backdoor* inserido pela NSA, bem como pela limitação sobre o tamanho máximo de chaves. Além disso, a publicação do método de encriptação assimétrica desenvolvido por Diffie e Hellman em 1976 sinalizava a possibilidade de sistemas criptográficos fortes em que chaves poderiam ser trocadas com frequência sem que fosse necessário um terceiro ao qual Estado poderia recorrer para obter acesso excepcional. Em 1979, o diretor da NSA, Bobby Inman, comentava o seguinte a respeito dessas mudanças:

> Da perspectiva da NSA, o cerne do problema é que preocupações maiores sobre a proteção das telecomunicações no setor não-governamental implica maior conhecimento e discussão pública sobre técnicas de proteção das comunicações. A principal dessas técnicas é, é claro, a criptografia. Há um perigo bastante real e crítico de que discussão pública irrestrita de questões criptológicas prejudicará seriamente a habilidade desse governo em conduzir inteligência de sinais e a capacidade desse governo para desempenhar sua missão de proteger informações de segurança nacional de exploração hostil. (INMAN, 1979, p. 130, trad. minha)

Essa contextualização mostra alguns elementos que perpassavam o contexto das políticas de regulação da encriptação nos Estados Unidos na segunda metade do século XX.

[14] Isso se dá devido ao fato de que sistemas com chaves menores são mais fáceis de serem quebrados através de ataques de força bruta (quando se testa todas as senhas/chaves possíveis). Froomkin (1995, p. 735, trad. minha) relata que críticos do LUCIFER/DES consideravam que o padrão foi pensado para que a chave fosse “longa o bastante para frustrar bisbilhoteiros de corporações, mas pequena o bastante para ser quebrada pela NSA”.

Para uma apreensão mais holística do contexto em que as guerras criptográficas se desenvolveriam, todavia, complemento-a com a apresentação de algumas das transformações nas políticas e percepções relativas a criminalidade e segurança pública na sociedade estadunidense entre as décadas de 1970 e 1990.

2.2 William, o Brando

No artigo artigo "Crime e castigo nos Estados Unidos: de Nixon a Clinton", Wacquant (1999) discute o processo de hiperinflação carcerária ocorrido no sistema penal estadunidense no último quarto do século XX. Sua análise de dados do *Bureau of Justice Statistics*, agência do Departamento de Justiça responsável por coletar, analisar e publicar dados relacionados à criminalidade nos EUA, revela um crescimento de 500% na taxa de encarceramento entre 1973 e 1995.

Na doutrina oficial, esse aumento figurava simplesmente como uma resposta ao aumento da criminalidade e da violência. Os dados analisados por Wacquant não indicam, todavia, qualquer aumento no volume total de crimes e delitos. A taxa de homicídios voluntários se manteve essencialmente a mesma em proporção ao crescimento populacional, ao passo que a frequência dos crimes contra bens "baixou de forma uniforme e contínua de 1974 a 1974" (WACQUANT, 1999, p. 44). O autor explica essa disparidade a partir de três séries de fatores: "o declínio do ideal de reabilitação dos prisioneiros, a instrumentalização do medo da violência pelos políticos e pela mídia e a função de mecanismo de controle racial assumido pelo sistema penal americano" (WACQUANT, 1999, p. 39).

O primeiro fator é entendido por ele nos termos de uma convergência entre duas posições. Uma seria a naturalização conservadora da segregação promovida pelas prisões, instituições cuja função seria proteger bons cidadãos inocentes de gente essencialmente má. A outra seria a crítica progressista ao reformismo das políticas de ressocialização, as quais discriminariam negativamente pessoas pobres e negras e acabariam por legitimar a instituição prisional em última análise. O resultado foi o desfinanciamento dos programas de ressocialização e a adesão crescente a um regime de penas fixas ao longo dos anos 1980.

O segundo fator seria a instrumentalização midiático-política da criminalidade para suscitar pânico moral e sufocar reivindicações de movimentos sociais dos anos 60 pela igualdade civil e contra a guerra do Vietnã. Esse processo, promovido por atores dos campos

jornalístico, político e penal, foi encarnado no mote "lei e ordem" com o qual Nixon conduziu sua campanha presidencial. Wacquant destaca o papel da mídia ao definir o tom de urgência com o qual o crime deveria ser tratado, mesmo quando a criminalidade permanecia estável ou diminuia. Nesse contexto, o peso político que uma acusação de laxismo teria operou como um potente incentivo para que atores políticos e penais adotassem um discurso *tough on crime* (duro com o crime).

Por fim, o terceiro fator seria funcional e teria relação com a ordem racial estadunidense. O pânico moral associado à guerra às drogas instaurada ao longo dos anos 1980 legitimaria o recrudescimento do aparato repressivo direcionado a bairros negros e periféricos, bem como a exploração eleitoral do racismo da sociedade estadunidense. Isso se insere no contexto de uma razão securitária neoliberal que não visa a eliminação ou prevenção do crime, uma vez que este deixa de ser um problema social resultante da desigualdade histórica e se torna fruto de uma escolha racional realizada por indivíduos maliciosos.

Foi nesse contexto produzido por décadas de instrumentalização midiático-política da atividade criminal associada a medidas de hiperinflação carcerária que as eleições presidenciais estadunidenses de 1992 foram realizadas. O democrata Bill Clinton saiu vitorioso, não obstante as acusações de que ele teria sido "brando com o crime" durante seu período anterior como governador do Arkansas (APPLEBOME, 1992). Essa imagem seria transformada rapidamente, porém, conforme o governo Clinton trabalharia ativamente pelo recrudescimento das medidas de combate ao crime nos anos seguintes, sobretudo ao chamado Crime Organizado Transnacional (COT).

Pereira (2015) nota, ao analisar a inserção do COT na agenda securitária dos EUA durante a administração Clinton, um marcado discurso de ineditismo em diversos enunciados do governo federal sobre o fenômeno. Nessa narrativa, a globalização e os processos de abertura econômica e política das fronteiras nacionais teriam produzido um fluxo de pessoas, mercadorias e capitais com efeitos facilitadores jamais antes vistos a nível de facilitação da atividade criminal transnacional. Dentre os fatores mobilizados por Clinton para justificar sua posição, um dos mais frequentes era o papel das novas tecnologias. Assim, num discurso realizado na Assembleia Geral da ONU em 1996, por exemplo, Clinton (apud Pereira, 2015, p. 87) afirma:

> [...] o surgimento da era da informação e da tecnologia nos trouxe todos mais próximos e nos deu extraordinárias oportunidades para construir um futuro melhor. Na nossa aldeia global o progresso pode se espalhar rapidamente, mas o problema também pode. Problemas na outra extremidade da cidade logo se tornam uma praga na casa de todo.

O tráfico internacional de pessoas, armas e drogas seria o principal exemplo a despertar preocupações no escopo do COT. A ameaça comunista da guerra fria paulatinamente dera lugar à ameaça do tráfico internacional de drogas enquanto inimigo que justificaria a manutenção e expansão do todo um aparato de vigilância, controle e segurança desenvolvido durante a guerra fria. A diferença seria, no entanto, a popularização das novas tecnologias, o que agravaria a ameaça na visão do governo. O argumento de que a tecnologia ampliaria as oportunidades de participação no crime organizado transnacional teve um papel importante na construção do suposto ineditismo dessa ameaça. Pereira (2015, p. 90), ressalta esse ponto:

> Os argumentos para o crescimento do COT se baseavam também no amplo acesso do cidadão comum a tecnologias revolucionárias a partir dos anos 1990. Teria importância fundamental o avanço das tecnologias via satélite, dos cabos de fibra ótica e da miniaturização e o aumento da capacidade dos computadores. Estes aspectos, somados aos telefones celulares, dinheiro eletrônico e internet, promoveram um aumento exponencial na comunicação, no transporte, na distribuição e, especialmente, no anonimato. Grupos criminosos transnacionais se utilizavam, por exemplo, de celulares e cartões de banco piratas, criptografados ou simplesmente roubados para se proteger de rastreamentos e investigação (Naím, 2006, 22-27).

Essa contextualização de alguns dos processos que marcaram a sociedade estadunidense nos fins do século XX esboça o cenário no qual a criptografia emergirá como objeto de debate público. Pela primeira vez, toda uma terminologia técnica antes restrita a círculos acadêmicos e militares passará a circular no congresso nacional e na mídia.

No centro dos conflitos, um chip chamado *Clipper*.

2.3 Anatomia de uma folha

Em 1992, a companhia *American Telephone and Telegraph* (AT&T) iniciou o desenvolvimento de um telefone no qual as comunicações de voz entre dois usuários

poderiam ser cifradas (SCHULZE, 2017, p. 55) Numa reação rápida, o diretor da NSA, Michael McConnell, acelerou o desenvolvimento do chip *Clipper*, que seria anunciado num comunicado de imprensa pelo governo Clinton em 16 de abril de 1993, poucos meses após o início da nova presidência. O documento ponderava que enquanto a encriptação poderia "ajudar americanos a proteger segredos de negócios e a divulgação não autorizada de informações pessoais, ela também poderia ser usada por terroristas, traficantes de drogas e outros criminosos." (EUA, 1993, trad. minha). Com base nisso, o governo propunha a implementação voluntária do *Clipper* (formalmente denominado MYK-78), um hardware a ser instalado em dispositivos de comunicação vocal telemática[15].

O governo propagandeava o chip como sendo capaz de encriptar "as comunicações telefônicas usando um algoritmo de encriptação mais poderoso que muitos em uso comercial hoje" (EUA, 1993, trad. minha). O algoritmo em questão chamava-se *Skipjack* e sua desenvolvedora havia sido a NSA, instituição que o classificava como secreto (BLAZE, 1994). O segredo envolvendo o *Skipjack* por si só foi motivo de indisposição entre a comunidade técnica e defensores da privacidade, uma vez que o funcionamento da cifra em questão não poderia ser examinado pelo público. O cerne da controvérsia envolvendo o Clipper, contudo, seria o mecanismo de *key escrow*[16] embutido em seu funcionamento.

Froomkin (1995) descreveu exaustivamente o funcionamento do Clipper, bem como a controvérsia que o envolveu, ao longo das quase 200 páginas que constituem seu artigo-livro *The Metaphor is the Key: Cryptography, the Clipper chip and the Constitution* (onde também me inspiro para o título desta monografia). Para os fins desta seção, entretanto, basta reconstituir seu funcionamento em termos bastante gerais.

> Do ponto de vista do usuário, o chip *Clipper* é uma caixa preta: pegue seu telefone com Clipper instalado, disque outro Clipper-fone, aperte um botão vermelho para ativar a funcionalidade de segurança, leia a sequência de caracteres exibida no telefone para a outra parte para confirmar a segurança da conversação e comece a falar. [...] O que acontece durante esses poucos segundos antes do início da

[15] Embora o foco da controvérsia tenha sido o *Clipper*, seu padrão de encriptação, o EES (*Escrowed Encryption Standard*), suscitaria questões similares caso fosse implementado em outros tipos de aparelhos como planejava o governo.

[16] O termo poderia ser traduzido como depósito, custódia ou armazenamento de chave. Como será exposto, o uso do termo *key escrow* foi em si mesmo um dos focos da controvérsia envolvendo o Clipper, pois opositores da tecnologia em questão consideraram que o termo amenizava a relação que ela estabeleceria entre Estado e usuários.

> conversa, e o motivo, são a essência do EES e a fonte da controvérsia. (FROOMKIN, 1995, pp. 753 - 754, tradução minha).

Quando uma nova unidade do *Clipper* fosse produzida, ela receberia dois identificadores únicos que seriam armazenados pelo governo: número de série e chave de unidade do chip. Para aumentar a segurança, a chave de unidade do chip seria dividida em duas partes, cada uma sendo atribuída a um *escrow agent* diferente: uma das partes ficaria com o Instituto Nacional de Padrões e Tecnologias (NIST)[17] e a outra com o Departamento do Tesouro. Um adversário capaz de reunir as duas partes dessa chave seria capaz de decifrar quaisquer conversações travadas entre usuários de dispositivos encriptados com o Clipper.

Para compreender isso, imaginaremos que Alice desejasse iniciar uma conversa com Bob. Ela pega seu Clipperfone, liga para ele e ativa a cifragem. A primeira coisa que ocorre, antes mesmo do estabelecimento de um canal cifrado, é a definição da chave de decifragem da sessão[18]. O *Clipper* não especifica o método de definição dessa chave, de modo que isso ficava a cargo do fabricante do telefone, mas ele impunha aos dois dispositivos participando da conversa o uso da mesma chave de decifragem[19]. Uma vez que ela fosse definida, os dispositivos a comunicariam aos seus respectivos *Clippers* para o início da sessão.

Após o recebimento da chave, os *Clippers* imediatamente impediriam o estabelecimento de um canal à prova de escuta. Isso era feito através da geração e transmissão de uma estrutura de dados denominada LEAF (*Law Enforcement Access Field*), a partir da qual seria possível decifrar a conversa com o com o auxílio dos *escrow agents*. No início da conversa, os dois dispositivos transmitiriam simultaneamente uma LEAF para o outro e testariam a validade da LEAF recebida. Se o dispositivo de Bob recebesse uma LEAF inválida do dispositivo de Alice ou vice-versa, seu *Clipper* bloquearia a conversação com o remetente da LEAF inválida. Isso porque, conforme exposto anteriormente, o funcionamento do *Clipper* fora planejado para que ninguém, exceto um agente governamental autorizado judicialmente, fosse capaz de decifrar as comunicações.

A arquitetura de uma LEAF reflete essa demanda. Para produzi-la, o *Clipper* inicialmente utilizaria a chave de unidade do chip para cifrar a chave da sessão, formando a

[17] O NIST era a antiga Agência Nacional de Padrões após passar por uma redefinição funcional e nominal em 1988

[18] Essa chave permitiria acessar todas as mensagens trocadas no âmbito daquela chamada.

[19] O modelo original do Clipper não continha essa exigência, mas isso foi revisado para que o grampeamento de um único permitisse monitorar todas as conversas nas quais o dispositivo participasse. Caso contrário, para grampear todas as conversas de Érica, por exemplo, seria necessário obter uma ordem judicial para cada dispositivo que houvesse comunicado com o dela.

primeira camada de encriptação. Essa versão cifrada da chave de sessão seria agregada ao número de série do dispositivo e a uma soma de verificação[20] e a esses três dados seria aplicada uma nova cifragem. Essa segunda cifragem seria realizada com o uso da chave de família, uma espécie de chave-mestra comum a todos os *Clippers*.

Se um agente fosse interceptar uma conversa realizada por meio de Clipperfones com as funções de segurança ativadas, ele deveria gravar a sessão inteira, incluindo a LEAF. A primeira coisa a fazer seria então obter a chave de família, caso o agente não a possuísse[21]. De posse da chave de família, o agente seria capaz de decifrar a segunda camada e acessar os três dados: texto cifrado da chave de sessão, número de série do chip e soma de verificação. A seguir, o agente "contataria as duas *escrow agencies*, dando a elas o número de série do chip e um motivo legalmente válido para a escuta" (FROOMKIN, 1995, p. 757, trad. minha), usualmente uma ordem judicial. Se a validade do pedido fosse constatada, cada agência teria de repassar sua parte da chave de unidade do chip. De posse de ambas, ele poderia reconstituir a chave de unidade e decifrar a primeira camada de encriptação, tornando legível a chave de sessão com a qual ele poderia decifrar o conteúdo da conversa.

2.4 Esplendores e misérias do mundo conectado

O anúncio do *Clipper* foi seguido por uma série de audiências públicas convocadas pelo Congresso dos Estados Unidos, as quais continuariam mesmo após o abandono da iniciativa nos anos seguintes. A socióloga Karina Rider analisou 35 dessas audiências realizadas entre os anos de 1993 e 2015, bem como 77 comunicados públicos de membros do congresso acerca do tema no mesmo período. Sua investigação revelou os principais argumentos que conformaram os discursos de oposição ou favorecimento da adoção do *Clipper*.

Defensores do *Clipper* eram essencialmente representantes de diferentes instâncias do Estado: do governo federal, das agências de inteligência e/ou das instituições policiais. A categoria de segurança nacional era fundamental nos discursos desse grupo, cujo argumento principal era de que a encriptação não regulada pelo governo favoreceria o aumento da

[20] Do inglês *checksum*, consiste num código utilizado para verificar a integridade de dados transmitidos por um canal ruídos ou armazenados em algum meio por algum tempo.
[21] Essa chave circularia num circuito especial a ser instalado nos computadores pessoais de agentes das instituições policiais.

atividade criminosa, em particular de crimes ligados a drogas. (RIDER, 2016, p. 15). Nessa narrativa, a encriptação aparecia como uma proteção acionada por criminosos, os quais utilizariam canais cifrados de comunicação que o governo não poderia decifrar.

Tratava-se de um argumento perfeitamente sintonizado com o contexto dos EUA no início dos anos 1990, quando décadas de legitimação político-midiática da urgência de medidas firmes contra o crime (*tough on crime*) se combinavam a um discurso governamental que alardeava o papel das novas tecnologias em tempos de globalização e crime transnacional organizado. Se o governo não pudesse decifrar comunicações, o tráfico de drogas aumentaria. Rider (2016, p.15, trad. minha) denomina essa forma de enquadrar a questão como "problema da decifragem".

Além disso, as dinâmicas institucionais protegeriam os usuários do chip contra abusos do mecanismo de *key escrow*: as forças policiais precisariam seguir procedimentos específicos para acessar às chaves e seria necessário que houvesse uma razão legal válida para tanto. Haveria também todo um leque de regras rígidas relativas ao modo como as chaves seriam armazenadas e gerenciadas. O conjunto de normas, leis, regulamentos, protocolos, algoritmos e concessões que definia os modos pelos quais as comunicações seriam interceptadas era visto como um produtor de privacidade, não como seu violador.

> Consequentemente, para apoiadores [do Clipper], o *key escrow* protegia e aumentava a privacidade porque utilizava competências previstas pela lei e seguia provisões de privacidade específicas que estipulavam as condições para o acesso à chave. Apoiadores construíam o *escrow* como nada além de uma adaptação da autoridade de policiamento para a era digital. (RIDER, 2016, p. 15, trad. minha)

Mas se os fluxos globais de ilícitos e ilicitudes seriam mobilizados com afinco pelos apoiadores do *Clipper*, os fluxos de mercadorias lícitas seriam acionados com igual ou maior veemência por seus opositores, que em sua maioria apareciam como representantes não da sociedade civil, mas do setor empresarial. Assim, o principal discurso mobilizado contra a adoção do chip em questão não apresentava a questão em termos de direito ou de ética, mas de eficiência econômica. Esse discurso, denominado por Rider (2016, p. 15, trad. minha) como "liberalização mercadológica", apontava os efeitos negativos que a regulamentação da encriptação teria na economia. Seus argumentos fundamentais eram três:

Primeiramente, dizia-se, à moda da razão neoliberal, que um setor privado não regulado era necessário para a manutenção de um ambiente inovativo aquecido. A imposição

do *Clipper* constituiria uma intervenção regulatória da qual adviria um ônus para a indústria, o que resultaria em última análise, num efeito inibitório no progresso tecnológico. Em segundo lugar, ressaltava-se a importância da privacidade garantida pela encriptação a competição da indústria estadunidense no mercado global em ascensão. A transmissão de dados financeiros sensíveis para bancos internacionais, filiais e subsidiárias de empresas dos EUA no exterior dependeria de encriptação forte, como o comércio eletrônico em geral. Por fim, o terceiro argumento desse discurso era baseado na relevância da encriptação forte enquanto instrumento publicitário. Esse argumento defendia que os usuários não se sentiriam confortáveis em participar no comércio eletrônico e na economia digital em geral sem a certeza de que sua privacidade seria assegurada. Diante da insegurança em relação a esse ponto, a tendência seria que os usuários ficassem receosos de cibercriminosos e não participassem ou participassem menos, o que resultaria em danos para a indústria.

O segundo discurso mais frequentemente acionado por opositores ao *Clipper* é designado por Rider "ceticismo governamental" (Ibid, p. 15) e se pautava por uma crítica aos possíveis problemas de sistemas estatais de *key escrow*. A socióloga os argumentos principais que estruturavam esse discurso. O primeiro consistia numa crítica à ausência de procedimentos mais rígidos relativos ao modo como os sistemas seriam acionados, o que favoreceria invasões da privacidade. Nessa linha de argumentação, sistemas de *key escrow* não eram vistos como invasivos da privacidade em si mesmos, mas demandariam proteções institucionais bastante robustas para evitar abusos.

O segundo argumento caracterizava o governo federal como inerentemente propenso ao abuso de poder independentemente das proteções institucionais existentes, as quais poderiam apenas atenuar tal propensão. Este ponto de vista considerava os sistemas de *key escrow* invasivos em si mesmos porque eles aumentariam o grau de exposição dos usuários à vigilância estatal. Numa linha de raciocínio similar a essa, a recém-formada *Eletronic Frontier Foundation* se referia ao mecanismo de *key escrow* como *key surrender*[22] com o objetivo de enfatizar a gravidade do que se visava com o *Clipper* (UMAR, 2017, p. 5)

Outro eixo dessa matriz argumentativa era baseado no questionamento da eficiência prática de sistemas de *key escrow* estatal. Opositores à implementação do *Clipper* pontuavam

[22] Em contraponto a uma ideia de custódia ou armazenamento de chave, o termo poderia ser traduzido por algo como "rendição de chave" ou "cessão de chave", o que sugere uma entrega forçosa realizada mediante algum tipo de pressão ou coerção.

que a existência de métodos alternativos para cifragem de comunicações tornariam o sistema, na prática, ineficaz porque criminosos cientes da possibilidade de monitoramento policial escolheriam se comunicar por outros meios em que o monitoramento não pudesse ocorrer. Dentre as alternativas mais comumente citadas estavam produtos estrangeiros e software livre ou de código aberto, os quais encontravam-se crescentemente disponíveis tanto na Web quanto em livros e textos. Ademais, tais sistemas gerariam demasiada burocracia e dispêndio governamental desnecessário.

Schulze (2017) observa dois outros argumentos de natureza técnica a partir dos quais se questionava a eficiência do *Clipper*. O primeiro apontava que a introdução de um canal de acesso para um terceiro implicaria num aumento dos riscos, pois os bancos de dados mantidos pelas agências poderiam cair nas mãos de atores maliciosos. Uma longa matéria intitulada "A Batalha do Chip *Clipper"* (trad. minha) e publicada no *The New York Times* em 12 de junho de 1994 observa: "Como [Whitfield] Diffie nota, o *key escrow* reintroduz a vulnerabilidade que o levou a inventar a encriptação de chave pública – qualquer sistema que dependa de um terceiro de confiança é, por definição, mais fraco que um que não dependa." (LEVY, 1994).

Além disso, a ausência de um escrutínio público sobre o sistema implicou num espaço de questionamento sobre a eficiência propagandeada pelo governo. Esse argumento foi corroborado pela descoberta de vulnerabilidades no *Clipper* pelo pesquisador Matthew Blaze (1994) no ano seguinte ao anúncio original. Blaze demonstrou que seria possível, em linhas muito gerais, comprometer a integridade de uma LEAF sem que ela se tornasse inválida, o que permitiria comunicar-se usando a cifragem do chip sem que fosse o Estado pudesse decifrar tais comunicações. "Além de ser uma má ideia, dizem agora os inimigos do *Clipper*, nem sequer funciona corretamente" (LEVY, 1994) comentava a matéria de 1994 acerca do artigo de Blaze.

A oposição voraz ao *Clipper* entre 1993 e 1996 reverberou fortemente na opinião pública, como atestou um questionário realizado pela CNN em 1994 que teve 80% dos respondentes contra a iniciativa (SCHULZE, 2017, p. 55). Comercialmente, o *Clipper* foi um fracasso: apenas 10 das 15 mil unidades originais foram compradas, em sua maioria pelo governo (DAM e LIN, 1996, p. 174). Como consequência, o governo recuou e abandonou silenciosamente a iniciativa em 1996. Longe de significar o fim das tentativas de regulação da encriptação, o que se viu nos anos seguintes foi uma reconfiguração tática.

2.5 A espiral centrípeta

A partir de 1996, a administração buscou avançar propostas de infraestruturas de gerenciamento de chave (KMI). A diferença essencial em relação ao *Clipper* seria que o Estado abriria mão de tentar impor tecnologias selecionadas por ele. A indústria poderia desenvolver e exportar seus próprios sistemas criptográficos desde que garantisse a existência de alguma forma de recuperação de chave para acesso estatal. Rider (*op. cit.)* nota que muitos dos argumentos mobilizados nos discursos pró-Clipper foram reciclados nos debates de KMI, com a atualização de que as novas propostas eram apresentadas por alguns de seus defensores como uma espécie de meio-termo e em oposição à iniciativa anterior.

Opositores ao *Clipper* similarmente mantiveram os mesmos argumentos baseados em liberalização mercadológica. Regular encriptação inibiria inovação, reduziria lucros, aumentaria custos, prejudicaria a capacidade competitiva global da indústria estadunidense e diminuiria a segurança dos usuários ao introduzir uma vulnerabilidade potencialmente explorável por atores maliciosos. Um ponto relativamente novo que emergiu entre os defensores da liberalização mercadológica durante os debates de KMI foi a importância destacada da encriptação como proteção da propriedade intelectual e contra espionagem corporativa. Dentro desse ponto de vista, a disponibilidade ampla de encriptação forte foi situada como condição para a proteção ordem e associada a lei e a propriedade privada.

Fenômeno similar no discurso de ceticismo governamental: não se poderia confiar no governo sem imensas medidas de proteção da privacidade e mesmo com elas haveria uma propensão ao abuso por parte das agências. Mobilizou-se extensamente, em oposição às iniciativas de KMI, o enquadramento discursivo da encriptação não-regulada como um "método tecnológico para o combate ao crime pelo setor privado" (RIDER, 2016, p. 19). A perspectiva segundo a qual a população confiaria suas chaves ao setor privado, mas em hipótese alguma ao governo, foi expressa numerosas vezes durante tais debates. O deputado Brad Sherman resumiu esse ponto de vista:

> Eu acho que muitas pessoas querem software em que elas possam ter sua própria cópia extra da chave. Algumas poderiam até confiar uma cópia extra da chave a Bill Gates, mas nenhuma das pessoas que me escreveu quer confiar sua chave ao governo (EUA, 197, p. 37, trad. minha.

O sucesso dos discursos de liberalização mercadológica e ceticismo governamental foi acionado por seus defensores para dar um passo à frente e assumir uma postura propositiva. Três contrapropostas legislativas foram apresentadas e apoiadas por grupos de defensores da privacidade, membros do Congresso e representantes da indústria. Todas as contrapropostas partilhavam das seguintes premissas:

> (1) o mercado estava numa posição melhor que o governo para responder à encriptação ubíqua porque os cidadãos confiavam em empresas privadas mais do que eles confiavam no governo federal; (2) um sistema administrado pelo governo exigiria uma burocracia imensa e desnecessária; e (3) realizar os interesses do mercado era bom para a segurança nacional. (RIDER, 2016, p. 20, trad. minha).

A primeira contraproposta foi apresentada em 1996 e consistiu no *Encrypted Communications Privacy Act* (ECPA). O projeto de lei foi descrito pelo senador democrata Patrick Leahy como "pró-empresas, pró-empregos e pró-privacidade" (*apud* RIDER, 2016, p. 20, trad. minha) e como uma resposta aos problemas do furto de informação privada e controle de exportações que "deixava as empresas de alta tecnologia americanas de mãos atadas" (ibid, p. 20, trad. minha).

O projeto facilitava o controle de exportações, definia proteções à privacidade a serem seguidas por sistemas de *key escrow* ou recuperação de chave, proibia o governo de ordenar o uso de um sistema de encriptação específico e criminalizava o uso de encriptação para facilitação de atividades criminosas. Apoiadores do projeto consideravam o último elemento como "pró-privacidade porque protegia as informações pessoais de consumidores" (ibid, p. 20). O projeto recebeu cartas de apoio de grandes nomes da defesa da privacidade como Bruce Schneier e Matthew Blaze.

A segunda proposta foi o *Promotion of Commerce On-line in the Digita Era Act* (*Pro-CODE Act*) de 1996. Seu conteúdo era similar ao ECPA, porém eliminava o controle de exportações totalmente e não incluía a criminalização do uso da encriptação para facilitar ilícitos e sem diretrizes para sistemas de *key escrow* de adesão voluntária - como o *Clipper* havia sido. O *Pro-CODE Act* fora proposto por um grupo bipartidário e era defendido por senadores como os republicanos Conrad Burns e Larry Pressler principalmente à guisa da defesa da competição de empresas dos EUA no exterior e da proteção da privacidade e da propriedade intelectual.

A terceira contraproposta foi o *Security and Freedom through Encryption* (SAFE) *Act* apresentado pelo deputado Bob Goodlatte que similarmente facilitava o controle de exportações e oferecia certas proteções ao setor privado. A popularidade do *SAFE Act* foi imensa: o projeto acumulou "294 co-patrocinadores e foi endossado por várias organizações como a Câmara do Comércio dos EUA, a Associação Nacional de Manufatureiros, a União Americana pelas Liberdades Civis e a Associação Nacional do Rifle" (RIDER, 2016, p. 22). Inobstante seu sucesso midiático, o *SAFE Act* acabou partilhando do mesmo destino do *ECPA* e do *Pro-CODE Act*: as três propostas jamais foram votadas.

As discussões sobre o *Clipper* entre 1993 e 1996 haviam feito proliferar dois grupos de argumentos que se alicerçavam em premissas distintas a respeito do mundo e das entidades que o compõem. Apoiadores do *Clipper* se colocavam antes de mais nada contra a ameaça representada por traficantes transnacionais de drogas - seu tipo ideal de criminoso[23] (SCHULZE, 2017, p. 57) –, indivíduos cujas condutas não representariam uma ameaça apenas para outros indivíduos, mas para a segurança nacional.

Nesse sentido, o discurso securitário pró-*Clipper* era em nome de algo maior que a soma dos indivíduos, era um discurso em nome da sociedade. Abusos potenciais por parte do Estado eram reconhecidos como um mal necessário que se deveria mitigar por meio de proteções institucionais. A privacidade, interesse individual, precisaria ser equilibrada com a segurança, interesse coletivo. O elemento fundamental para essa segurança, aquele do qual verdadeiramente não se poderia abrir mão era a vigilância sobre os criminosos, pois a América estava em meio a uma guerra contra as drogas e a guerra exigia certos sacrifícios.

O grupo anti-*Clipper*, por sua vez, construiu seu caso a partir de uma oposição entre uma sociedade civil composta por sujeitos auto interessados realizando trocas voluntárias de acordo com leis naturais e um Estado anômalo cujas intervenções regulatórias tendem à ineficiência e à produção de externalidades negativas. Esses pressupostos cosmológicos ofereceram a base comum para os discursos de liberalização mercadológica e ceticismo governamental. Tal posicionamento era irreconciliável com a implementação do *Clipper* porque a ameaça primária nesse prisma era o próprio Estado cuja ação regulatória reduziria a liberdade.

[23] Outros crimes como terrorismo e pornografia infantil também eram acionados como justificativas para a implementação do *Clipper*, embora com menos frequência.

E de que liberdade se está a falar? Da liberdade do indivíduo comunicar-se sem a possibilidade de vigilância estatal? Sim, em alguma medida, mas sobretudo da liberdade de empresas de tecnologia para selecionar, desenvolver e exportar seus produtos como melhor julgassem. O que havia de inerentemente problemático na vigilância estatal é menos a vigilância e mais seu caráter estatal. Daí o modo como a privacidade aparecia nos discursos de liberalização mercadológica: como um meio para garantir a competitividade da indústria estadunidense na economia global.

Isso explica o movimento centripetal que envolveu o debate a partir de 1996. Defensores do *Clipper* passaram a apoiar iniciativas de KMI como uma concessão à liberdade de mercado, pois as empresas poderiam escolher suas próprias tecnologias de decifragem. De modo correlato, apoiadores das contrapropostas buscaram uma aproximação com a demanda de segurança nacional ao atualizar seu discurso para ressaltar a importância de assegurar a dominação da indústria nacional na economia digital para os fins de segurança pública. Além disso, o setor empresarial se comprometeria a cooperar com as forças de segurança e agências de inteligência para garantir a elas acesso às comunicações decifradas.

O principal argumento propagado por apoiadores desta perspectiva era que seria do interesse nacional "encorajar a adoção generalizada de produtos criptográficos dos EUA porque companhias americanas estariam mais dispostas a cooperar com agências de inteligência e instituições policiais que empresas estrangeiras" (RIDER, 2016, p. 22). Esse tipo de posicionamento foi reiterado em diversas instâncias entre 1996 e 1999. Por exemplo, numa audiência pública realizada em 1997 a respeito do *Safe Act*, o deputado Bob Goodlatte questionou Ira Rubinstein, um advogado sênior da Microsoft, se ele concordaria com a afirmação de que haveria uma dicotomia entre "as necessidades da indústria e as necessidades das forças policiais" (EUA, 1997b, p. 15)". Ao que Rubinstein (ibid.) responde prontamente:

> Não, eu não concordo com isso de modo algum. Eu acredito que a indústria está na posição de auxiliar as forças policiais e de segurança nacional em alcançar seus objetivos porque nós somos capazes de vender produtos dos EUA em volume massivo. [...]

Em outra audiência realizada no mesmo ano, o deputado Rick White (ibid, trad. minha) pondera: "se nós não a produzirmos [a encriptação] aqui e se o nosso governo não entender e tiver relações com as pessoas que a produzem, nós seremos menos capazes, em

vez de mais capazes, de decifrar mensagens cifradas no futuro". Já em 1999, o deputado Patrick J. Kennedy (apud RIDER, 2016, p. 23, trad. minha) reflete:

> Penso que nós precisamos co-optar, digamos assim, a alta tecnologia americana… Se pretendemos ser líderes no mundo para nossos propósitos de segurança nacional, me parece que vamos desejar trabalhar com elas [as empresas] e garantir que essas coisas serão vendidas de qualquer forma, então por que não assegurar que elas estarão do nosso lado? Se o produto está sendo vendido pelo mundo todo, por que não garantir que é o nosso produto, de empresas domésticas que tenham alguma aliança e algum interesse nesse país porque elas conhecem e apreciam o valor do nosso grande país.

A análise desses enunciados evidencia que um certo meio-termo conceitual começava a ser produzido em torno da ideia de aumento, a médio prazo, da capacidade de vigilância do Estado *através* da ausência de regulação sobre a encriptação.

No batalha do *Clipper*, as antinomias conceituais entre privacidade e segurança (na perspectiva pró-*Clipper*) ou privacidade e vigilância (na leitura anti-*Clipper*) haviam sido o efeito da forma como essa tecnologia específica organizava os interesses econômicos do mercado e securitários de setores do Estado. Para a indústria, o *Clipper* significava menos espaço para atualização e lançamento de novos produtos, bem como um poderoso recurso publicitário para suscitar engajamento de consumidores, ao passo que a vigilância equivaleria a uma intervenção regulatória que impunha uma série de ônus financeiros. Para o Estado, a o chip era um aumento em sua capacidade de recuperação de informações produzidas e veiculadas através da tecnologia. Sua não-implementação, por outro lado, significava uma redução efetiva em sua capacidade investigativa, pois o volume de informação cresceria de um modo que seria impossível acompanhar.

Entre 1996 e 1999, uma readequação tática mútua permitiu desaparecer com tais antinomias. Do Estado, o reconhecimento da importância de encriptação não-regulada para a hegemonia industrial nacional na economia digital. Do mercado, garantias de cooperação para que as autoridades acessassem às comunicações decifradas de criminosos, desde que nenhuma intervenção regulatória impedisse a popularização dos produtos – caso no qual o Estado precisaria negociar com empresas de outro país. O que ocorreu, segundo Rider, foi uma instrumentalização da privacidade a serviço da vigilância:

> A habilidade de assegurar a privacidade para consumidores em transações de mercado contra criminosos foi, portanto, atrelada a ofertas para trabalhar

> cooperativamente com o governo a fim de garantir que as instituições policiais e agências de inteligência obtivessem comunicações decifradas. A privacidade contra criminosos no mercado teve o efeito paradoxal de facilitar a redução da privacidade contra a vigilância policial. (RIDER, 2016, p. 24 - 25, trad. minha)

2.6 Liberdade ainda que tardia

Os últimos anos da década de 1990 pareciam ser também os últimos anos das guerras criptográficas. As tentativas do governo Clinton de implementação massiva do *Clipper* tinham sido um tremendo fracasso e desgastado a imagem da administração com a opinião pública no processo. Clinton tampouco obtivera grandes avanços com suas proposições de infraestruturas de gerenciamento de chave. Todas as tentativas de produzir um sistema de *key escrow* no qual o governo federal manteria a custódia das chaves tinham sido ineficazes.

Em 1997, nova vitória do movimento contra controle estatal sobre encriptação: a responsabilidade pela emissão de licenças de exportação de produtos criptográficos seria transferida do Departamento de Estado para o Departamento de Comércio, sendo este último mais sensível às reivindicações da indústria por regulamentações mais frouxas. Apesar dos protestos do FBI contra a flexibilização dessas regulações (CNET, 1998), o controle das instituições de segurança sobre a encriptação parecia estar sendo cada vez mais refreado. O ativista John Gilmore resumiu o sentimento otimista de alguns dos envolvidos no conflito: "1997 pode ser o ano em que nós finalmente vencemos as guerras criptográficas" (LAPPIN, 1997).

Embora a previsão de Gilmore viesse se provar apressada, a privacidade parecia ganhar terreno cada vez maior na guerra contra a vigilância estatal. O ano de 1999 traria um novo desenvolvimento: o anúncio realizado pela Casa Branca de que o governo federal estaria afrouxando as regulamentações existentes sobre o controle de exportações criptográficas (THOMPSON et al, 2015). Embora o mesmo anúncio sinalizasse a introdução de um novo projeto voltado à instauração de um mecanismo de *key escrow* estatal, era evidente para muitos dos envolvidos no debate que o projeto não iria a lugar algum (BLACK, 2001, p. 308).

Não por acaso, 1999 foi o último ano em que o debate público das guerras criptográficas foi intensamente realizado. Em comparação com as 4 audiências públicas e 17

comunicados de imprensa emitidos no Congresso a respeito da temática da regulação de encriptação em 1999, o ano seguinte teve um total de 0 audiências públicas e 0 comunicados (RIDER, 2016, p. 25). Ao que tudo indicava, as guerras criptográficas tinham finalmente acabado. O artigo *Taking Account of the World As it Will Be: The Shifting Course of U.S. Encryption Policy* publicado no *Federal Communications Law Journal* em 2001 comentava a mudança com certo otimismo:

> Cada clichê espalhado durante os últimos cinco anos - a estrada da informação, a revolução tecnológica, a era da informação - é literalmente verdade, mesmo que sejam utilizados exageradamente. A tecnologia de encriptação está na vanguarda dos próximos desenvolvimentos nas áreas de comércio eletrônico, varejo online e na criação de um mundo interconectado. Ao nivelar o campo de jogo com competidores estrangeiros, o recente relaxamento das regulações sobre encriptação certamente será benéfico para a indústria de alta tecnologia dos Estados Unidos. (BLACK, 2001, p. 314)

O novo milênio, tudo indicava, seria uma era de liberdades: liberdade para acessar a informação a qualquer momento e em qualquer lugar, liberdade para o desenvolvimento e exportação de produtos sem a intervenção regulatória do Estado, liberdade para que usuários pudessem se comunicar sem que o Estado pudesse interceptar o conteúdo de suas comunicações. Ainda que tivesse demorado quase uma década, as guerras criptográficas finalmente pareciam ter sido vencidas. Tempos áureos viriam, tempos em que a liberdade e a privacidade do indivíduo triunfariam incontestadas sobre os olhos curiosos do *Big Brother*.

Ou assim parecia.

CAPÍTULO 3 – EM NOME DA AMÉRICA

3.1 Coletar o palheiro

A despeito do silenciamento dos debates em torno do acesso público à encriptação forte, numerosas outras guerras irromperam durante os primeiros anos do terceiro milênio . Da já conhecida guerra às drogas à logo declarada guerra ao terror e seus desdobramentos nas invasões do Afeganistão e do Iraque, era como se a lista de inimigos públicos dos Estados Unidos estivesse em permanente aumento. Consequentemente, a demanda por novas e mais eficazes tecnologias de vigilância não parava de crescer. A expansão do aparato tecnológico e jurídico de vigilância dos Estados Unidos após o atentado terrorista de 11 de setembro de 2001 tem sido alvo de amplas discussões (CHEVIGNEY, 2004; RAMIREZ PARTIDA, 2014). Menos discutido, porém de igual significância, foi um fato ocorrido ainda no ano 2000, mesmo ano em a palavra “encriptação” praticamente desapareceu dos comunicados de imprensa e das pautas de audiências públicas do Congresso.

O evento a que me refiro foi o início de um programa secreto intitulado Bullrun pela NSA (PERLROTH et al., 2013), cujo objetivo consistia em

> tornar softwares comerciais de encriptação "mais tratáveis" para ataques da NSA ao "moldar" o mercado mundial e seguindo com os esforços para quebrar a encriptação usada pela próxima geração de telefones 4G (BALL et al., 2013, trad. minha)

Diversos métodos seriam empregados para alcançar esse objetivo, alguns dos mais importantes sendo parcial ou inteiramente baseados na cooperação entre a NSA e as empresas de tecnologia. Ao “obter sua cooperação voluntária, forçar sua cooperação com ordens judiciais ou furtivamente roubar suas chaves criptográficas ou alterar seu software ou hardware” (PERLROTH et al., 2013), a NSA foi capaz de fazer um uso ótimo da popularização dos produtos estadunidenses que a encriptação não-regulada havia favorecido. A verba do projeto em 2013, $ 254.9 milhões, superava em mais de 1000% a verba de outro grande programa de vigilância da agência, o PRISM, no mesmo ano.

Para compreender tamanho investimento é necessário situá-lo na racionalidade mais ampla que direcionou as ações da NSA ao longo de toda a década de 2000. A estratégia na qual o programa se inseria fora concebida pelo então diretor da agência, o general Keith Alexander, e aplicada originalmente no contexto da guerra do Iraque. O fundamento tático da

ação é bastante simples e podia ser resumido na seguinte metáfora: em vez de procurar por uma agulha no palheiro, coleta-se o palheiro inteiro (NAKASHIMA e WARRICK, 2013).

Assim, a NSA armazenava todas as comunicações eletrônicas possíveis, estivessem elas cifradas ou não, para posteriormente viabilizar sua decifragem. Um memorando de 2010 descrevia um avanço recente do Bullrun da seguinte forma: "Uma vasta quantia de dados cifrados da Internet que até então haviam sido descartados agora são exploráveis." (PERLROTH et al, 2013.). O que se fazia era materializar a estratégia anunciada durante os anos de discussão sobre KMI e as contrapropostas das guerras criptográficas originais: facilitar a massificação de produtos tecnológicos industriais estadunidenses no mundo para facilitar a coleta das comunicações eletrônicas e paralelamente utilizar de cooperação e (se necessário) coerção para assegurar o acesso às comunicações decifradas.

Ainda que os nomes das empresas que cooperaram com a NSA permaneçam em segredo de modo geral, um caso publicizado em 2010 é emblemático. O caso em questão dizia respeito a uma empresa denominada *RSA Data Security Inc.*, a qual havia sido fundada por Ron **R**ivest, Adi **S**hamir e Len **A**dleman, pesquisadores responsáveis pelo primeiro sistema criptográfico assimétrico forte a ganhar grande difusão, o RSA, sistema que implementara bastante cedo a encriptação de Diffie-Hellman.

Em 1994, auge do conflito envolvendo o *Clipper*, o então presidente da empresa, James Bidzos, disse ao *The New York Times*: "O sucesso dessa empresa [a RSA] é a pior coisa que pode acontecer a eles [agências de inteligência]. Para eles, nós somos o verdadeiro inimigo, nós somos o verdadeiro alvo" (LEVY, 1994). Quando os documentos de Snowden vieram a público em 2013, uma das revelações foi a existência de um acordo de $ 10 milhões para que a RSA permitisse à NSA definir o método padrão ou preferencial para geração de números em um dos principais produtos de segurança distribuídos pela empresa para uso em computadores e outros dispositivos, o software BSafe. (MENN, 2013).

O que ocorreu entre 1999 e 2000 pode ser compreendido, portanto, como uma transferência das discussões para um canal sigiloso no qual os setores que já protagonizavam o debate público (indústria e Estado) poderiam conversar e decidir livremente sobre a questão, ao passo que outros setores menos centrais na condução dessas discussões foram excluídos. Esse movimento possibilitou à NSA e às empresas de tecnologia o desenvolvimento de soluções convenientes tanto com a expansão das capacidades de

vigilância estatal quanto com a manutenção de um ambiente mercadológico não regulamentado.

A análise de dados quantitativos referentes às participações nas audiências públicas conduzidas pelo congresso corroboram esse ponto. Rider registra os seguintes números entre 1991 e 1999: de um total de 174 participações, 73 eram do setor empresarial, 65 do setor estatal (sendo 15 das agências de inteligência, 19 das polícias e 31 de outras instâncias do governo), 17 de organizações da sociedade civil, 13 do setor acadêmico e 6 diversas. Os números em questão indicam que o debate público já era conduzido predominantemente por representantes de interesses estatais e mercadológicos. Esses setores não eram centrais somente no nível dos enunciados, mas também e sobretudo no nível dos sujeitos que realizavam as discussões.

A estratégia adotada revelou-se excepcionalmente vantajosa para ambos os setores. A indústria de tecnologia da informação dos Estados Unidos conseguiu multiplicar incomensuravelmente o alcance de seus produtos. Empresas como Google, Apple, Facebook, Amazon, Microsoft, dentre outras, dominaram o mercado da inovação digital. O Estado estadunidense, por sua vez, foi beneficiado tanto economicamente quanto a nível securitário, uma vez que algumas dessas e de outras empresas participariam ativamente nos programas de vigilância empregados pela NSA ao longo da década de 2000. Tudo estava bem enquanto os programas em questão eram sigilosos.

Então veio Snowden.

3.2 O efeito Snowden

Nos meses finais de 2012 e iniciais de 2013, o ex funcionário da CIA Edward Joseph Snowden entrou em contato com jornalistas Glenn Greenwald, Laura Poitras e Ewen MacAskill. Snowden, então funcionário da *Booz Allen Hamilton* – uma das maiores prestadoras de serviços para a NSA – compartilhou com a dupla milhares de documentos secretos relativos a programas de vigilância global levados a cabo pela NSA e por governos dos países do grupo da Aliança de Inteligência dos Cinco Olhos[24].

[24] Aliança de inteligência formada pela Austrália, Canadá, Nova Zelândia, Reino Unido e Estados Unidos (LYON, 2016, p. 25).

A publicização dos programas em questão através de uma onda de matérias inicialmente publicadas em junho de 2013 tomou de assalto os debates internacionais do período. Com base em Lyon (2016), pode-se destacar três elementos das práticas de vigilância massiva que ganharam destaque com as revelações: i) governos de democracias ocidentais liberais comumente tidos como não-autoritários espionam massivamente as comunicações privadas de seus cidadãos; ii) eles o fazem com a conivência das grandes empresas de tecnologia da informação; iii) as práticas de consumo dos cidadãos são talvez a principal fonte a partir da qual tais dados são produzidos e coletados.

Dentre os grandes programas então revelados estavam o Bullrun e o programa PRISM. Esse último garantia à NSA acesso ao conteúdo de e-mails, históricos de buscas, arquivos transferidos e mensagens trocadas por usuários em aplicações fornecidas por grandes empresas de tecnologia como Microsoft, Yahoo, Google, Facebook e Apple. Um dos documentos adquiridos por Greenwald acerca do PRISM mostrava especificamente a cooperação da Apple com o programa a partir de 2012. Na ocasião das revelações, todavia, a Apple negou já ter ouvido falar no PRISM (GREENWALD, 2013).

Os impactos e as implicações políticas, econômicas e culturais dessas revelações ainda estão sendo debatidos e experienciados, de modo que é difícil avaliar com precisão sua extensão. É inegável, contudo, que o acontecimento Snowden elevou significativamente a dimensão do debate público sobre a mediação sociotécnica operada pelas tecnologias digitais nas relações entre pessoas, Estados e empresas de tecnologia, em especial no que diz respeito a questões como privacidade, segurança e liberdades civis. No Brasil, por exemplo, impactos das revelações de Snowden influenciaram imensamente a aprovação do Marco Civil da Internet (SOLAGNA et al., 2015) e o desenvolvimento do cabo submarino Ellalink, que conecta o Brasil e a Europa sem a mediação estadunidense(BLANC e POZNANSKI, 2017).

Quanto à encriptação, observou-se uma resposta mercadológica voltada à valorização da privacidade. Hoboken e Schulz (2016, p. 10) constatam, por exemplo, um "aumento notório na disponibilidade de ferramentas de encriptação ponta-a-ponta[25] desenvolvidas e disponibilizadas para os usuários" após Snowden. Diversos provedores de serviços-web

[25] Recurso de segurança destinado a assegurar que somente as partes se comunicando tenham acesso ao conteúdo comunicado. Quando utilizado, a mensagem é cifrada em uma ponta da comunicação e só é decifrada na outra ponta. Em princípio, isso garantiria que nenhum terceiro tenha acesso ao conteúdo comunicado, incluindo o próprio provedor de serviço.

também passaram a adotar o protocolo TLS[26] em seus sites após as revelações em questão. Ao comentar a respeito do fenômeno em 2016, o diretor de inteligência nacional dos Estados Unidos, James Clapper, alegou que "Como resultado das revelações de Snowden, a implementação da encriptação comercial foi acelerada em 7 anos." (MCLAUGHLIN, 2016, trad. minha)

A Apple, especificamente, introduziu uma modificação decisiva na encriptação de seus produtos após as revelações em questão. Para entender o significado da decisão tomada pela empresa torna-se necessário examinar brevemente a evolução dos níveis de encriptação empregados nos produtos da empresa em questão ao longo do tempo. Esse exercício foi realizado pelas analistas forenses Heather Mahalik, Cindy Murphy e Sarah Edwards (2016). Apresento aqui uma breve síntese de suas constatações relativas às mudanças do período entre 2010 e 2016.

Entre 2010 e 2011, o nível máximo de segurança que usuários da Apple teriam no iPhone seria em dispositivos contendo o chip A4 (iPhone 4, iPad). Se um adversário apreendesse um dispositivo do tipo, seria relativamente fácil obter acesso a todo ou à maior parte do conteúdo armazenado no aparelho sem que para isso fosse necessário conhecimento prévio da senha. Seria possível fazê-lo por meio da extração de uma imagem de disco, ou seja, grosso modo, da produção de uma cópia da estrutura e do conteúdo da unidade.

Isso mudaria com o lançamento do chip A5 em 2011, chip esse presente no iPhone 4S e no iPad 2. Dispositivos contendo o chip em questão traziam encriptação forte no nível do hardware que agora utilizava um dos padrões de encriptação simétrica mais seguros existentes, o *Advanced Encryption Standard* (AES) de 256 bits. Um dos principais efeitos do novo design era aumentar a segurança do sistema ao proteger o conteúdo dos arquivos contra acesso indevido por meio da extração de imagens de disco. Se um adversário realizasse o procedimento em questão nos novos dispositivos, ele obteria acesso apenas ao sistema de arquivos e aos metadados dos arquivos, não a seu conteúdo. Esse conteúdo permaneceria cifrado, a menos que a senha do usuário fosse empregada para decifrá-lo antes da extração da imagem.

[26] *Transport Layer Security* (TLS), protocolo de segurança utilizado em serviços web para autenticação das partes envolvidas e cifragem dos dados transmitidos entre elas, o que visa assegurar a integridade e a confidencialidade dessas informações.

Isso se dá devido à forma como a encriptação funciona nesses novos dispositivos. Cada aparelho contém um identificador único e exclusivo na forma de uma chave atribuída ao aparelho durante sua fabricação, o chamado UID. Esse dado não pode ser lido diretamente, somente os resultados das operações de cifragem e decifragem que o envolvem. Além disso, o UID assegura que os dados estejam criptograficamente atrelados àquele dispositivo particular, o que torna os arquivos inacessíveis caso os chips de memória sejam movidos fisicamente de um aparelho para outro (APPLE INC., 2012, p. 7).

Ao definir uma senha para o dispositivo, o usuário de um iPhone portador do chip A4 ativa automaticamente uma tecnologia intitulada Proteção de Dados. Essa tecnologia combina a senha escolhida ao UID do dispositivo para gerar uma chave com a qual os arquivos são cifrados. Sempre que o usuário digita sua senha para desbloquear a tela, o algoritmo de decifragem recombina a senha ao UID para reconstruir essa chave[27] e decifrar os arquivos. O adversário é forçado a realizar tentativas de bloqueio naquele dispositivo específico porque a chave não pode ser reconstruída sem o UID e o UID não pode ser lido por nenhum software. Na prática, o efeito de tudo isso era impossibilitar a decifragem do conteúdo dos arquivos sem o conhecimento prévio da senha definida do usuário.

A alternativa restante para um adversário seria, então, o emprego de um ataque criptoanalítico de força bruta. Ciente dessa possibilidade, a Apple (2012, p. 9) adicionou duas funções extras destinadas a "desencorajar ainda mais ataques de força bruta": i) um tempo de espera crescente a partir de cada tentativa mal sucedida; ii) uma função de ativação opcional que destrói uma das chaves necessárias para acessar os dados após 10 tentativas falhas de inserção da senha. Essas duas funções inviabilizavam ataques de força bruta, pois além do tempo absurdo que se levaria para realizá-los, 10 tentativas falhas destruiriam o conteúdo que se pretende ler caso a função opcional esteja ativada[28].

Essa era a encriptação empregada no iPhone antes de Snowden, mas depois dele o tratamento dado à encriptação pela Apple passaria por uma mudança importante, como se pode constatar num anúncio realizado em setembro de de 2014, pouco antes do lançamento da versão 8 do iOS. Na ocasião, a empresa lançou um novo site destinado a aumentar sua

[27] Por se tratar de encriptação simétrica, a mesma chave é utilizada para cifrar e decifrar os arquivos.
[28] Gilmor (2016) sugere uma forma de contornar essa função, porém o tempo de espera automático entre as tentativas permaneceria existindo.

transparência ao explicitar sua política de privacidade de forma detalhada. A página central do site mostrava uma carta aberta assinada por Tim Cook acerca da privacidade.

Na carta, o presidente da empresa enfatizava a importância que a privacidade teria para a Apple como um diferencial em relação a outras empresas de tecnologia. Além de negar a cooperação prévia da empresa com a vigilância estatal, Cook explicita a política de privacidade da companhia através do que poderia ser lido como um ataque evidente aos modelos de negócios de companhias rivais como Google e Facebook[29]:

> Alguns anos atrás, usuários de serviços da internet começaram a perceber que quando um serviço online é gratuito, você não é o cliente. Você é o produto. Mas na Apple, nós acreditamos que uma ótima experiência enquanto consumidor não deveria vir às custas da sua privacidade. Nosso modelo de negócios é bastante direto: Nós vendemos ótimos produtos. Nós não construímos um perfil baseado no conteúdo dos seus e-mails ou hábitos de navegação para vender para anunciantes. Nós não "monetizamos" a informação que você armazena no seu iPhone ou no iCloud. E nós não lemos o seu e-mail ou suas mensagens para obter informação. (COOK apud MCGARRY, 2014).

Em outra parte do site, a empresa trazia uma seção especialmente dedicada à política da Apple em relação a mandados do governo. Nessa seção, a Apple assegurava a seus usuários que a encriptação utilizada no iOS 8 impediria a própria companhia de cooperar com mandados judiciais que demandassem a extração de informações dos usuários a partir de dispositivos apreendidos pelo governo. Segundo a empresa, tal conteúdo estaria inacessível para qualquer um que não conhecesse a senha definida pelo usuário, incluindo a própria Apple (QUIRK, 2014; APPLE INC., 2017: p. 10).

Isso ocorre devido a uma mudança no modo como a Proteção de Dados é empregada na nova versão do iOS. Na versão anterior do guia de segurança do iPhone, lançada em fevereiro de 2014, seção "*Encryption and Data Protection*", subseção "*File Data Protection*", lê-se: "O Mail usa Proteção de Dados por padrão e aplicativos de terceiros instalados no iOS 7 ou posterior recebem essa proteção automaticamente" (APPLE INC., 2014a: p. 9, ênfase minha). O significado disso era que toda a sofisticada infraestrutura

[29] Ambas as empresas são conhecidas por monetizar os dados de seus usuários, usualmente através do direcionamento de anúncios personalizados a partir dos dados resultantes do monitoramento de seus comportamentos. Zuboff (2015, p. 77) denomina tal lógica de acumulação de capital como "capitalismo de vigilância".

técnica de encriptação utilizada não era aplicada à maior parte dos arquivos do sistema, somente àqueles referentes aos e-mails trocados no Mail.

Na versão seguinte do Guia de Segurança, por outro lado, pode-se constatar uma mudança. Na mesma seção, mesma subseção do documento, agora lê-se:

> Os aplicativos principais do sistema como o Mensagens, Mail, Calendário, Contatos, Fotos e os valores de dados do Saúde, usam Proteção de Dados por padrão, e os aplicativos de terceiros instalados no iOS 7 ou posterior recebem essa proteção automaticamente. (APPLE INC., 2014b: p. 10, ênfase minha)

Isto é, agora a empresa estendia todo o seu poder criptográfico a um extenso leque de aplicativos anteriormente excluídos dela, incluindo os de Mensagens pessoais. Assim, embora os níveis de encriptação empregados no iPhone tenham aumentado historicamente a cada lançamento, essa escolha pós-Snowden teve efeitos bastante específicos nas relações entre a empresa, seus consumidores e as instituições policiais. A mudança foi resumida pelo pesquisador e ativista Christopher Soghoian (2014, trad. minha) da seguinte forma: "A política antiga da Apple para extrair dados dos usuários para a polícia a partir de iPhones: Volte com um mandado. Sua política nova: Cai fora."

Cerca de um mês após o anúncio, o diretor do FBI, James Comey, fez referência a essa mudança numa palestra intitulada "Obscurecimento: Tecnologia, Privacidade e Segurança Pública estão em Rota de Colisão?". O argumento central da palestra era que as revelações de Snowden teriam levado à uma "perspectiva dominante" (COMEY, 2014), porém equivocada, segundo a qual o Estado estaria coletando todas as comunicações dos cidadãos. Para Comey, "o pêndulo pós-Snowden balançou demais para uma direção - a direção de medo e desconfiança" (ibid.) em relação ao Estado.

Para o diretor, ao contrário, a popularização das tecnologias digitais teria levado ao problema que ele denomina "obscurecimento"[30]: uma lacuna existente entre a autoridade legal das forças policiais para interceptar comunicações em conformidade com mandados judiciais e sua incapacidade técnica para fazê-lo devido ao uso de encriptação. Nessa narrativa, "toda a esfera das comunicações digitais poderia estar metaforicamente envolta em escuridão, ilegível para a NSA." (SCHULZE, 217, p. 55). "Em nome da privacidade e

[30] Do inglês *Going Dark*, o termo é utilizado no jargão militar para designar uma interrupção súbita da comunicação. A expressão costumava se referir a uma situação em que a comunicação parece ter cessado, mas na verdade foi apenas deslocada de um canal passível de monitoramento para um canal privado e protegido contra escutas. O termo foi traduzido como "obscurecimento" pelo Instituto de Tecnologia e Sociedade do Rio em sua publicação brasileira de Berkman (2018).

segurança de rede" (COMEY, 2014), essa esfera estaria tornando-se um território em que condutas criminosas poderiam ser realizadas livremente. Na ocasião da palestra, Comey explicitamente comentou a respeito das novas medidas de encriptação anunciadas pela Apple afirmar que a encriptação "não é apenas uma característica técnica, é uma jogada de marketing" (ibid.).

3.3 A aliança rompida

Não tardou para que a tensão entre a implementação de medidas destinadas ao aumento da privacidade por parte de grandes empresas de tecnologia da informação e os interesses securitários das instituições policiais resultasse na deflagração de um novo conflito. No ano seguinte à palestra de Comey, um caso envolvendo um iPhone cujo conteúdo o FBI não conseguia acessar devido à encriptação resultaria no que atores diversos enquadrariam como um novo capítulo nas guerras criptográficas dos anos 1990. Descrevo os aspectos principais do caso a seguir.

Em 2 de dezembro de 2015, um atentado terrorista deixou 14 pessoas mortas e 22 pessoas feridas no Inland Regional Center, em San Bernardino, Califórnia. O ataque ocorreu durante um evento de treinamento de pessoal e festa natalina promovida pelo Departamento de Saúde Pública do Condado de San Bernardino (SBCDPH) e consistiu num tiroteio e numa tentativa malsucedida de explosão (MEDINA et al., 2015). Os atiradores, o casal Syed Rizwan Farook e Tashfeen Malik, fugiram imediatamente após o tiroteio em um veículo alugado. Farook e Malik foram localizados e perseguidos pela polícia algumas horas após o ataque, o que resultou nas mortes de ambos em meio a uma troca de tiros com a polícia.

Nos dias seguintes ao ataque, o grupo terrorista internacional Estado Islâmico do Iraque e do Levante (EIIL) declarou durante uma transmissão de rádio online que Farook e Malik eram seus seguidores. James Comey, veio a público informar que as investigações evidenciavam sinais de radicalização e inspiração por grupos terroristas por parte do casal, embora não houvesse evidências de que os dois fizessem parte de uma rede terrorista maior. Além disso, o FBI declarou ainda que havia recuperado dois celulares atribuídos ao casal, porém ambos estavam destruídos e haviam sido descartados numa lixeira porque os atiradores haviam tentado destruir seus "rastros digitais" (SERRANO et al., 2015).

Alguns meses depois, no dia 9 de fevereiro de 2016, Comey afirmou em audiência pública que o FBI havia adquirido outro celular pertencente a um dos atiradores e que, embora a agência estivesse trabalhando nisso pelos dois meses anteriores, o FBI não conseguia acessar as informações contidas no dispositivo, pois o conteúdo do aparelho estava cifrado (EUA, 2016a, p. 43). Na ocasião, o diretor do FBI acrescentou que o uso da encriptação estava "afetando de forma esmagadora" (Ibid.) as forças policiais ao impedir o acesso tanto a comunicações trocadas através de cabos de fibra ótica – como em aplicativos de mensagens – quanto a dados armazenados em celulares protegidos por senhas (caso do celular em questão). O dispositivo, um iPhone 5C, estava protegido com uma senha definida pelo usuário sem a qual não era possível acessar seu conteúdo decifrado.

Em 16 de fevereiro, O FBI entrou com um pedido para que a Apple auxiliasse as forças policiais a acessar o conteúdo do celular em questão (EUA, 2016c). No mesmo dia, a juíza Sheri Pym, do Tribunal Distrital da Califórnia, emitiu uma ordem judicial compelindo a empresa a prover "assistência técnica razoável" (EUA, 2016c, p. 2) para os agentes da lei no acesso ao conteúdo do dispositivo. Ainda naquele dia, a Apple respondeu com a publicação de uma mensagem assinada por seu presidente (COOK, 2016b) e destinada a seus consumidores. Na carta, a empresa fazia uma oposição contundente ao pedido e expunha os motivos de sua recusa em cumprir a ordem judicial. Três dias depois, o Departamento de Justiça (DoJ) entrou com um pedido para que a Apple fosse compelida a cumprir a ordem (EUA, 2016d), ao qual a empresa respondeu em 25 de fevereiro com um pedido de revogação da ordem (EUA, 2016e). Uma audiência sobre o caso foi marcada para o dia 22 de março.

Nas semanas seguintes, Tim Cook, o então presidente da companhia, falou na mídia numerosas vezes sobre os motivos que o levaram a se opor à ordem judicial do governo. A cobertura midiática do caso foi bastante ampla: O então presidenciável Donald Trump convocou uma campanha de boicote à Apple (NASHRULLA, 2016), enquanto sua adversária Hillary Clinton caracterizou a situação como "um difícil dilema" (MCLAUGHLIN, 2016). Bill Gates se posicionou a favor do FBI (SOPRANA, 2016) ao passo que o ex-chefe da CIA e ex-diretor da NSA, Michael Hayden, se colocou a favor da Apple (WEBER, 2016). O então presidente dos Estados Unidos Barack Obama se pronunciou apontando um suposto perigo de uma visão "absolutista" em defesa da encriptação (SCOLA, 2016).

Uma enquete nacional realizada entre 11 e 15 de março pela *CBS News* e *The New York Times* (2016) com 1,022 adultos revelou que 50% pensavam que a Apple deveria

desbloquear o iPhone, enquanto cerca de 45% pensavam que a empresa não deveria cumprir com a ordem judicial. Diversas entidades[31] se envolveram no caso como *Amicus curiae* a favor da Apple (APPLE INC., 2016), enquanto outras[32] o fizeram a favor do FBI. O caso foi rapidamente associado por jornalistas (FROOMKIN & MCLAUGHLING, 2016) e acadêmicos (RIDER, 2016; SCHULZE, 2017) às guerras criptográficas dos anos 1990. Nesse sentido, as posições expressas pelos atores não diriam respeito somente a esse caso, mas estariam remetendo a toda a controvérsia mais ampla sobre o papel político da encriptação, os limites da vigilância governamental e as relações entre privacidade e segurança na era digital.

No dia 21 de março, um dia antes da audiência, o FBI entrou com um pedido de adiamento alegando que uma terceira parte havia entrado em contato com a agência demonstrando uma forma possível de desbloquear o iPhone. O adiamento foi autorizado e uma semana depois o FBI anunciou publicamente ter desbloqueado o aparelho com o auxílio dessa terceira parte (DATE et al., 2016). O Departamento de Justiça abandonou o caso. Nos meses seguintes, Comey sugeriu publicamente que o FBI havia pagado mais de $ 1,3 milhões pela solução (LITCHBLAU e BENNER, 2016), o que ele considerou custoso e afirmou não ser uma solução "escalável" (AHMED, 2016).

3.4 A tecnologia que amamos, a segurança de que precisamos

No caso San Bernardino, o dispositivo apreendido pelo FBI era um iPhone 5C, modelo A1532, P/N: MGFG2LL/A, S/N: FFMNQ3MTG2DJ, IMEI: 358820052301412, chip A6, da rede Verizon, atualizado com a versão 9 do iOS. A propriedade do dispositivo era do SBCDPH, onde Farook trabalhava como inspetor de saúde, e o aparelho foi designado e utilizado por ele como parte de seu emprego. Segundo o FBI (EUA, 2016c, p. 6), o iPhone foi entregue a Farook com a função de apagamento automático após 10 tentativas falhas de inserção de senha ativada e o último back-up do dispositivo na nuvem também a mostrava ativada. Isso significa que ela provavelmente estava ativada na ocasião da apreensão do celular pela agência de investigação.

[31] Amazon, Box, Cisco, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, Whatsapp, Yahoo, Eletronic Frontier Foundation, Eletronic Privacy Information Center, entre outras.
[32] Gabinete do Procurador Distrital do Condado de San Bernardino, Associação Nacional de Delegados, Associação Nacional de Promotores de Justiça, Associação Nacional de Policiais, entre outras.

O pedido original encaminhado pela agência alegava que assistência da Apple era necessária para determinar com quem os atiradores haviam se comunicado para planejar o ataque, para onde o casal poderia ter viajado antes e depois do incidente e outras informações pertinentes acerca do incidente (ibid.: p. 2). A Apple possuiria os "meios técnicos exclusivos" (ibid.: p. 1) para prover a assistência necessária para o exame do conteúdo do dispositivo. A assistência em questão compreendia a produção, por parte da empresa, de um arquivo de software, iPhone Software – IPSW ou Software Image File – SIF, para ser instalado no dispositivo.

O arquivo deveria cumprir os seguintes requisitos, de acordo com o pedido do FBI (ibid: p 8): desativar a função opcional de apagamento automático dos dados pessoais após dez tentativas falhas de inserção de senha no dispositivo existente na versão 9 do sistema operacional do iPhone (iOS); permitir que o FBI testasse senhas eletronicamente e não apenas manualmente; remover a função de atraso do dispositivo que previne o usuário de tentar inserir sua senha por períodos de tempo cada vez maiores a cada tentativa incorreta.

A agência demandava ainda que o arquivo fosse desenvolvido com um identificador compatível apenas com aquele dispositivo específico e afirmava que a Apple poderia trabalhar no aparelho em um de seus prédios e reter o arquivo de software, de modo que o governo trabalhasse apenas com a inserção das senhas. Isto é: o FBI não demandava acesso ao software em questão (o qual seria retido pela empresa), apenas seu desenvolvimento e emprego no iPhone, o que possibilitaria acessar o conteúdo do aparelho mediante um ataque criptoanalítico de força bruta.

No pedido de compelimento entregue ao tribunal pelo DoJ, nega-se que tal software seja um backdoor para a encriptação da Apple, pois a reivindicação do governo seria da suspensão de funções "adicionais, não ligadas à encriptação" (EUA, 2016d: p. 19). Alega-se também que o FBI realizaria o ataque de força bruta por acesso remoto, de modo que o processo poderia ser realizado inteiramente em uma instalação da Apple. Segundo o documento, isso eliminaria a possibilidade de obtenção do software por criminosos ou atores mal-intencionados (ibid.: p 20), pois

> a Apple poderia manter custódia do software, destruí-lo após seu propósito sob a Ordem [judicial] ter sido cumprido, recusar-se a disseminá-lo fora da Apple e deixar claro para o mundo que ele não se aplica a outros dispositivos ou usuários sem ordens judiciais legais.(ibid.: p. 15)

Os argumentos apresentados pelo FBI não apresentam diferenças substanciais em relação aos empregados durante as guerras criptográficas dos anos 1990. Tratava-se de uma argumentação majoritariamente focada na narrativa de "obscurecimento": a agência reconhece a importância da encriptação, mas entende que seu uso por criminosos inviabilizava a persecução de crimes, portanto um meio-termo era necessário. Esse meio-termo seria entendido como a possibilidade de acesso excepcional por parte do Estado[33] . Schulze (2017, p. 57) nota, todavia, que os exemplos principais de criminosos deixaram de ser traficantes de drogas e passaram a ser terroristas e abusadores de crianças. Esse tipo de argumento era complementado por declarações de impacto emocional, como:

> O contencioso de San Bernardino não é sobre tentar estabelecer um precedente ou mandar algum tipo de mensagem. É sobre as vítimas e justiça. Catorze pessoas foram assassinadas e muitas outras tiveram suas vidas e corpos arruinados. Nós devemos a eles uma investigação profissional sobre a lei. É sobre isso. O povo americano não deveria esperar nada menos do FBI. [...] Nós não queremos quebrar a encriptação de ninguém ou liberar uma chave mestra solta na terra. [...] Nós não podemos olhar nos olhos dos sobreviventes ou para nós mesmos no espelho se não seguirmos essa pista. [...] Embora esse caso seja sobre os inocentes atacados em San Bernardino, ele de fato evidencia que nós temos novas tecnologias incríveis que criam uma tensão séria entre dois valores que todos valorizamos - privacidade e segurança. [...] eu também espero que todos os americanos participem no longo diálogo que precisamos ter sobre como simultaneamente abraçar a tecnologia que amamos e garantir a segurança de que precisamos (COMEY, 2016).

Os trechos acima – extraídos de uma carta aberta escrita por Comey durante o conflito – evidenciam um aspecto intrigante do discurso do FBI: a insistência simultânea na particularidade do caso (a agência ressalta não estar agindo de caso pensado em função das consequências jurisprudenciais ou midiáticas do caso) e na generalidade da "tensão séria" entre privacidade e vigilância que demanda uma solução mais ampla. Para além desses pontos, a agência acusa a Apple de utilizar a encriptação como ferramenta de marketing e insiste numa argumentação "majoritariamente legalista, focando no argumento de que não deveriam existir espaços "a prova de mandados'" (SCHULZE, 2017, p. 59).

[33] Diversos especialistas da área técnica consideram o meio-termo sugerido tecnicamente impossível devido ao fato de que ele envolve a introdução de um terceiro no sistema, o que por definição aumenta a insegurança. O entendimento de que o uso da expressão 'meio-termo' para designar o que tecnicamente seria encriptação fraca suscitou uma série de críticas de que tal solução seria uma "solução imaginária" (MCLAUGHLIN, 2015), "um mito" (BLUE, 2017), "encriptação amigável à vigilância" (PFEFFERKON, 2017) ou ainda uma "solução do pônei mágico" (MCLAUGHLIN, 2016).

3.5 Um conto de duas portas

A recusa da Apple em cumprir a ordem judicial esteve fundamentada numa argumentação heterogênea que articulava questões técnicas, políticas e culturais. A narrativa produzida pela empresa acionava os valores de privacidade, segurança, democracia, identidade nacional e liberdades civis. O primeiro parágrafo da introdução ao pedido de revogação da ordem judicial oferece um panorama dos pontos levantados:

> Esse caso não é sobre um iPhone isolado. Ao invés disso, esse caso é sobre o Departamento de Justiça e o FBI buscando através de tribunais um poder perigoso que o povo americano não concedeu: a habilidade de forçar companhias como a Apple a fragilizar a segurança básica e os interesses de privacidade de centenas de milhões de indivíduos pelo globo. O governo demanda que a Apple crie um backdoor para anular a encriptação no iPhone, tornando as informações mais confidenciais e pessoais vulneráveis a hackers, ladrões de identidade, agentes estrangeiros hostis e vigilância governamental injustificada (EUA, 2016d: p. 1)

Para fins analíticos, dividirei a argumentação utilizada pela Apple em dois eixos, dois problemas levantados pela empresa como implicações caso as demandas do FBI fossem cumpridas: i) o problema da chave-mestra; ii) o problema do precedente perigoso. O primeiro argumento, de caráter mais técnico, consistiu na asserção de que o FBI estava demandando era o desenvolvimento de uma nova versão do iOS sem as proteções de segurança existentes nas versões anteriores, portanto um software que só poderia ser classificado um backdoor, algo que fragilizaria a segurança do iPhone de modo nunca antes realizado. Tal software é metaforizado por Tim Cook como uma chave-mestra que, uma vez existente, poderia ser utilizada por para obter acesso a qualquer iPhone. A ferramenta chega a ser descrita por ele como "o equivalente em software ao câncer" (COOK, 2016b).

Cook reitera diversas vezes que o software em questão, uma vez existente, poderia ser utilizado "milhões e milhões de vezes" (ibid.) para desbloquear "qualquer iPhone" (ibid.). O presidente da empresa defende que tal tecnologia jamais deveria ser produzida, pois sua produção implicaria no perigo de sua obtenção por parte de atores maliciosos, como criminosos e hackers. Os valores subjacentes são a privacidade e a segurança dos usuários do iPhone. Nessa narrativa, a privacidade é tratada como condição para a segurança, uma vez que o iPhone contém dados tão sensíveis quanto "seus dados de saúde, dados bancários, suas localizações, as localizações de seus filhos, etc" (ibid.)

A Apple (EUA, 2016e, p. 53 - 57) contrapõe a argumentação do governo de que o software poderia ser facilmente destruído após sua utilização no iPhone de Farook com os seguintes pontos: o processo de fabricação de tal software demandaria entre 2 e 4 semanas e entre 6 e 10 engenheiros da empresa. Ele precisaria ser registrado, armazenado e testado em todas as suas etapas caso a metodologia da empresa fosse questionada no tribunal. Mesmo que fosse possível erradicar completamente o código dos servidores da Apple de forma a torná-lo irrecuperável (possibilidade que a empresa questiona), sua metodologia de implementação existiria nos registros da empresa e nas memórias dos engenheiros envolvidos no processo, portanto poderia ser recriada.

O segundo argumento, de caráter mais explicitamente político, diz respeito ao precedente estabelecido caso o tribunal decidisse compelir a Apple a cumprir as demandas do FBI. Dada a existência de numerosos casos envolvendo celulares protegidos por encriptação[34] , o precedente estabelecido permitiria às forças policiais demandar a produção desse software diversas vezes.

> O governo diz: "só dessa vez" e "só esse telefone". Mas o governo sabe que essas declarações não são verdade. [...] Se essa ordem for sustentada, será questão de dias até algum outro promotor, em algum outro caso importante, diante de algum juiz, busque uma ordem similar usando este caso como precedente. (EUA, 2016d: p. 3)

Como evidencia, a empresa apresenta cita o promotor distrital de Manhattan, Cyrus Vance, afirmando ter entre "155 a 160" (ibid.) celulares que gostaria de acessar. Além disso, a Apple observa que seria difícil impor um limite sobre o precedente estabelecido:

> Se a Apple pode ser forçada a escrever software nesse caso para contornar recursos de segurança e criar nova acessibilidade, o que impede o governo de demandar que a Apple escreva código para ligar o microfone em auxílio à vigilância governamental, ativar a câmera de vídeo, furtivamente gravar conversas, ou ligar serviços de localização para rastrear o usuário do celular? Nada. (ibid., p. 4)

O FBI estaria tentando produzir jurisprudência que, na prática, resultaria no aumento de suas capacidades de vigilância. Segundo Cook, isso seria uma forma de contornar o debate democrático ao utilizar o poder judiciário para resolver uma questão que deveria ser debatida no âmbito do legislativo, uma "*backdoor* [jurídico-midiático] para o *backdoor* [técnico]" (COOK, 2016b). O argumento questionava a legitimidade das demandas do FBI ao apontar que as implicações políticas do estabelecimento desse precedente ultrapassam em muito o

[34] Comey (apud EUA, 2016f, p. 47): "As forças policiais crescentemente encontram celulares que não podem ser desbloqueados em investigações por todos os lados".

caso em questão. Os valores aqui acionados são democracia, as liberdades civis e a identidade nacional, valores dos quais a empresa se posiciona como protetora:

> Se opor ao seu governo em algo não é agradável, e se opor a ele em algo em nós estamos advogando pelas liberdades civis, – que eles deveriam proteger – é incrivelmente irônico, mas é onde nós nos encontramos. Então, por todas as pessoas que querem ter uma voz e tem medo, nós estamos nos levantando. (COOK, 2016b)

3.6 A mão ubíqua

Alguns dos argumentos reiterados no caso Apple vs FBI ecoam os discursos mobilizados nas guerras criptográficas dos anos 1990, sobretudo os de ceticismo governamental e o argumento técnico sobre como um mecanismo de acesso excepcional poderia ser apropriada por atores maliciosos. Uma diferença notória é o desaparecimento do discurso de liberalização mercadológica do escopo dos enunciados: Schulze (2017, p. 58) identifica 21 ocorrências do emprego de argumentos relativos aos impactos econômicos negativos durante o caso *Clipper* contra somente 1 ocorrência no caso Apple v. FBI.

Rider interpreta esse diferença como um indicativo de que o discurso de liberalização mercadológica tornou-se ubíquo na década de 2010. A ideia de que a responsabilidade pela tomada de decisões relativa à implementação é do mercado passou a ser inteiramente aceita como legítima nos debates públicos nos Estados Unidos. Por isso, diz Rider (2016, p. 26 - 27, trad. minha, ênfase da autora):

> Se nos anos 1990 as instituições policiais citavam o *problema da decifragem* como a justificativa primária para regular a encriptação, a importância da questão desapareceu durante a reencarnação mais recente das guerras criptográficas. Em vez disso, as instituições policiais enfatizam agora a falta de cooperação das empresas com ordens judiciais - o que eu chamo de *problema do mandado*. [...] As instituições policiais agora afirmam que os principais problemas que eles enfrentam estão ligados à aquiescência das empresas às relações construídas na esteira das primeiras guerras criptográficas.

Esse ponto é reiterado por dados quantitativos relativos às participações em audiências públicas entre 2011 e 2016, quais sejam: de um total de 19, 16 são do setor estatal (sendo 13 das instituições policiais, 1 das agências de inteligência e 2 de outras instâncias do governo), 3 da academia, 0 do setor empresarial, 0 da sociedade civil e 0 diversos. Para Rider, isso sugere que a discussão não é mais sobre qual setor deve ser responsável por

regular a encriptação, e sim sobre como o setor governamental deve responder à falta de cooperação do setor empresarial.

Essa interpretação facilita a compreensão da posição adotada pelo FBI no caso em questão. Num contexto em que a ausência de cooperação atrapalha a intervenção sobre o desenvolvimento e implementação da encriptação, ao menos do ponto de vista público, torna-se necessário empregar mecanismos para minimizar ou anular o efeito de tais tecnologias sobre a ação policial. O método adotado para tal foi legal: tratava-se de obter, através do poder judiciário, um precedente que possibilitaria demandar o desenvolvimento de software capaz de anular os efeitos das tecnologias de encriptação que as agências públicas consideram como obstáculos a seu trabalho.

Nesse sentido, é compreensível que o FBI não exigisse acesso ao software criado e restringisse sua aplicabilidade técnica ao dispositivo de Farook. O que se buscava era tanto a capacidade técnica atual de decriptar conteúdo cifrado naquele caso específico quanto a capacidade política virtual de fazê-lo em geral: o poder de compelir empresas de tecnologia a escrever software que tornaria tal processo realizável. Ainda nesse sentido, é interessante observar que afinal o FBI foi capaz de acessar o conteúdo do dispositivo de qualquer forma, o que sugere a possibilidade de a agência tivesse ciência da existência de alternativas técnicas para fazê-lo desde o início[35]. Isso reiteraria o ponto de que a capacidade objetiva de decifragem não era o único elemento em jogo.

A recusa da Apple em cumprir a ordem judicial e sua justificativa pautada em valores como identidade nacional, liberdades civis e democracia assim produz alguns efeitos favoráveis à empresa. Tal posição reafirma a eficácia técnica dos produtos da empresa, uma vez que sua encriptação é tão segura que nem o FBI e a NSA são capazes de ultrapassá-la. Em segundo lugar, a justificativa da empresa a situa explicitamente como protetora dos direitos de seus usuários, o que contribui para ocultar a participação prévia da empresa nas práticas de vigilância estatal no PRISM. Finalmente, o precedente de uma vitória forneceria uma proteção contra todos os impactos econômicos negativos que a obrigação de produzir softwares específicos para cumprir ordens judiciais significaria.

[35] Essa hipótese foi defendida abertamente por Snowden (A CONVERSATION... 2016, trad. minha): "O FBI diz que a Apple possui os 'meios técnicos exclusivos' para desbloquear o celular. Com todo o respeito, isso é balela".

CONCLUSÃO – MOCINHOS E VILÕES

Foucault (1978, p. 267) afirmou em certa ocasião que o objeto de suas reflexões era o problema da tecnologia do poder, o "como" do poder. Ele estava a dizer que sua discussão era menos sobre quem exerce o poder e mais sobre "como o poder domina e se faz obedecer". Um mundo no qual esse como tornou-se amplamente identificado com a manipulação da informação é um mundo em que se atribui relevância considerável à encriptação. No nível mais conceitual, trata-se de um procedimento abstrato geral que pode assumir distintas formas em padrões, protocolos e algoritmos igualmente abstratos. Na existência mundana, para usar uma expressão de Haraway, pode ser arma de guerra, proteção pessoal, instrumento de marketing, recurso criminoso, necessidade institucional e ferramenta de resistência.

Isso posto, não surpreende que atores tão distintos quanto instituições policiais, agências de inteligência, grupos de experts, organizações de ativistas e empresas de tecnologia se envolvam na tentativa de definir as respostas para algumas questões cruciais em torno da encriptação: Quem deve desenvolver os sistemas? Quais regras devem ser obedecidas? Quem deve guardar as chaves? O que conta como segurança? Quais os efeitos de cada uma das possibilidades de resposta? Sem a pretensão de extrapolar tais considerações para outros contextos, me parece ser possível esboçar algumas conclusões relativas às guerras criptográficas nos Estados Unidos à luz da descrição apresentada.

O período imediatamente posterior à Segunda Guerra Mundial foi um de controle estatal forte sobre a encriptação. Esse controle foi paulatinamente complexificando ao longo do último quarto do século XX. A informatização da vida social, a globalização neoliberal e os avanços associados na criptografia significaram um setor empresarial mais combativo em relação a regulações e mais capaz de influenciar a esfera pública. Conectado a esses processos esteve o movimento das agências de inteligência de buscar a expansão contínua de seus olhos rumo aos novos territórios digitais recém-produzidos.

Esses desdobramentos conformaram as condições de possibilidade para o anúncio do *Clipper* e o início das guerras criptográficas nos anos 1990. O *Clipper* colocava em conflito dois valores bastante caros ao neoliberalismo: vigilância, enquanto capacidade objetiva de monitorar multiplicidades e acessar suas informações e comunicações, e liberdade. Mas o que conta como liberdade nesse contexto? Trata-se de uma versão específica de liberdade concebida pela razão neoliberal enquanto um território em que habitam tanto a autonomia

política do sujeito frente ao Estado (aqui associada à capacidade de indivíduos se comunicarem sem interceptação estatal) quanto e a capacidade de ação irrefreada de empresas (aqui associada à capacidade para desenvolver e distribuir seus produtos sem intervenções regulatórias).

O *Clipper* postula um conflito entre esses dois valores historicamente aliados na arte de governar liberal menos por impor vigilância sobre as pessoas e mais porque isso é viabilizado através do que é percebido como uma intervenção regulatória, ainda que a adesão ao chip pelas empresas fosse voluntária. É por esse motivo que o período entre 1996 e 1999 é marcado por readequações táticas dos discursos por parte dos principais atores até que os valores percebidos como essenciais (vigilância e liberdade) pudessem convergir numa solução comum. Essa solução envolveu o ocultamento do debate de canais públicos, a terceirização da vigilância estatal e a privatização do controle sobre a encriptação.

Parte desses apontamentos foi realizada por Rider (2016), mas considero relevante pontuar as implicações desse uso da liberdade em que pessoas físicas e empresas são colocadas no mesmo plano. Um já comentado é a expansão da capacidade empresarial de conduta da conduta, de modo que liberdade de mercado significa liberdade de governo (privado). Olhar etnograficamente para as guerras criptográficas dos anos 1990 permite constatar outro efeito: uma vez assegurada a liberdade econômica da empresa, aquilo que era percebido como a liberdade política do indivíduo pôde ser silenciosamente suprimido, inclusive por meio do exercício dessa liberdade econômica. Isso se insere num contexto em que o neoliberalismo simultaneamente destitui o Estado de suas funções de provimento social e o povoa com demandas securitárias associadas a crime e terror. O crescimento da vigilância estatal e do controle privado sobre as multiplicidades são dois sintomas da mesma doença.

As revelações de Snowden publicizaram a cooperação público-privada para monitoramento dos usuários, o que expandiu imensamente a conversação cultural sobre vigilância, privacidade e afins. Dessa conversação resultou demanda por tecnologias de encriptação, o que significou um novo recurso publicitário para exploração pelas empresas de tecnologia. A exploração do recurso em questão foi viabilizada a partir da implementação de tecnologias cujo fundamento é a exclusão da possibilidade de decifragem dos dados pelas próprias empresas. Essa escolha técnica pode ser metaforizada como uma traição às alianças forjadas ao fim das primeiras guerras criptográficas e ela se torna um dos principais fatores

que ensejam as novas guerras criptográficas. No caso Apple v. FBI, isso se efetuou pela extensão da tecnologia Proteção de Dados à maior parte dos arquivos dos iPhones em 2014.

A decisão em questão foi uma das condições de possibilidade para o caso Apple v. FBI, no qual a agência estatal articulou os velhos discursos de oposição entre segurança e privacidade à narrativa do "obscurecimento" e buscou assegurar o acesso através de um mecanismo jurídico que lhe viabilizaria uma capacidade de ação incomensuravelmente maior: a de compelir empresas de software a escrever código. Uma vez que isso significaria um espaço de intervenção estatal sobre o setor empresarial, a tensão fundamental que suscitou as guerras criptográficas reemergiu: uma tensão que não opõe exatamente privacidade e segurança, e sim uma disputa entre Estado e mercado em torno de controle sobre a implementação das tecnologias de encriptação.

Ademais, há uma especificidade relevante nessa tecnologia para o debate sobre controle que reside justamente fato dela tender a ser percebida por defensores de direitos humanos e ativistas da privacidade como uma das principais ferramentas por meio das quais se pode exercer resistência em relação ao controle na era digital. O apoio de desses sujeitos (eu incluso no caso Apple v. FBI) às empresas de tecnologia em ambos os momentos das guerras criptográficas, ainda que majoritariamente ou inteiramente tático, indica um contexto no qual o mercado é legitimado enquanto provedor dos meios de resistência ao controle que ele mesmo ajuda a viabilizar.

Optei durante este trabalho em enfatizar as disputas econômicas e políticas em torno da encriptação, mas os dados que utilizei aqui poderiam ser mobilizados para a construção de uma etnografia em que as guerras criptográficas fossem apresentadas como disputas entre sistemas mais ou menos seguros de um ponto de vista técnico. Essa escolha seria válida e dela poderia resultar um trabalho dotado de eficácia política e epistemológica igual ou maior que a deste trabalho. Não obstante a escolha de não situar a eficiência no centro de minha ficção, tentei manter em evidência os impactos objetivos e materiais de cada decisão técnica sobre os desdobramentos políticos subsequentes.

Similarmente, insisti em colocar os enunciados dos atores em relação a atos não-enunciativos, o que gerou imagens potencialmente contrastivas em diversos momentos. Me parece, no entanto, que há muito mais robustez em suas ficções que palavras jogadas ao vento, sobretudo em suas acusações mútuas, como quando o FBI acusa a Apple de utilizar a privacidade como marketing ou a empresa o acusa de buscar um precedente. Ainda assim, me

parece igualmente que de um ponto de vista analítico é saudável manter uma atitude duvidosa em relação a suas declarações. Como comenta Haraway (1991, p. 232, trad. minha) em sua análise das ficções materiais e semióticas das biologias do século XX: "Não houve distinção clara entre ciência objetiva e ideologia abusiva porque as relações de saber e determinantes históricos demandam conceitos mais complexos. [...] Está no nível de teoria e prática fundamentais, não no nível de mocinhos e vilões."

REFERÊNCIAS

A CONVERSATION on Surveillance, Democracy and Civil Society. Realização de Common Cause. Coordenação de Dan Froomkin. Oakland, California, 2016. (33 min.), son., color. Comunicações orais de Edward Snowden e Malkya Cyril. Disponível em: <https://www.youtube.com/watch?v=cJ6PpX6xg-E->. Acesso em: 05 mai. 2018.

AHMED, M. FBI paid more than $1.4m for iPhone hack. **Financial Times**, Londres, 21 abr. 2016. Disponível em: <https://www.ft.com/content/af23e3ea-07f1-11e6-b6d3-746f8e9cdd33> Acesso em 27 out. 2018.

ALAIMO, S.; HEKMAN, S. «Introduction: Emerging Models of Materiality in Feminist Theory». In **Material Feminisms**, editado por Stacy Alaimo e Susan Hekman, 1-22. Bloomington: Indiana University Press, 2008.

ALVES, M. A. S. Cristianismo e racionalidade política moderna em Michel Foucault. **Revista Estudos Filosóficos**, v. 17, p. 76-88, 2016.

APPLE INC... Amicus briefs in support of Apple. **Comunicado de imprensa**, 2 mar. 2016. Disponível em: <https://www.apple.com/newsroom/2016/03/03Amicus-Briefs-in-Support-of-Apple/>. Acesso em 12 dez. 2017.

_____. iOS Security. February 2014. **White Paper**, fev. 2014a. Disponível em: <https://www.documentcloud.org/documents/1302616-ios-security-feb14.pdf>. Acesso em: 15 mai. 2018.

_____. iOS Security. September 2014. **White Paper**, set. 2014b. Disponível em: <https://assets.documentcloud.org/documents/1302613/ios-security-guide-sept-2014.pdf>. Acesso em: 09 dez. 2017.

_____. iOS Security. May 2012. **White Paper**, mai. 2012. Disponível em: <https://css.csail.mit.edu/6.858/2014/readings/ios-security-may12.pdf>. Acesso em: 09 dez. 2017.

AGAMBEN, G. De l'Etat de droit à l'Etat de sécurité. **Le Monde**, Paris, 21 dez. 2015. Disponível em: <https://www.lemonde.fr/idees/article/2015/12/23/de-l-etat-de-droit-a-l-etat-de-securite_4836816_3232.html>. Acesso em: 17 nov. 2018.

APPLEBOME, P. The 1992 Campaign Death Penalty; Arkansas Execution Raises Questions on Governor's Politics. **The New York Times**, Nova Iorque, 25 jan. 1992. Disponível em: <https://www.nytimes.com/1992/01/25/us/1992-campaign-death-penalty-arkansas-execution-raises-questions-governor-s.html>. Acesso em: 18 out. 2018.

<https://digitalforensics.sans.org/blog/2016/02/23/iphone-forensics-separating-the-facts-from-fictiona- technical-autopsy-of-the-apple-fbi-debate/>. Acesso em: 12 dez. 2017.

BALL, J.; BORGER, J.; GREENWALD, G. 2013. Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security. **The Guardian**, Londres, 6 set. 2013. Disponível em: <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>. Acesso em 17 out. 2018.

BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY (BERKMAN). **Não Entre em Pânico**: Avançando no debate sobre "obscurecimento" (Going Dark). Tradução de Rio de Janeiro, 2018. Tradução brasileira pelo Instituto de Tecnologia e Sociedade do Rio. Disponível em:<https://itsrio.org/wp-content/uploads/2018/10/Dont_Panic_Making_Progress_on_Going_Dark_Debate_PT.pdf> Acesso em 5 nov. 2018.

BLACK, T. E. Taking Account of the World As it Will Be: The Shifting Course of U.S. Encryption Policy. **Federal Communications Law Journal**, v. 52, n. 2, p. 290-314, 2001.

BLANC, F; POZNANSKI, F. ELLALink no caminho de um novo modelo de governança da Internet. **Convergência Digital**, [S. l.], 12 dez. 2017. Disponível em: <www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=46941&sid=15>. Acesso em 28 out. 2018.

BRADY, M. Ethnographies of Neoliberal Governmentalities: from the neoliberal apparatus to neoliberalism and governmental assemblages. **Foucault Studies**, n. 18, pp. 11- 33, out. 2014.

BLAZE, M. Protocol Failure in the Escrowed Encryption Standard. **AT&T Bell Laboratories**, [S. l.], 20 ago. 1994. Disponível em: <www.cryptomuseum.com/crypto/usa/files/eesproto.pdf> . Acesso em 10 out. 2018.

BLUE, V. Great, now there's 'responsible encryption'. **Engadget**, [S. l.], 27 out. 2017. Disponível em: <https://www.engadget.com/2017/10/27/great-now-theresresponsible-encryption/>. Acesso em: 16 dez. 2017.

CAMATI, O. Uma análise da razão de Estado em Michel Foucault a partir do curso Segurança, território e população. **Intuitio** (Porto Alegre), v. 8, p. 171-184, 2015.

CANDIOTTO, C. Técnicas de poder, segurança e liberdade. **Revista Ecopolítica**, São Paulo, n. 8, jan-abr, pp. 2-18, 2014.

CASTELFRANCHI, Y. **As serpentes e o bastão**. Tese de doutorado em Sociologia. Campinas: Unicamp, 2008.

CASTRO-GÓMEZ, S. Ciências sociais, violência epistêmica e problema da "invenção do outro. *In*: E. Lander, **A colonialidade do saber***:* eurocentrismo e ciências sociais - perspectivas latino-americanas, Buenos Aires, Clacso, 2005.

CESARINO, L. Estudos pós-coloniais da ciência e tecnologia: desafios e possibilidades . En: **V Reunião de Antropologia da Ciência e Tecnologia**, 2015, Porto Alegre. Anais da V ReACT, 2015.

CHEVIGNY, P. Repression in the United States after the September 11 attack. **Sur**, Rev. int. direitos human. [online]. 2004, vol.1, n.1 [cited 2018-11-27], pp.150-167.

COLUMBIA BROADCASTING SYSTEM NEWS (CBS NEWS); THE NEW YORK TIMES. Poll: Apple, Privacy and the Fight against Terrorism. 18 mar. 2016. Disponível em: <https://pt.scribd.com/doc/305268467/CBS-News-New-York-Times-Poll-Apple-Privacy-and-the-Fight-against-Terrorism>. Acesso em: 11 dez. 2017.

COLEMAN, E. G. **Coding Freedom**: The Ethics and Aesthetics of Hacking. Princeton: Princeton University Press, 2013. 264 p.

_____. The Anthropology of Hackers. **The Atlantic**, Boston, 21 set. 2010. Disponível em: <https://www.theatlantic.com/technology/archive/2010/09/the-anthropology-of-hackers/63308/>. Acesso em 24 out. 2018.

COMEY, James. Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? **FBI News**, Washington, 16 out. 2014. Speeches. Disponível em: <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-publicsafety-on-a-collision-course>. Acesso em: 08 dez. 2017.

_____. FBI Director Comments on San Bernardino Matter. FBI News, 21 fev. 2016. Disponível em: <https://www.fbi.gov/news/pressrel/press-releases/fbi-director-comments-on-san-bernardino-matter>. Acesso em 28 out. 2018.

COOK, Tim. A message to our customers. **Apple Inc**, 16 fev. 2016a. Disponível em:

<https://www.apple.com/customer-letter/>. Acesso em: 20 set. 2017.

_____. Exclusive: Apple CEO Tim Cook Sits Down With David Muir (Extended Interview). **ABC News**, 24 fev. 2016b. Entrevista concedida a David Muir. Disponível em: <https://www.youtube.com/watch?v=tGqLTFv7v7c>. Acesso em: 15 set. 2017.

_____. Here's the full transcript of TIME's interview with Apple CEO Tim Cook. **Time**, 17 mar. 2016c. Entrevista concedida a Nancy Gibbs e Lev Grossman. Disponível em:<http://time.com/4261796/tim-cook-transcript/>. Acesso em: 15 set. 2017.

CLIFFORD, James. Sobre a autoridade etnográfica. In: CLIFFORD, James. **A experiência etnográfica**: antropologia e literatura no século XX. Rio de Janeiro : Ed. UFRJ, 1998.

CNET. Winning the crypto war. **CNET**, [S. l.] 8 jan. 1998. Disponível em: <https://www.cnet.com/news/winning-the-crypto-war/> Acesso em 24 out. 2018.

DAM, K. W.; LIN, H. S. **Cryptography's role in securing the information society**. Washington, DC: National Research Council, 1996.

DATE, J; LEVINE, M; NEWCOMB, A. Justice Department withdraws request in Apple iPhone encryption case after FBI accesses San Bernardino shooter's phone. **ABC NEWS**, 28 mar. 2016. Technology. Disponível em: <http://abcnews.go.com/Technology/justice-department-withdraws-request-appleiphone-encryption-case/story?id=37986428>. Acesso em: 11 dez. 2017.

DELEUZE, G. Post-scriptum sobre as sociedades de controle. In: _____. **Conversações**, 1972-1990. Rio de Janeiro: Editora 34, 1992. p.219-226.

DIFFIE, W.; LANDAU, S. **Privacy on the Line**: The Politics of Wiretapping and Encryption. MIT Press, 2007. 215 p.

DUPONT, D.; PEARCE, F. Foucault contra Foucault: Rereading the 'Governamentality' papers. **Theoretical Criminology**, v. 5, n. 2, p. 123 - 158, 2001.

ESTADOS UNIDOS DA AMÉRICA (EUA). National Security Agency. **Basic Cryptologic Glossary**. Washington, 1955.

_____. Casa Branca. Escritório da secretaria de imprensa. Statement by the press secretary. **Casa Branca**, 16 abr. 1993a. Disponível em: <https://www.epic.org/crypto/clipper/white_house_statement_4_93.html>. Acesso em 10 out. 2018.

_____. Departamento de Justiça. Agência Federal de Investigação. Encryption: The Threat, Applications, and Potential Solutions, 1993b. Disponível em: <https://www.epic.org/crypto/clipper/foia/crypto_threat_2_19_93.html>.

_____. House of Representatives. **Encryption**: Individual Right to Privacy VS. National Security. Hearing Before the Subcommittee on International Economic Policy and Trade of the Committee on International Relations. 1997a. Disponível em: <https://fas.org/irp/congress/1997_hr/hfa44838_0.htm> Acesso em 20 out. 2018.

_____. House of Representatives. **Security and Freedom Through Encryption (SAFE) Act.** Hearing Before the Subcommittee on Courts and Intellectual Property and the Committee on the Judiciary, 1997b. Disponível em: <https://fas.org/irp/congress/1997_hr/hju41233_0.HTM>

_____. Senate. **CURRENT and Projected National Security Threats to the United States**: Hearing before the Select Committee on Intelligence of the United States Senate, 114th Congress, 2nd Session, 09 fev. 2016a. Transcrição. Washington: US Government Publishing Office, Disponível em: <https://www.intelligence.senate.gov/sites/default/files/hearings/S.%20Hrg.%20114-623.pdf>. Acesso em: 15 mai. 2018.

_____. United States District Court for the Central District of California. Government's ex parte application for order compelling Apple Inc. to assist agents in search; Memorandum of points and authorities; Declaration of Christopher Pluhar; Exhibit. **In the matter of the search of an Apple iPhone seized during the execution of a search warrant on a black Lexus IS300, California License Plate 35KGD203FBI**. Número do processo: 5:16-CM-00010. 16 fev. 2016b. Disponível em: <https://epic.org/amicus/crypto/apple/In-re-Apple-FBI-AWAApplication.pdf>. Acesso em: 21 set. 2017.

_____. United States District Court for the Central District of California. **Order compelling Apple Inc. to assist agents in search. In the matter of the search of an Apple iPhone seized during the execution of a search warrant on a black Lexus IS300, California License Plate 35KGD203FBI**. Número do processo: 5:16-CM-00010. 16 fev. 2016c. Disponível em: <https://epic.org/amicus/crypto/apple/In-re-Apple-AWA-Order.pdf>. Acesso em: 21 set. 2017.

_____. United States District Court for the Central District of California. **Government's motion to compel Apple Inc. to comply with this Court's February 16, 2016 order compelling assistance in Search; Exhibit. In the matter of the search of an Apple iPhone seized during the execution of a search warrant on a black Lexus IS300, California License Plate 35KGD203FBI**. Número do processo: 5:16-CM-00010. 19 fev. 2016d. Disponível em: <https://epic.org/amicus/crypto/apple/In-re-Apple-FBIMotion-to-Compel.pdf>. Acesso em: 21 set. 2017.

_____. United States District Court for the Central District of California Eastern Division. **Apple INC's motion to vacate order compelling Apple Inc. to assist agents in search and opposition to government's motion to compel assistance. In the matter of the search of an Apple iPhone seized during the execution of a search warrant on a black Lexus IS300, California License Plate 35KGD203FBI**. Número do processo: 5:16-CM-00010. 25 fev. 2016e. Disponível em: <https://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf>. Acesso em: 21 set. 2017.

_____.THE ENCRYPTION Tightrope: Balancing Americans' Security and Privacy. Hearing Before the Committee on the Judiciary House of Representatives 114th Congress, 2nd Session, 01 mar. 2016f. Transcrição. Washington: US Government Publishing Office, Disponível em: < https://judiciary.house.gov/wp-content/uploads/2016/02/114-78_98899.pdf>. Acesso em: 15 mai. 2018

FERREIRINHA, I. M. N.; RAITZ, T. R. As relações de poder em Michel Foucault: reflexões teóricas. **Rev. Adm. Pública**. 2010, vol.44, n.2, pp.367-383.

FONSECA, M. A.. **Michel Foucault e Constituição do Sujeito**. São Paulo: EDUC, 1995.

FOUCAULT, Michel. **Microfísica do poder**. Organização e tradução de Roberto Machado. Rio de Janeiro: Edições Graal, 1979.

_____. Omnes et singulatim: por uma crítica da razão política. **Revista Novos Estudos Cebrap**, v. 1, n. 26, mar. 1990a.

_____. Entrevista ao 'Le Monde' (fev. 1975). In: ERIBON, Didier. **Michel Foucault - uma biografia**. São Paulo: Companhia das Letras, 1990b.

_____. **Em defesa da sociedade**: curso no College de France (1975-1976). São Paulo: Martins Fontes, 1999a.

_____. **História da sexualidade I**: a vontade de saber. 13.ed. Rio de Janeiro: Graal, 1999b.

_____. **Vigiar e Punir**: nascimento da prisão. Tradução de Raquel Ramalhete. 34. ed. Petrópolis, RJ: Vozes, 2007.

_____. **Segurança, Território, População**. São Paulo: Martins Fontes, 2008a.

_____. **Nascimento da biopolítica**: curso dado no College de France (1978-1979). Tradução de Eduardo Brandão. São Paulo: Martins Fontes, 2008b.

_____. A sociedade disciplinar em crise. In: **Ditos e escritos IV**: estratégia, poder-saber. Org. Manoel Barros da Mota. Trad. Vera Lúcia A. Ribeiro. Rio de Janeiro: Forense Universitária, 2003.

FOUNDATION FOR INFORMATION AND POLICY RESEARCH (FIPR). The Crypto Wars Are Over! **Comunicado de imprensa**. Foundation for ºInformation and Policy Research, 25 mai. 2005. Disponível em: <https://www.fipr.org/press/050525crypto.html> Acesso em 14 set. 2018.

FROOMKIN, M. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. **University of Pennsylvania Law Review**, v. 143, n. 3, p. 709–897, 1995.

FROOMKIN, D; MCLAUGHLIN, J. FBI vs. Apple establishes a new phase of the crypto wars. **The Intercept**, 26 fev. 2016. Disponível em: <https://theintercept.com/2016/02/26/fbi-vs-apple-post-crypto-wars/>. Acesso em: 10 dez. 2017.

GABRIELE, M. C.; OLIVEIRA M. A.; ARRAIS, R.H. **Uma introdução ao estudo do Dispositivo de Sexualidade, a partir da leitura da obra "História da Sexualidade – A vontade de saber" de Michel Foucault**. Disponível em: <http://www.petpsi.ufc.br/JornalMural/Conceito_dispositivo.doc>. Acesso em 10 out. 2018.

GILLMOR, D. K. One of the FBI's major claims in the iPhone case is fraudulent. **ACLU**, [S. l.], 7 mar. 2016. Disponível em: <https://www.aclu.org/blog/privacytechnology/internet-privacy/one-fbis-major-claims-iphone-case-fraudulent>. Acesso em: 16 dez. 2017.

GOLDMAN, M. & LIMA, T. "Como se faz um grande divisor?", in GOLDMAN, M.(org.), **Alguma Antropologia**, Rio de Janeiro, Relume-Dumará, 1999.

GREENWALD, G. NSA Prism program taps into user data of Apple, Google and others. **The Guardian**, 07 jun. 2013. US National Security. Disponível em:

<https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>. Acesso em: 08 dez. 17.

HANSEN, M. P. Foucault's Flirt? Neoliberalism, the left and the welfare state; A commentary on la dernière leçon de Michel Foucault and Critiquer Foucault. **Foucault Studies**, v. 20, n. 20, p. 291- 306. 2015.

HAN, B. A Agonia de Eros. Tradução de Miguel Serras Pereira. Relógio D'Água Editores, 2014.

HARAWAY, D. The Biological Enterprise - Sex, Mind & Profit from Human Engineering to Sociobiology. In: HARAWAY, D. **Simians, Cyborgs & Women**. The reinvention of nature. New York: Routledge, 1991.

_____. Manifesto ciborgue: ciência, tecnologia e feminismo-socialista no final do século XX. In: SILVA, T. T. (Org.). **Antropologia do ciborgue**. Belo Horizonte: Autêntica, 2000. p. 37-129.

HOBOKEN, J. V.; SCHULZ, W. **Human rights and encryption**. Paris: UNESCO, 2016. Disponível em: <http://unesdoc.unesco.org/images/0024/002465/246527E.pdf>. Acesso em: 17 abr. 2017.

INMAN, B. R. The NSA perspective on telecommunications protection in the nongovernamental sector. **Cryptologia**, v. 3, n. 3, 129 - 135, 1979.

LAPPIN, T. Winning the Crypto Wars. **Wired**, [S. l.], 05 jan. 1997. Disponível em: <https://www.wired.com/1997/05/cyber-rights-10/>. Acesso em 27 out. 2018.

LATOUR, B. **Jamais fomos modernos**: ensaio de antropologia simétrica. Rio de Janeiro: Editora 34, 1994.

_____.**A esperança de Pandora**. Tradução de Gilson César Cardoso de Sousa. São Paulo: Edusc, 2001.

LEVY, S. Battle of the Clipper Chip. **The New York Times**, Nova Iorque, 12 jun. 1994. Disponível em: <https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html>. Acesso em 10 out. 2018.

_____. **Crypto**: How the Code Rebels Beat the Government Saving Privacy in the Digital Age. EUA: Penguin Books, 2001.

LICHTBLAU, E.; BENNER, K. F.B.I. Director Suggests Bill for iPhone Hacking Topped $1.3 Million. **The New York Times**, 21 abr. 2016. Disponível em:

<https://www.nytimes.com/2016/04/22/us/politics/fbi-director-suggests-bill-for-iphone-hacking-was-1-3-million.html>. Acesso em 28 out. 2018.

LIU, H. Inside the Black Box: Political Economy of the Trans-Pacific Partnership's Encryption Clause. **Journal of World Trade**, v. 51, n. 2, p. 309 - 334, 2017.

LYON, D. As apostas de Snowden: desafios para entendimento de vigilância hoje. **Cienc. Cult**., São Paulo , v. 68, n. 1, p. 25-34, Mar. 2016 .

MAHALIK, H.; MURPHY, C; EDWARDS, S. A Technical Autopsy of the Apple - FBI Debate using iPhone forensics. **SANS Digital Forensics and Incident Response Blog**, 23 fev. 2016. Disponível em: <https://digitalforensics.sans.org/blog/2016/02/23/iphone-forensics-separating-the-facts-from-fictiona-technical-autopsy-of-the-apple-fbi-debate/>. Acesso em: 12 dez. 2017.

MARCUS, G. Ethnography in/of the world system: the emergence of multi-sited ethnography. **Annual Review of Anthropology**, n. 24, p. 95-117, 1995.

MBEMBE, A. Necropolítica. **Artes & Ensaios**, nº 32, 123-151, 2017.

MEDINA, J.; PÉREZ-PEÑA, R.; SCHMIDT, M.; GOODSTEIN, L. San Bernardino suspects left trail of clues, but no clear motive. **The New York Times**, Nova Iorque, 03 dez. 2015. Disponível em: <https://www.nytimes.com/2015/12/04/us/sanbernardino- shooting.html>. Acesso em: 08 dez. 2017.

MCCARTHY, K. Look who's joiner the anti-encryption posse: Germany, come on down. **The Register**, 15 jun; 2017. Disponível em: https://www.theregister.co.uk/2017/06/15/germany_joins_antiencryption_posse/. Acesso em 15 set. 2018.

MCGARRY, C. Apple updates privacy policy: 'We sell great products,' not your data, says Tim Cook. **Macworld**, Security. 18 set. 2014. Disponível em: <https://www.macworld.com/article/2685600/apple-updates-privacy-policy-we-sellgreat-products-not-your-data-says-tim-cook.html>. Acesso em: 08 dez. 2017.

MCLAUGHLIN, J. Spy Chief complains that Edward Snowden sped up spread of encryption by 7 years. **The Intercept**, 25 abr. 2016. Disponível em:<https://theintercept.com/2016/04/25/spy-chief-complains-that-edward-snowden-sped-up-spread-of-encryption-by-7-years/> Acesso em 22 out. 2018.

_____. Hillary Clinton and Bernie Sanders refuse to choose between Apple and the FBI. **The Intercept**, 19 fev. 2016. Disponível em

<https://theintercept.com/2016/02/19/clinton-and-sanders-refuse-to-choose-betweenapple-and-the-fbi>. Acesso em: 10 dez. 2017.

_____. FBI director says scientists are wrong, pitches imaginary solution to encryption dilemma. **The Intercept**, 8 jul. 2015. Disponível em: <https://theintercept.com/2015/07/08/fbi-director-comey-proposes-imaginary-solutionencryption/>. Acesso em: 16 dez. 2017

MENN, J. Exclusive: Secret contract tied NSA and security industry pioneer. **Reuters** [S. l.], 20 dez. 2013. Disponível em: <https://www.reuters.com/article/us-usa-security-rsa/exclusive-secret-contract-tied-nsa-and-security-industry-pioneer-idUSBRE9BJ1C220131220> Acesso em 23 out. 2018.

MOL, A. **Ontological politics**: a word and some questions. In: Law J, Hassard J. Actor network theory and after. Oxford: Blackwell Publishing; 1999.

_____. **The body multiple**: ontology in medical practice. Londres: Duke University Press; 2002.

NADER, L. Up the Anthropologist - perspectives gained from studying up. In: HYMES, D. (Ed.). **Reinventing Anthropology**. New York: Random House, pp. 284–311, 1972.

NASHRULLA, T. Donald Trump calls for Apple boycott. **Buzzfeed News**, [S. l.], 19 fev. 2016. Disponível em: <https://www.buzzfeed.com/tasneemnashrulla/donald-trumpcalls-for-apple-boycott?utm_term=.smeWQ1zZee#.bsj8EKpqww>. Acesso em: 10 dez. 2017.

NAKASHIMA, E.; WARRICK, J. For NSA chief, terrorist threat drives passion to 'collect it all'. **The Washington Post**, Washington, 14 jul. 2013. Disponível em: <https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html>. Acesso em: 22 out. 2018.

PFLEEGER, C. P.; PFLEEGER, Shari L.; MARGULIES, Jonathan. **Security in Computing**. 5. ed. [S.l.]: Prentice Hall, 2015.

PFEFFERKORN, R. The rhetoric of "Responsible Encryption". **Just Security**, 19 out. 2017. Disponível em: <https://www.justsecurity.org/46102/rhetoric-responsibleencryption/>. Acesso em: 16 dez. 2017.

REZENDE, P. A. D. A lei de Kerckhoffs. **Segurança Computacional**, Brasília, abr. 2009. Disponível em: <https://cic.unb.br/~rezende/trabs/kerckhoffs.html> Acesso em 19 set. 2018.

PEIRANO, M. Etnografia não é método. **Horiz. antropol**., Porto Alegre , v. 20, n. 42, p. 377-391, Dec. 2014 .

PEREIRA, P. Os Estados Unidos e a ameaça do crime organizado transnacional nos anos 1990. **Rev. bras. polít. int.**, Brasília , v. 58, n. 1, p. 84-107, Jun. 2015.

PERLROTH, N.; LARSON, J. SHANE, S. N.S.A. Able to Foil Basic Safeguards of Privacy on Web. **The New York Times**, New York, 05 sept. 2013. Disponível em: <> Acesso em:

PRECIADO, P. B**.** Transfeminismo no regime fármaco-pornográfico. Tradução de Thiago Coacci. in L. Borghi, F. Manieri e A. Pirri**, Le cinque giornate lesbiche in teoria**. Roma, Ediesse, 2011.

_____. **Manifesto Contrassexual**. Políticas subversivas de identidade sexual. São Paulo: n-1 edições, 2014.

PRINS, B. and MEIJER, I. C. Como os corpos se tornam matéria: entrevista com Judith Butler. **Rev. Estud. Fem.** [online]. 2002, vol.10, n.1 [cited 2018-12-17], pp.155-167.

RAMIREZ PARTIDA, H. R. Post-9/11 U.S. Homeland Security Policy Changes and Challenges: A Policy Impact Assessment of the Mexican Front. **Norteamérica**, México , v. 9, n. 1, p. 55-78, jun. 2014.

RIDER, K. **The Privacy Paradox**: Privacy, Surveillance, and Encryption. Tese de mestrado em Artes pelo programa de Sociologia da University of Washington. 2016.

ROBERTS, R. Prime Minister claims laws of mathematics 'do not apply' in Australia. **The Independent**, 15 jul. 2017. Disponível em: <https://www.independent.co.uk/news/malcolm-turnbull-prime-minister-laws-of-mathematics-do-not-apply-australia-encryption-l-a7842946.html> Acesso em 15 set. 2018.

SANT'ANNA, D. B. de. Transformações do corpo: controle de si e uso dos prazeres. In: RAGO, M.; ORLANDI, L.B.L.; VEIGA-NETO, A. (Org.). **Imagens de Foucault e Deleuze**: ressonâncias nietzschianas. Rio de Janeiro: DP&A, 2002

RIFKIN, Jeremy. **A era do acesso**: a transição de mercados convencionais para networks e o nascimento de uma nova economia. Trad. Maria Lucia G. L. Rosa. São Paulo: Makron Books, 2001.

SANTOS, M. **Por uma outra globalização:** do pensamento único à consciência universal. Rio de Janeiro: 2001.

SANTOS, R. E. **Genealogia da Governamentalidade em Michel Foucault**. Dissertação de mestrado em Filosofia. Belo Horizonte: UFMG, 2010.

SCHULZE, M. Clipper meets Apple vs. FBI – a comparison of the cryptography discourses from 1993 and 2016. **Media and Communication**, v. 5, n. 1, p. 54-62, 22 mar. 2017.

SCOLA, N. Obama rejects 'absolutist' defense of encryption. **Politico**, [S. l.], 11 mar. 2016. Disponível em: <https://www.politico.com/story/2016/03/obama-appleencryption-battle-220656>. Acesso em: 10 dez. 2017.

SERRANO, R.; BENNET, B.; KARLAMANGLA, S.. FBI probes Islamic State, terror links to San Bernardino massacre. **Los Angeles Times**, Los Angeles, 05 dez. 2015. Disponível em: <http://beta.latimes.com/local/lanow/la-me-ln-san-bernardino-shootingisis-20151204-story.html>. Acesso em: 08 dez. 2017.

SILVA, M. R. **Refigurando monstros**: a perspectiva parcial de Donna Haraway como crítica da ciência. Dissertação de mestrado em Medicina Social. Rio de Janeiro: UERJ, 2009.

SOUZA, I. V. A. **Decifrando um Enigma entre ciência e política**: Relações entre humanos e não humanos em Alan Turing. Monografia de graduação em Ciências Sociais. Belo Horizonte: UFMG, 2016.

SINGH, S. **The Code Book**: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. First Anchor Books Edition: New York, 2000.

SOGHOIAN, C. Tweet nº 512414781312360448. **Twitter**, 17 set. 2014. Disponível em: <https://twitter.com/csoghoian/status/512414781312360448>. Acesso em: 13 dez. 2017.

SOLAGNA, F.; DE SOUZA, R.; LEAL, O. Quando o ciberespaço faz as suas leis: o processo do marco civil da internet no contexto de regulação e vigilância global. **Vivência: Revista de Antropologia**, v. 1, n. 45, 18 nov. 2015.

SOPRANA, P. Bill Gates defende que a Apple forneça dados ao FBI. **Época**, [S. l.], 11 mar. 2016. Experiências Digitais. Disponível em: <http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/02/gates-defende-queapple-forneca-dados-ao-fbi.html>. Acesso em: 10 dez. 2017.

SOUZA, L. G. R. **Quem Calculava?** Representações de gênero na relação mulher-matemática na obra O Homem que Calculava de Malba Tahan. 2013. 72f. Dissertação (Mestrado em Ensino de Ciências e Educação Matemática) – Universidade Estadual de Londrina, 2013.

STAR, S. L. The Ethnography of Infrastructure. **American Behavioral Scientist**, v. 43, n. 3, p. 377–391, 27 nov. 1999.

STRATHERN, Marilyn. **Fora de contexto**: as ficções persuasivas da antropologia. 2013. Terceiro Nome, São Paulo: 160p

THOMPSON, A. W.; KEHL, D.; BANKSTON, K. Doomed to Repeat History? Lessons from the Crypto Wars of the 1990s. **New America**, [S. l.], 17 jun. 2015. Disponível em: <https://www.newamerica.org/cybersecurity-initiative/policy-papers/doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/>. Acesso em 24 out. 2018.

UMAR, A. Is the national prohibition of strong encryption feasible, and would it prove effective in the fight against crime? **Cryptolosophy**, 28 abr. 2017. Disponível em: <https://cryptolosophy.org/assets/papers/epq.pdf> Acesso em 15 out. 2018.

VEIGA-NETO, A. **Foucault e a Educação**. Belo Horizonte: Autêntica, 2003. 191p.

VINUTO, Juliana. A amostragem em bola de neve na pesquisa qualitativa: um debate em aberto. **Revista Temáticas**, Campinas, 22, (44), p. 203-220, ago/dez. 2014.

WACQUANT, Loïc. Crime e castigo nos Estados Unidos: de Nixon a Clinton. **Rev. Sociol. Polit.**, Curitiba , n. 13, p. 39-50, Nov. 1999.

_____.WACQUANT, L. Três etapas para uma antropologia histórica do neoliberalismo realmente existente. **Cad. CRH**. 2012, v. 25, n. 66, pp. 505-518.

WEBER, P. Ex-NSA, CIA chief Michael Hayden sides with Apple in FBI iPhone encryption fight. **The Week**, 18 fev. 2016. Disponível em: <https://theweek.com/speedreads/606641/exnsa-cia-chief-michael-hayden-sidesapple-fbi-iphone-encryption-fight>. Acesso em: 10 dez. 2017.

WOOLLACOTT, E. UK Prime Minister Demands Internet Regulation Following London Terror Attack. **Forbes**, 05 jun. 2017. Disponível em: <https://www.forbes.com/sites/emmawoollacott/2017/06/05/why-theresa-may-is-really-calling-for-a-ban-on-encryption/#66deffdc229b> Acesso em 15 set. 2018.

ZUBOFF, S. **Big other**: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, v. 30, pp.75-89, 2015.