Artigos Selecionados REDE 2017
I Encontro da Rede de Pesquisa em Governança da Internet
Rio de Janeiro, 14 de Novembro de 2017

DE VOLTA ÀS CRIPTOGUERRAS: o caso Apple contra o FBI

Gustavo Ramos Rodrigues
gustavoramos_102@hotmail.com
Graduando em Antropologia pela Universidade Federal de Minas Gerais

RESUMO
O presente trabalho consiste numa etnografia multissituada sobre um conflito travado entre a empresa de tecnologia Apple e a Agência Federal de Investigação (FBI) dos Estados Unidos em torno do desbloqueio de um iPhone utilizado por um dos atiradores no atentado terrorista de San Bernardino, ocorrido no final de 2015. A disputa jurídica e política recebeu cobertura midiática ampla e tornou-se um símbolo dos conflitos contemporâneos envolvendo o emprego da criptografia no contexto das complexas relações entre privacidade e segurança na era da informação. A descrição etnográfica foi produzida a partir da análise de fontes heterogêneas, as quais incluem documentos jurídicos referentes ao caso em questão, depoimentos públicos de representantes das partes envolvidas e publicações técnicas acerca da criptografia empregada no iPhone Operating System (iOS). As narrativas de segurança adotadas pela Apple e pelo FBI em relação ao tema da segurança foram examinadas de modo mais aprofundado a luz de suas associações com decisões técnicas, interesses econômicos, valores culturais e processos políticos envolvendo a criptografia nas últimas três décadas. O objetivo foi compreender, a partir de uma perspectiva orientada principalmente pelo campo dos estudos de Ciência, Tecnologia e Sociedade (STS), as formas concretas pelas quais fatores diversos convergem para a construção das controvérsias atuais em torno das tentativas de regulação da criptografia - as chamadas guerras criptográficas ou criptoguerras.

PALAVRAS-CHAVE: cibersegurança, criptografia, vigilância, tecnopolítica

Sugestão de citação (ABNT): SOBRENOME, Nome. **Título do artigo**. I ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, NOVEMBRO DE 2017. Disponível em: <endereço na web>. Acesso em: mês. ano.

INTRODUÇÃO: O CASO

> A criptografia reorganiza o poder: ela configura quem pode fazer o que, a partir de que. Isso torna a criptografia uma ferramenta inerentemente *política*, e confere ao campo uma dimensão intrinsecamente *moral* (ROGAWAY, 2015, p. 1).[1]

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 na morte 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. O diretor da Agência Federal de Investigações (FBI) dos Estados Unidos, 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 esmagados numa lixeira, pois os atiradores haviam tentado destruir seus “rastros digitais” (SERRANO; BENNET; KARLAMANGLA, 2015).

Em 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 encriptado[2] (CURRENT... 2016, p. 43). Na ocasião, o diretor do FBI declarou 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 – o caso do celular em questão.

---

1 Tradução minha, assim como todas as outras neste artigo.

2 Encriptação é o processo de transformação de dados legíveis em dados ininteligíveis (dados encriptados ou cifrados) através do emprego de um algoritmo criptográfico. O processo geralmente visa assegurar a confidencialidade e a integridade dos dados, de forma que estes só poderão ser tornados legíveis (decriptados ou decifrados) por aqueles que detiverem uma informação particular conhecida como chave criptográfica.

O dispositivo, um iPhone 5C, estava protegido com uma senha definida pelo usuário sem a qual não era possível acessar seu conteúdo decriptado. 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 (USA, 2016a). No mesmo dia, a juíza Sheri Pym, do Tribunal Distrital da Califórnia, emitiu uma ordem judicial compelindo a Apple a prover "assistência técnica razoável" (USA, 2016b, p. 2) para os agentes da lei no acesso ao conteúdo do dispositivo.

Ainda no mesmo dia, a Apple respondeu com a publicação de uma mensagem assinada por seu presidente (COOK, 2016a) e destinada aos consumidores da empresa. 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 (USA, 2016c), ao qual a empresa respondeu em 25 de fevereiro com um pedido de revogação da ordem (USA, 2016d). 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 Agência de Segurança Nacional (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[3] se envolveram no caso como *amicus curiae* a favor da Apple (APPLE INC., 2016), enquanto outras[4] o fizeram a favor do FBI. O caso foi rapidamente associado por jornalistas (FROOMKIN; MCLAUGHLING, 2016) e acadêmicos (RIDER, 2017; SCHULZE, 2017) às guerras criptográficas[5] dos anos 1990. Nesse sentido, as posições expressas pelos atores não

3 Amazon, Box, Cisco, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest, Pinterest, Slack, Snapchat, Whatsapp, Yahoo, Eletronic Frontier Foundation, Eletronic Privacy Information Center, entre outras.

4 Associação Nacional de Delegados, Associação Nacional de Promotores de Justiça, Associação Nacional de Policiais, o Ministério Público do condado de San Bernardino, entre outras (NELSON; EMERSON, 2016).

5 *Crypto Wars,* ou guerras criptográficas, foi um nome informal dado ao conjunto de tentativas de governos (principalmente dos Estados Unidos e da Inglaterra) de limitar o

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; LEVINE; NEWCOMB, 2016). O Departamento de Justiça abandonou o caso, no que poderia ser considerado uma vitória da Apple. O presente trabalho investiga algumas das causas e consequências do desenrolar do caso.

OBJETIVO E MÉTODOS

A inspiração temática para o desenvolvimento desta pesquisa vem do clássico trabalho de Laura Nader acerca das perspectivas adquiridas ao se estudar "acima", isto é, lançar o olhar etnográfico para os atores bem posicionados nas relações de poder que permeiam o espaço social: os ricos, os poderosos, o centro. Ao observar sobre a tendência da antropologia para o estudo da periferia e das margens, a autora pondera:

> Antropólogos poderiam de fato se perguntar se a totalidade do trabalho de campo não depende de uma certa relação de poder a favor do antropólogo, e se tais relações de dominação-subordinação não estão afetando os tipos de teorias que estamos tecendo. E se, em reinventar a antropologia, antropólogos fossem estudar os colonizadores em vez dos colonizados, a cultura do poder em vez da cultura dos impotentes, a cultura da afluência em vez da cultura da pobreza? (NADER, 1972, p. 289).

Nesse sentido, o presente trabalho adota uma abordagem empírica para investigar o tipo de racionalidade que informa dois tipos de atores envolvidos no debate acerca do emprego de métodos criptográficos: as forças policiais e as grandes empresas de tecnologia da informação. Ao analisar as demandas do FBI e a oposição da Apple, busco compreender os tipos de racionalidade que os informam tanto em relação a sua coerência discursiva interna (argumentos utilizados para justificar sua ação, com base na alegação de quais valores, etc.) quanto em relação às possíveis conexões com outros fatores de ordem política, econômica e/ou social, os quais podem figurar de modo implícito ou mesmo ausente no discurso público oficial dos

acesso da população à encriptação.

atores. Em especial, me debruço sobre os diferentes sentidos e implicações que a noção de “segurança” assume para esses atores.

A pesquisa aqui realizada é de orientação qualitativa. Optei por adotar como método a chamada “etnografia multissituada” (MARCUS, 1995; CESARINO, 2014) desenvolvida pela antropologia pós-modernista das décadas de 1980 e 1990 como resposta às críticas ao método etnográfico tradicional. Ela consiste na prática de seguir etnograficamente os atores conforme eles circulam e interagem no contexto de uma rede heterogênea que envolve diferentes escalas (muitas vezes nacionais ou mesmo internacionais) e atores dispersos e distribuídos (*experts*, empresas, órgãos estatais, instituições, acadêmicos, grupos de ativistas, etc.). Abordagens de inspiração similar podem ser encontradas nos trabalhos de autores como Arjun Appadurai (1995) e Bruno Latour (2012).

Uma vez que esta pesquisa investiga uma rede de contextos tão dispersa espacialmente, cuja escala é tão grande e que atraiu tanto interesse da imprensa, faço uso extenso de fontes documentais jurídicas (documentos do processo) e técnicas (os *White papers* de segurança da Apple, as análises técnicas publicadas por especialistas sobre o caso) e uma ampla variedade de fontes jornalísticas, tanto para contextualizar o caso quanto para apreender, a um só tempo, as ações dos atores e seus discursos públicos. A expectativa é que a descrição etnográfica resultante possa oferecer uma imagem que compreenda as formas como o dito e o não-dito, o técnico e o legal, se articulam na interação entre os atores, especialmente a relação entre a Apple, o FBI, a imprensa e o público.

Para compreender a postura do FBI sobre o caso, utilizo os seguintes contextos: A) a palestra “*Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?”,* dada pelo diretor da agência em 2014; B) o testemunho de James Comey na audiência pública do congresso americano sobre ameaças à segurança nacional em 2016; C) o pedido original encaminhado pelo FBI ao tribunal distrital da Califórnia em 16 de fevereiro de 2016; D) o pedido de compelimento encaminhado pelo DoJ no dia 19 de fevereiro.

Para apreender os argumentos da Apple sobre o caso, analiso três contextos diretamente relacionados: A) o texto “*A Message to Our Customers”* publicado no site da Apple e assinado por Tim Cook em 16 de fevereiro de 2016 como resposta à ordem judicial assinada pela juíza Pym; B) o pedido de revogação da ordem judicial (USA, 2016a) entregue pela empresa ao tribunal em 25 de fevereiro; C) duas entrevistas dadas por Cook nas quais o caso foi discutido amplamente, uma para o veículo de notícias ABC News (COOK, 2016b) em 25 de fevereiro e outra para a revista Time (COOK, 2016c) em 17 de março.

CRIPTOGUERRAS 1.0: O CHIP *CLIPPER*

Debates em torno das implicações do uso de encriptação ocorreram amplamente nos Estados Unidos durante a década de 1990, e a socióloga Karina Rider (2017) analisa os discursos acionados tanto pelos defensores do acesso irrestrito do público à encriptação quanto por seus opositores. Em 1993, o governo Clinton tentou legislar pela obrigatoriedade da adoção do chip *Clipper* em celulares e computadores, um hardware de encriptação que empregava um algoritmo criptográfico secreto desenvolvido pela NSA denominado *Skipjack*, cuja chave criptográfica seria copiada e armazenada em bancos de dados do governo americano (SCHULZE, 2017, p. 55).

Na ocasião, diversas audiências públicas foram convocadas para debater os prós e contras da proposta. A justificação para a implementação do *Clipper* era segurança nacional. Em meio às políticas de combate radical ao crime dos anos 1990, os defensores do *Clipper* argumentavam que encriptação não-regulada pelo Estado favorecia o aumento na atividade criminosa, em particular crimes ligados a drogas (RIDER, 2017, p. 7), pois os criminosos se comunicariam por canais protegidos com encriptação que a polícia não poderia decriptar facilmente. Rider (2017) chama isso de “problema da decriptação”.

Os opositores do *Clipper*, por outro lado, justificavam sua posição com base em dois discursos:

O primeiro – “liberalização de mercado” (RIDER, 2017) – enfatizava os benefícios econômicos de encriptação não-regulada pelo Estado: regulação governamental nesse caso inibiria inovação no setor privado, de forma que o *Clipper* atrapalharia o progresso tecnológico. Além disso, medidas de privacidade e segurança eram necessárias para que as empresas estadunidenses pudessem competir no mercado global de informação, uma vez que sem tais medidas os usuários seriam desencorajados a participar na economia digital por medo de cibercriminosos e *hackers*. Finalmente, a encriptação era necessária para o comércio digital internacional, pois sem ela as empresas não poderiam enviar dados financeiros sensíveis para bancos internacionais.

O segundo discurso - “ceticismo governamental” (RIDER, 2017, p. 8) – enfatizava a possibilidade de abusos de poder por parte do Estado caso as comunicações dos usuários fossem facilmente acessíveis por ele. Rider (2017) relaciona isso à tendência da cultura política estadunidense para enxergar a autoridade centralizada com desconfiança e considerar as agências federais como propensas ao abuso de poder. Esse discurso sugeria que o mercado era mais

capacitado para lidar com os riscos inerentes ao manejo de dados sensíveis e uso de encriptação.

A eficácia desses discursos foi notória, e em meados dos anos 1990 o projeto *Clipper* foi descartado. Para a autora, a aceitação de que a encriptação deve ser regulada pelo mercado tornou-se tácita no século XXI, de forma que a questão central das guerras criptográficas muda. O problema "quem deve implementar a encriptação, o Estado ou as empresas de tecnologia?" dá lugar a "as empresas de tecnologia podem cooperar com a efetivação de mandados judiciais para a extração de dados encriptados? Em caso afirmativo, elas devem fazê-lo?". Ora pelo não-reconhecimento da legitimidade de tais mandados em abrir as comunicações, ora pelo emprego de meios técnicos que impedem as próprias empresas de acessar o conteúdo comunicado, o "problema do mandado" (RIDER, 2017, p. 13) caracteriza a década de 2010. Como veremos a seguir, o conflito entre a Apple e o FBI traz à tona todas essas questões.

CRIPTOGRAFIA DO IPHONE: ANTES DE SNOWDEN

Em uma análise minuciosa sobre o caso, as analistas forenses Heather Mahalik, Cindy Murphy e Sarah Edwards (2016) observam como os níveis de encriptação aumentaram a cada lançamento do sistema operacional do iPhone (iOS). Dispositivos iOS com o chip A4 (iPhone 4, iPad) e anteriores (operando com iOS 7 ou mais antigos) não ofereciam grande resistência para a extração de imagens de disco[6], o que possibilitava o acesso a todo ou a maior parte do conteúdo de dados armazenado no aparelho.

A partir do lançamento do chip A5 (iPhone 4S, iPad 2), em 2011, os aparelhos ofereceram criptografia *Advance Encryption Standard* (AES) de 256 bits no nível do *hardware*. A implicação disso é que a extração de imagens de disco permite apenas a visualização do sistema de arquivos e os metadados[7], enquanto o conteúdo dos arquivos permanece encriptado a menos que a senha do usuário seja utilizada para decriptação desse conteúdo antes da extração.

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 de 256 bits fundida no dispositivo durante sua fabricação, o chamado UID. O UID não pode ser lido diretamente por nenhum *software* ou *firmware*, apenas os resultados das operações de encriptação e decriptação que o envolvem. Além disso, o UID assegura que os dados estejam criptograficamente atrelados àquele dispositivo

6 Arquivo único que replica a estrutura e conteúdo de uma unidade de armazenamento digital de dados, geralmente criada a partir da cópia bit-a-bit, setor-a-setor da mídia de origem.

7 Dados sobre outros dados, por exemplo: nome do arquivo, seu tamanho e seu tipo.

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 configurar uma senha para o dispositivo, o usuário ativa automaticamente uma tecnologia intitulada “Proteção de Dados”. Essa tecnologia encripta um conjunto de arquivos a partir de uma combinação do UID com a senha do usuário. Sempre que o usuário insere sua senha, ela é trançada[8] com a UID do dispositivo, o que assegura que as tentativas de desbloqueio precisem ser realizadas naquele dispositivo específico. Se a senha inserida for correta, a chave capaz de decriptar o conteúdo dos arquivos é produzida e o aparelho é desbloqueado. Isso significa que sem o conhecimento prévio da senha definida pelo usuário, o conteúdo dos dados normalmente não pode ser decriptado.

Para acessar o conteúdo desses dados sem conhecer a chave, seria necessária então a utilização de um ataque criptoanalítico de força bruta[9] com o objetivo de descobrir a senha do usuário. Para “desencorajar ainda mais ataques de força bruta” (APPLE INC., 2012, p. 9), a Apple adiciona duas funções: 1) um tempo de espera crescente a partir de cada tentativa malsucedida; e 2) uma função de ativação opcional que destrói uma das chaves necessárias para acessar os dados automaticamente após 10 tentativas malsucedidas consecutivas de digitação da senha. Isso torna os ataques de força bruta inviáveis, pois além do tempo absurdo que se levaria para realiza-los, 10 tentativas falhas poderiam resultar na perda do conteúdo que se quer ler caso a função opcional esteja ativada[10].

CRIPTOGRAFIA DO IPHONE: DEPOIS DE SNOWDEN

Em 2013, o mundo recebeu as revelações de Edward Snowden sobre os diversos programas de vigilância massiva empregados pela Agência de Segurança Nacional (NSA) dos Estados Unidos[11]. 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

8 O “trançamento” referido nos *White Papers* de segurança do iOS é um processo de fortalecimento de chave no qual o algoritmo PBKDF2 é utilizado como função de derivação de chave utilizando AES chaveado com o UID do dispositivo como função pseudorrandômica (PRF) em cada iteração.

9 Criptoanálise refere-se ao conjunto de técnicas destinadas à decriptação de texto encriptado sem que se tenha o conhecimento prévio da chave criptográfica. Um ataque criptoanalítico de força bruta é um método específico que consiste na verificação sistemática de todas as senhas ou chaves possíveis até que as corretas sejam encontradas, também conhecido como busca exaustiva de chave.

10 Gilmor (2016) sugere uma forma de contornar essa função, porém o tempo de espera automático entre as tentativas permaneceria existindo.

11 PRISM, *Xkeyscore, Upstream, Quantuminsert, Bullrun e Dishfire*, para citar alguns desses programas.

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.

O programa PRISM, em especial, atraiu bastante atenção da mídia devido à cooperação de grandes empresas de tecnologia como Microsoft, Yahoo, Google, Facebook e Apple na vigilância. Ao garantir à NSA acesso ao conteúdo de e-mails, o histórico de buscas, os arquivos transferidos e as mensagens trocadas pelos usuários, essas empresas efetivamente tornaram-se participantes ativas nas violações de direitos perpetuadas pelo Estado estadunidense. Um dos documentos adquiridos pelo jornalista Glen Greenwald sobre esse programa mostrava especificamente a cooperação da Apple com o programa a partir de 2012. Na ocasião das revelações, a Apple negou já ter ouvido falar no PRISM (GREENWALD, 2013).

Em setembro de 2014, pouco antes do lançamento da versão 8 do iOS, a companhia lançou um novo site destinado a aumentar a 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 com a vigilância estatal no texto, Cook explicita a política de privacidade da companhia através do que poderia ser lido como um ataque evidente aos modelos de negócios de empresas rivais como Google e Facebook[12]:

> 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. (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 assegura 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 em posse do governo. Segundo a empresa, tal conteúdo estaria inacessível para qualquer um que não conhecesse a

12 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”.

senha definida pelo usuário, incluindo a própria empresa (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*). Por outro lado, na versão seguinte do guia de segurança, lançada em setembro do mesmo ano, mesma seção, mesma subseção, lê-se:

> *Os aplicativos principais do sistema como o Mensagens, Mail, Calendário, Contatos, Fotos e os valores de dados do Saúde, usam a 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*).

Na época, o pesquisador e ativista Christopher Soghoian (2014) resumiu a mudança da seguinte forma: "A política antiga da Apple para extrair dados dos usuários a partir de iPhones para a polícia: volte com um mandado. Sua política nova: cai fora".

Hoboken e Schulz (2016, p. 10) observam que o debate ascendido pós-Snowden levou a um aumento notório no emprego de medidas de encriptação por parte dos provedores de serviços de internet. Empresas como Whatsapp e Facebook, por exemplo, passam a utilizar encriptação de ponta-a-ponta[13] por padrão em seus dispositivos, ao passo que diversos provedores de serviços-web adotam o protocolo TLS[14] em seus sites.

Embora a Apple historicamente tenha aumentado a encriptação a cada lançamento do iOS, as novas medidas de segurança da versão 8 tem implicações especialmente decisivas para as relações entre a empresa, o público e o Estado, de forma que me parece adequado situá-las nesse contexto pós-Snowden de reforço da privacidade por parte das empresas de tecnologia da informação. Tal fato foi observado pelo diretor do FBI numa palestra ministrada cerca de um mês após o anuncio das novas medidas de encriptação da Apple.

---

13 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 asseguraria que nenhum terceiro tenha acesso ao conteúdo comunicado, incluindo o próprio provedor de serviço.

14 *Transport Layer Security*, 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.

O título da palestra de James Comey era “Going Dark: Tecnologia, privacidade e segurança pública estão em curso de colisão? ” (COMEY, 2014). O argumento central era que as revelações de Snowden teriam levado à uma “perspectiva dominante”, porém equivocada, segundo a qual o Estado estaria coletando todas as comunicações dos cidadãos. Segundo ele “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 de *Going Dark*[15]: 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 na escuridão, ilegível para a NSA” (SCHULZE, 217, p. 55). A difusão da encriptação tornaria essa esfera uma espécie de território livre para a atividade criminal, “tudo em nome da privacidade e segurança de rede” (COMEY, 2014). Nessa narrativa, a privacidade é encarada em oposição à segurança pública. Na ocasião da palestra, Comey explicitamente comentou a respeito das novas medidas de encriptação anunciadas pela Apple, afirmando que a encriptação “não é apenas uma característica técnica, é uma jogada de marketing” (Ibid.).

“ASSISTÊNCIA TÉCNICA RAZOÁVEL”: AS DEMANDAS DO FBI

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 o 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 (USA, 2016a, 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.

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

15 Termo 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.

incidente e outras informações pertinentes acerca do incidente (USA, 2016a, p. 2). A Apple possuía os “meios técnicos exclusivos” (USA, 2016a, 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 (USA, 2016a, 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*[16] para a encriptação da Apple, pois a reivindicação do governo seria da suspensão de funções “adicionais, não ligadas à encriptação” (USA, 2016c, 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 (USA, 2016a, 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.* (USA, 2016a, p. 15, *ênfase minha*).

16 Em termos muito gerais, *backdoor* pode ser definido como uma vulnerabilidade (frequentemente colocada intencionalmente) em um sistema que possibilita a um atacante contornar os mecanismos de autenticação convencionais para obter acesso não-autorizado a dados desse sistema.

“UM BACKDOOR PARA O BACKDOOR”: A OPOSIÇÃO DA APPLE

A recusa da Apple em cumprir a ordem judicial fundamentou-se 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. (USA, 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: A) o problema da chave-mestra; B) o problema do precedente perigoso.

O primeiro argumento, de caráter mais técnico, consiste na asserção de que o 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 como 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).

> Eu sei que todo mundo gosta de colocar isso como privacidade versus segurança, como se você pudesse abrir mão de uma e obter mais da outra. Eu acho que isso é muito simplista e incorreto, eu não vejo dessa forma de modo algum. (COOK, 2016c).

A Apple (USA, 2016d, 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 torna-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[17], 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. (USA, 2016d, p. 3).

Como evidência, a empresa cita o promotor de justiça de Manhattan, Cyrus Vance, afirmando ter entre “155 a 160” (USA, 2016d) 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. (USA, 2016d, 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. O argumento questiona a

17 Comey (THE ENCRYPTION... 2016, p. 47): “As forças policiais crescentemente encontram celulares que não podem ser desbloqueados em investigações por todos os lados”.

legitimidade das demandas do FBI ao apontar que as implicações políticas do estabelecimento desse precedente ultrapassam em muito o 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).

"Então isso pareceu como um *backdoor* para o *backdoor*. Você sabe, tentar forçar alguém a colocar um *backdoor*, tornar as pessoas mais vulneráveis, claramente atropelando liberdades civis" (COOK, 2016c). "Estamos desafiando as demandas do FBI com o mais profundo respeito pela democracia americana e amor por nosso país" (COOK, 2016b).

"*GOING DARK*" x "A ERA DE OURO DA VIGILÂNCIA": NARRATIVAS DE SEGURANÇA EM CONTRASTE

Wolfendale (2017) discute as diferentes formas como "segurança" pode ser definida. Segundo a autora, o conceito só pode ser definido negativamente: "é a ausência de ameaças contra valores importantes como a vida, a integridade corporal, a saúde e a propriedade" (WOLFENDALE, 2017, p. 76-77). Além disso, deve ser definida em referência "ao ator cujos valores devem ser assegurados, os valores envolvidos, o grau de segurança, os tipos de ameaça, as formas de lidar com tais ameaças, os custos de fazê-lo e o período de tempo relevante" (BALDWIN, 1997, p. 17 apud WOLFENDALE, 2017, p. 76).

No caso aqui investigado, o FBI e a Apple constroem narrativas opostas acerca da segurança. Para a agência de investigação, segurança é segurança pública ou segurança nacional, noções diretamente atreladas nessa perspectiva à capacidade do Estado para investigar e prevenir ameaças físicas, como terrorismo. As ameaças à segurança nesse caso são tanto os criminosos quanto, indiretamente, as empresas de tecnologia na medida em que estas desenvolvem e empregam tecnologias cujo efeito é impedir o acesso das forças policiais às comunicações das pessoas. A privacidade é vista como um valor individual em oposição à ao bem-estar coletivo.

Se assumirmos, conforme a sugestão de Rider (2017), que na década atual a responsabilidade sobre o modo como os métodos criptográficos são empregados tornou-se legitimamente aceita como sendo das empresas de tecnologia e não do Estado, isso coloca as agências de investigação numa posição delicada. Na

impossibilidade de interferir no desenvolvimento técnico da criptografia, ferramenta que, na perspectiva dessas agências, ameaça a segurança pública, é necessário desenvolver outros 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 exija acesso ao *software* criado e restrinja sua aplicabilidade técnica ao dispositivo de Farook. O que se buscava não era a capacidade técnica atual de decriptar conteúdo cifrado, e sim a capacidade política virtual de fazê-lo: o poder de compelir empresas de tecnologia a escrever *software* que tornaria tal processo realizável. Na prática, esse poder me parece ainda mais perigoso devido à possibilidade das forças policias compelirem as empresas a desenvolver outros tipos de *software* invasivo, como apontado pela Apple. 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 que a agência tivesse ciência da existência de alternativas técnicas para fazê-lo desde o início[18].

O posicionamento da Apple, por outro lado, tem como base uma noção de segurança diretamente atrelada à privacidade. O argumento técnico aqui é que a única forma segura de impedir a exploração de uma vulnerabilidade técnica por parte de criminosos ou *hackers* é não a permitindo existir, em primeiro lugar, algo que tem como consequência impedir sua exploração pela polícia do mesmo modo. Nas palavras de Tim Cook (2016b): “Não há algo como um *backdoor* para os mocinhos. Uma vez que você tem isso, os vilões vão encontrá-lo também”. Nesse sentido, os benefícios da segurança de um sistema criptográfico tão forte quanto possível simplesmente ultrapassam os malefícios no quadro geral das coisas.

Além disso, a noção de segurança atrelada à privacidade acionada aqui é tributária do discurso de ceticismo governamental dos anos 1990. O Estado não é apenas considerado inapto para garantir tal segurança (de forma que a responsabilidade por tal garantia seria das empresas de tecnologia da informação), mas ele próprio é concebido como uma das ameaças a ela. A concepção de mundo digital como imerso em trevas inacessíveis aos olhos do Estado dá lugar a uma que aponta a multiplicação dos olhos e ouvidos de uma autoridade pública que registra, armazena e analisa incessantemente as comunicações dos cidadãos. No lugar de “*Going Dark”*, “a era de ouro da vigilância” (SWIRE, 2015).

18 Snowden (A CONVERSATION... 2016): “O FBI diz que a Apple possui os ‘meios técnicos exclusivos’ para desbloquear o celular. Com todo o respeito, isso é balela”.

A recusa da Apple em cumprir a ordem judicial e sua justificativa pautada em valores como identidade nacional, liberdades civis e democracia assim cumprem uma dupla função. Em primeiro lugar, 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 as diferentes formas como a empresa tem repetidamente participado na violação desses mesmos direitos[19].

CONCLUSÃO

Casos como o caso Apple contra o FBI tem se tornado cada vez mais frequentes em todo o mundo. Na Inglaterra, o então primeiro ministro David Cameron expressou a intenção de banir dispositivos criptografados que as autoridades policiais não pudessem acessar (LOMAS, 2015). Em 2017, o Departamento de Justiça dos Estados Unidos fez reivindicações sucessivas por uma espécie de meio-termo denominado como "encriptação responsável" por oposição à "encriptação à prova de mandados"[20] (PFEFFERKORN, 2017). No Brasil, os bloqueios sucessivos do aplicativo WhatsApp, mediante a impossibilidade por parte das autoridades públicas de acessar o conteúdo encriptado das mensagens trocadas, resultaram numa audiência pública convocada pelo Supremo Tribunal Federal (EXTRA, 2017).

Uma vez que as guerras criptográficas estão de volta e não parecem estar indo embora no futuro próximo, me parece fundamental um esforço de engajamento efetivo com a técnica e suas implicações para além de uma mera denúncia do teor político existente "por trás" de toda e qualquer decisão técnica. Para além dos vícios disciplinares e das afirmações generalistas sobre a política nos artefatos, disputar as implicações práticas de decisões técnicas concretas. Como afirma Haraway (1995, p. 13):

> Desmascaramos as doutrinas de objetividade porque elas ameaçavam nosso nascente sentimento de subjetividade e atuação histórica coletiva e nossas versões 'corporificadas' da verdade, e acabamos por ter mais uma desculpa para não aprendermos nada da Física pós-Newton [...]

19 A participação da empresa com a vigilância da NSA no PRISM em 2012 e sua cooperação com as medidas de censura do governo chinês em 2017 (CADELL, 2017) são exemplos dessas violações da privacidade e da liberdade de expressão de seus usuários.

20 Especialistas em segurança tem observado que o que esses termos efetivamente designam são encriptação fraca e forte, respectivamente. A inexistência de um meio-termo real apoiado pela comunidade técnica tem levado especialistas a classificar a tal encriptação responsável como "solução imaginária" (MCLAUGHLIN, 2015), "um mito" (BLUE, 2017), "encriptação amigável à vigilância" (PFEFFERKON, 2017) e "solução do pônei mágico" (MCLAUGHLIN, 2016).

Finalmente, reitero a importância de observar os sentidos específicos dos termos empregados pelos atores ao navegar pelas operações de objetos técnicos. Esses termos, assim como as metáforas utilizadas, são acionados para a produção de narrativas políticas. As disputas em torno dos sentidos de termos como *backdoor* e "encriptação responsável" evidenciam o peso que tais expressões adquirem no reforço de narrativas específicas sobre segurança. Similarmente, metáforas como "*Going Dark*" e "chave-mestra" são empregadas para a legitimação de certas posições. Como nos lembra Gillespie (2014, p. 181), "mesmo o que parecem ser descrições nítidas de um processo por-trás-das-cenas são sempre *backstage* performado".

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.

APPADURAI, Arjun. **Modernity at large: cultural dimensions of globalization**. Minneapolis: University of Minnesota Press, 1996.

APPLE INC. Legal **Process Guidelines. Government & Law enforcement within the United States**. 23 jun. 2017. Disponível em: <https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf>. Acesso em: 12 dez. 2017.

_____. **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.

BALDWIN, David. A. The concept of security. **Review of International Studies**, v. 23, n. 1 pp. 5–26, 1997.

BLUE, Violet. Great, now there's 'responsible encryption'. **Engadget**, 27 out. 2017. Bad Password. Disponível em: <https://www.engadget.com/2017/10/27/great-now-theres-responsible-encryption/>. Acesso em: 16 dez. 2017.

CADELL, Cate. Apple, Facebook find something to praise China for amid internet clamp**. UK Reuters**, 6 dez. 2017. Business News. Disponível em:

<https://uk.reuters.com/article/uk-china-cyber/apple-facebook-find-something-to-praise-china-for-amid-internet-clamp-idUKKBN1DZ1A3>. Acesso em: 16 dez. 2017.

CESARINO, Letícia. Antropologia multissituada e a questão da escala: reflexões com base no estudo da cooperação sul-sul brasileira. **Horizontes Antropológicos**, Porto Alegre, v. 20, n. 41, p. 19-50, jun. 2014

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.

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

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.

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. 2016. **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.

DATE, Jack; LEVINE, Mike; NEWCOMB, Alyssa. 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-apple-iphone-encryption-case/story?id=37986428>. Acesso em: 11 dez. 2017.

EXTRA. **STF discute bloqueio do WhatsApp e Marco Civil da Internet, em audiência pública**. 02 jun. 2017. Disponível em: <https://extra.globo.com/noticias/celular-e-tecnologia/stf-discute-bloqueio-do-whatsapp-marco-civil-da-internet-em-audiencia-publica-21429234.html>. Acesso em: 15 mai. 2018.

FROOMKIN, Dan; MCLAUGHLIN, Jenna. 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.

GILLESPIE, Tarleton. The Relevance of Algorithms. In: GILLESPIE, Tarleton, BOCZKWSKI, Pablo. J. e FOOT, Kirsten. A. **Media Technologies: Essays on Communication, Materiality and Society**. Cambridge: MIT Press. 2014.

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

GREENWALD, Glen. 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.

HARAWAY, Donna. Saberes localizados: a questão da ciência para o feminismo e o privilégio da perspectiva parcial. **Cadernos Pagu**, Campinas, n. 5, pp.7-41, 1995.

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

LATOUR, Bruno. **Reagregando o social: uma introdução à teoria do ator-rede**. Salvador/Bauru : Edufba/Edusc, 2012.

LOMAS, Natasha. Here's what happened on Twitter after the UK PM said he wants to ban encryption. **Tech Crunch**, 13 jan. 2015. Disponível em: <https://techcrunch.com/2015/01/13/clearly-an-idiot/>. Acesso em: 16 dez. 2017.

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

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

MCGARRY, Caitlin. 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-sell-great-products-not-your-data-says-tim-cook.html>. Acesso em: 08 dez. 2017.

MCLAUGHLIN, Jenna. 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-between-apple-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-solution-encryption/>. Acesso em: 16 dez. 2017.

MEDINA, Jennifer; PÉREZ-PEÑA, Richard; SCHMIDT, Michael; GOODSTEIN, Laurie. San Bernardino suspects left trail of clues, but no clear motive. **The New York Times**, 03 dez. 2015. Disponível em: <https://www.nytimes.com/2015/12/04/us/san-bernardino-shooting.html>. Acesso em: 08 dez. 2017.

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

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

NELSON, Joe; EMERSON, Sandra. State, federal law enforcement agencies file in support of FBI in Apple battle. **The Sun**, 3 mar. 2016. Disponível em: <http://www.sbsun.com/2016/03/03/state-federal-law-enforcement-agencies-file-in-support-of-fbi-in-apple-battle/>. Acesso em: 13 dez. 2017.

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

QUIRK, Mary Beth. Apple: We won't unlock devices when the police ask, because iOS 8 doesn't let us. **Consumerist** 18 set. 2014. Disponível em: <https://consumerist.com/2014/09/18/apple-we-wont-unlock-devices-when-the-police-ask-because-ios-8-doesnt-let-us>. Acesso em: 09 dez. 2017.

RIDER, Karina. The privacy paradox: how market privacy facilitates government surveillance. **Information Communication and Society**, v. 4462, p. 1–17, abr. 2017.

ROGAWAY, Phillip. The moral character of cryptographic work. In: ASIACRYPT, 2015, Auckland. **Ensaio escrito para acompanhar fala proferida no evento.** Disponível em: <http://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf>. Acesso em: 11 abr. 2017.

SCHULZE, Matthias. 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, Nancy. Obama rejects 'absolutist' defense of encryption. **Politico**, 11 mar. 2016. Disponível em: <https://www.politico.com/story/2016/03/obama-apple-encryption-battle-220656>. Acesso em: 10 dez. 2017.

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

SOGHOIAN, Christopher. Tweet. **Twitter**, 17 set. 2014. Disponível em: <https://twitter.com/csoghoian/status/512414781312360448>. Acesso em: 13 dez. 2017.

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

SWIRE, Peter. The Golden Age of Surveillance. **Slate**, 15 jul. 2015. Disponível em: <http://www.slate.com/articles/technology/future_tense/2015/07/encryption_back_door

s_aren_t_necessary_we_re_already_in_a_golden_age_of.html>. Acesso em: 16 dez. 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. 2016. **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

UNITED STATES OF AMERICA (USA). 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. 2016a. Disponível em: <https://epic.org/amicus/crypto/apple/In-re-Apple-FBI-AWA-Application.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. 2016b. 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. 2016c. Disponível em: <https://epic.org/amicus/crypto/apple/In-re-Apple-FBI-Motion-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. 2016d. Disponível em: <https://epic.org/amicus/crypto/apple/In-re-Apple-Motion-to-Vacate.pdf>. Acesso em: 21 set. 2017.

WEBER, Peter. 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-sides-apple-fbi-iphone-encryption-fight>. Acesso em: 10 dez. 2017.

WOLFENDALE, Jessica. Terrorism, Security, and the Threat of Counterterrorism. **Studies in Conflict & Terrorism**, v. 30, n. 1, p. 75–92, 21 jan. 2007.

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