A Construção de Imaginários nas Narrativas Governamentais sobre Criptografia

André Ramiro

Resumo: Padrões e projetos políticos habitam as narrativas promovidas por setores governamentais em torno do desenvolvimento tecnológico. A segurança pública e nacional, o combate ao terrorismo, ao tráfico de drogas e outros fenômenos conhecidos são, historicamente, instrumentalizados para sedimentar um imaginário proposto pelas agendas das forças de investigação contra estruturas técnicas e sociais que protegem a privacidade. A criptografia é um símbolo fundamental dessas estruturas. Sendo assim, o estudo busca analisar as particularidades das narrativas governamentais que tensionam em favor da flexibilização da criptografia. Esse discursos dão forma a "imaginários sociotécnicos", exercícios de poder que moldam moralidades, materialidades e significados relacionados à ciência e à tecnologia. Procurou-se, portanto, apontar suas potências, fissuras e fundamentos com a intenção de poder contribuir para uma melhor compreensão sobre as disputas narrativas geopolíticas em torno da criptografia e, assim, auxiliar em incidências políticas.

1. Introdução: contexto histórico e pertinência política

Sintomas de disputas por direitos humanos na Internet se refletem em discursos. Isso pode ser encontrado, de forma sistêmica, em retóricas encampadas por agentes políticos que atraem o debate sobre o fortalecimento e a necessidade de estruturas de vigilância, sobretudo aqueles que simbolizam instituições centrais na dinâmica geopolítica de cooperações para investigações criminais e compartilhamento de informações de inteligência. As expressões discursivas que têm por objeto a criptografia simbolizam esse movimento, permitindo-nos uma análise sobre as narrativas e recursos retóricos que dão a roupagem dessas manifestações.

A encriptação moderna acompanha, lado a lado, o desenvolvimento tecnológico e está presente de maneira cada vez mais fundamental e robusta na construção de serviços de comunicação, comércio online, transações financeiras, dispositivos conectado e uma ampla extensão de sistemas, de aplicação extraterritorial, que dependem da segurança que a criptografia provê (Abelson et al, 2015). Além disso, é compreendida como método cada vez mais necessário à garantia e proteção de posicionamentos políticos, defesa da liberdade de expressão e da privacidade (Kaye, 2015). Apenas assegurando a comunicação contra a interferência de terceiros é que usuários comuns da Internet, defensores dos direitos humanos, ativistas políticos e jornalistas investigativos podem se proteger dos suspeitos olhos dos governos ao redor do mundo (Anistia Internacional, 2016) – e a criptografia é um recurso central para essa finalidade.

Contudo, casos judiciais emblemáticos, fatos políticos sensíveis e regulações têm impulsionado investidas argumentativas que apontam para a relativização do potencial de encriptar comunicações. Ao passo que avançam algoritmos que tornam comunicações cada vez mais privadas, a exemplo da encriptação ponta-a-ponta encontrada em aplicações de mensageria e a encriptação de disco *por padrão* encontrada em aparelhos celular, o repertório de testemunhos e discursos governamentais, sobretudo dos Estados Unidos, Reino Unido, Austrália e, na América Latina, do Brasil, em sua esmagadora maioria investem em favor do relaxamento de uma "criptografia inquebrável" e questionam o interesse social uma suposta "privacidade absoluta" (G7 France, 2019).[1]

[1] Mais recentemente, o G7 (Grupo dos países de industrialização mais expressiva, formado por Alemanha, Canadá, Estados Unidos, França, Itália Japão e Reino Unido) propôs, como uma de suas meta, mais esforços e cooperação multilateral para que "soluções de acesso" (a conteúdos encriptados) sejam atingidas. Mais detalhes em **Combating the**

Afinal, argumenta-se, a popularização do uso da criptografia tem "obscurecido″ as investigações, fenômeno que vem sendo reforçado e repetido sistematicamente como "*Going Dark"* (Zittrain et al, 2016), já definido como "um eclipse nas capacidades investigativas do governo" (Barr, 2019a), o que vem mantendo viva a falsa dicotomia entre privacidade e segurança pública (Solove, 2011; Landau, 2018).

Não são recentes os recursos narrativos que sustentam o *lobby* governamental por cooperações mais estreitas e permissivas com empresas de tecnologia ou por regulações mais restritivas à criptografia. Pornografia infantil, crime organizado, terrorismo e tráfico de drogas[2] são algumas das frequentes cartadas dos agentes de investigação quando querem dar substância às suas narrativas e, assim, convencer seu público através de retóricas que provocam o pânico e o medo. No entanto, não somente essas figuras são utilizadas para alicerçar seus posicionamentos, mas outras ferramentas discursivas mais sutis – mais adiante analisadas - vêm sendo tecidas nas palavras das principais figuras dos órgãos de investigação criminal, a exemplo do *Federal Bureau of Investigation* (FBI) e do *Department of Justice* (DOJ) nos Estados Unidos, e do Ministério Público Federal no Brasil.

Com efeito, é possível afirmar que a frequência e a forma com são costurados esses padrões retóricos, ao longo de décadas, constroem imaginários sociotécnicos. Abstrações governamentais que dizem respeito, por um lado, aos cenários sociais e políticos aos quais a população estará destinada com o aumento drástico e impune dos mais graves delitos e associações criminosas, possibilitado por uma criptografia "à prova de mandados" - deixando como vítimas as crianças e instituições tradicionais, como a "família", a "polícia" e a própria "nação" - e, por outro, aos impactos tecnológicos refletidos na massificação do uso da criptografia – como o crescimento exponencial do seu uso para finalidades ilícitas.

Performados publicamente, os imaginários contribuem para a construção de entendimentos que servem de ferramentas políticas, ou seja, utilizados para intervir em configurações e distribuições de poder. Constituem "imaginários sociotécnicos" que, para Sheila Jasanoff (2015), moldam moralidades, materialidades e significados das formas que constituem a vida social. Ainda que possam ser originados a partir de visões de indivíduos específicos, ganham tração através de exercícios de poder ou mesmo de atos sustentados pela construção de coalizões institucionais.

O status da criptografia, atualmente, é resultado de décadas de construção de imaginários através da história, compartilhados por distintos setores da sociedade. Monges e outras figuras religiosas da Idade Média, por exemplo, utilizavam-a para enviar mensagens cifradas, o que rendeu à criptologia associações com artes ocultas. Estados investiam em desenvolvimento de técnicas de encriptação enquanto recursos crítico para épocas de tensão política e informacional, como a Guerra Fria[3]. Estigmas sobre espionagem internacional, programas e documentações governamentais secretas, amplamente explorados pela cultura popular[4], também tinham o uso de cifras como elemento central de comunicação.

Já na segunda metade do século 20, cruzadas contra o uso massificado da encriptação foram se articulando, enquanto que a instrumentalização da criptografia foi ganhando espaço para dar eficácia à garantia de direitos fundamentais. Assim, foi ganhando corpo uma robusta narrativa da

---

`use of the Internet for terrorists and violent extremist purposes. G7 France, 2019. Disponível em http://www.g7.utoronto.ca/justice/2019-internet.pdf. Acesso em 15/12/2019

[2] Por convenção, naturalizou-se chamar de "Cavaleiros do Infocalipse" as figuras que habitam as justificativas por medidas restritivas de direitos na Internet. Parece não haver consenso sobre quais seriam os "cavaleiros". Ao longo de anos, já figuraram o sequestro, a pirataria, a espionagem, lavagem de dinheiro ou tráfico de armas, também associados ao por quê de, supostamente, haver prejuízos no anonimato online ou, nesse caso, em uma criptografia forte. Mais em Carey e Burkel (1999), May (1994).

[3]Cfr. KHAN, David (1996).`

[4]*Sneakers* (1992), *Enigma* (2001), *The Imitation Game* (2014), *Pi* (1998), *North by Northwest* (1959), para citar alguns.

sociedade civil para empoderar o indivíduo com a popularização de técnicas acessíveis de encriptação e mobilizações sociais (o *Pretty Good Privacy* – PGP[5], o movimento *cipherpunk*[6] ou, mais recentemente, as c*ryptoparties*[7]) - diante de uma emergente vigilância abusiva governamental, potencialmente onipresente, simbolizada pela banalização de grampos ilegais[8], pelo acesso direto de agências de inteligência a servidores de provedores de aplicação (Greenwald e MacAskill, 2013) e uma diversidade de outros programas de vigilância que vieram à tona.

Nesse mosaico de significados, os discursos legitimadores são fundamentais e a tecnologia – nesse caso, a criptografia - se era vista meramente como um domínio dos "fatos e artefatos", agora é associada ao *storytelling,* à imagem e à imaginação (McNeil et al, 2017). Historicamente, o Estado é o principal ator na expansão e evolução de imaginários sociotécnicos, sobretudo por meio de políticas públicas, regulações e outros institutos (Jasanoff e Kim, 2009; McNeil et al, 2017), ainda que, hoje, a atuação do marketing privado seja central na afirmação de um ideal de modernidade (ref. Sadowski e Bendor, 2018; White, 2016) estabelecendo seus limites, necessidades e negue, na maioria das vezes, seu conteúdo ético.

De toda forma, a disputa de narrativas parece residir em toda construção política, sobretudo quando se tratando da regulação de tecnologias e suas interseções com a garantia de direitos. Testemunhar, nesse caso, as nuances dos imaginários que estão sendo projetados pelo Estado significa realizar um mapeamento de fragilidades e potencialidades de seus discursos, como interpretam o alcance da privacidade e, assim, como justificam racionalidades que resultam em programas de vigilância, na violação estrutural de direitos humanos e em projetos hegemônicos de poder. Por fim, essa análise também objetiva fortalecer o ferramental discursivo da sociedade civil e da comunidade acadêmica no âmbito das lutas sobre políticas públicas que tenham por objeto a (não-)regulação da criptografia. Na medida em que imaginários sociotécnicos estão em constante mutação e disputa por uma diversidade de setores de interesse, tornar evidentes esses elementos narrativos também significa afastar leituras que historicamente procuram criminalizar ferramentas e indivíduos (Derechos Digitales, 2019) cuja missão é fortalecer a proteção à privacidade.

2. Metodologia - quatro recortes: setorial, territorial, temporal e material.

Qualificar uma linha evolutiva sobre as narrativas construídas a respeito da criptografia alcança um escopo territorial e temporal que, a rigor, remonta a milhares de anos, como por exemplo, à Segunda Guerra Mundial e mesmo ao Egito Antigo (Kahn, 1996). Na tentativa de contextualizar politicamente, inclusive a partir de realidades tecnológicas contemporâneas e tomando o estado da arte da criptografia, foi necessário realizar quatro recortes de diferentes naturezas em relação à extensão da pesquisa.

O primeiro deles é de caráter setorial. A natureza pluri-participativa da Internet sugere que protocolos, infraestruturas, práticas e, sobretudo, políticas e legislações que dizem respeito à rede sejam construídos por todos aqueles setores da sociedade que carregam interesses naturais no desenvolvimento dos seus recursos críticos. No âmbito da Governança da Internet, a abordagem se convencionou chamar de "multissetorialismo" (Kurbalija, 2016), experiência de construção política que procura agregar a participação de setores distintos, porém de igual importância na construção da Internet, entre eles a comunidade técnica/acadêmica, o governo, o setor privado e a sociedade civil

[5]ZIMMERMAN, Phil (1999).
[6]HUGHES, Eric (1993).
[7]Movimento descentralizado de eventos que percorre várias partes do mundo com o objetivo de transmitir conhecimento acerca de segurança e liberdade digital, incluindo, principalmente, técnicas de encriptação das comunicações. Mais em https://www.cryptoparty.in/. Acesso em 15 de dezembro de 2019.
[8]Para mais informações, recomenda-se o portal disponível em https://grampo.org. Um "dossiê" online com materiais sobre a cultura ilegal de grampos telefônicos no Brasil. Acesso em 15 de dezmbro de 2019.

organizada, cada um com agendas específicas e, muitas vezes, conflitantes. Estes mesmos conflitos apontam para o fato de que a atenta observação das ferramentas narrativas de cada setor auxilia na construção política ao desvendar coerências, incoerências, interesses colaterais e, principalmente, parâmetros de respeito aos direitos fundamentais.

Em se tratando da criptografia, representações estatais como nações e instituições públicas são historicamente centrais, ora investindo em pesquisa, incentivo e desenvolvimento científico, ora procurando limitar seu uso, disponibilidade, regras de exportação e robustez (Abreu, 2017) - como atualmente - ao tempo em que procuram legitimar práticas que esvaziam a privacidade e a liberdade de expressão. Portanto o interesse específico em narrativas governamentais reflete uma forma de promover o constante escrutínio público sobre como o Estado constrói imaginários que justificam suas ações.

Outro recorte é de natureza territorial. O delineamento geopolítico em torno da criptografia assume diferentes formatos, ora ganhando força em torno de coalizões de países como os Cinco Olhos[9] ou o G7, ora em forma de outras configurações que, de uma maneira ou de outra, refletem a influência do norte-global. Porém, por motivos de maior centralidade político-econômica, por historicamente ter se posicionado com mais vocalidade e consistência em torno do debate sobre o acesso excepcional e por influenciar, em razão de sua hegemonia, políticas públicas de outros países, os Estados Unidos protagonizam as investidas contra a criptografia forte. O país vem contribuindo para um repertório de narrativas e, portanto, para a criação de um imaginário encabeçado pelas principais figuras-chave das forças de investigação criminal no país, em especial os membros do FBI e do DOJ.

Logo, em razão de um contexto sociopolítico propício para a observação, essa pesquisa, procurou analisar, em primeiro plano, o debate no território estadunidense. De toda forma, em situações em que foi necessário ressaltar discursos de outros países cruciais na contextualização do debate atual sobre criptografia, este fundamentalmente transnacional, discursos proferidos em outros países também foram levados em consideração para tornar mais claros e sugestivos os padrões narrativos identificados.

A partir uma realidade sociopolítica distinta, porém de forma paralela, a América Latina também vem protagonizando episódios de bloqueios de aplicações[10] e retirada de conteúdo[11] tanto por imprecisões legais, quanto por motivações políticas. Entre os episódios, a negativa (e impossibilidade) de provedores de aplicação em ceder conteúdo de comunicações encriptadas, "descumprindo" ordens judiciais, vem animando a justiça brasileira, levando ao bloqueio do aplicativo Whatsapp por três vezes no Brasil. Atualmente, tramitam perante o Supremo Tribunal Federal brasileiro duas ações - a Ação Direta de Inconstitucionalidade nº 5.527 e a Ação de Descumprimento de Preceito Fundamental nº 403 (ref.) - que tematizam, entre outras questões, os bloqueios do Whatsapp e põe em jogo, ainda que de forma indireta, regulações à criptografia. Serão centrais na criação de precedentes judiciais sobre bloqueio de aplicações ou suspensão de atividades em razão de impossibilidade técnica em ceder comunicações encriptadas. Além disso, as representações das forças de investigação brasileiras, em especial do Ministério Público Federal (MPF) e da Polícia Federal (PF), também têm dado um passo à frente e firmado sua participação no debate em uma série de declarações, notas técnicas, participação em audiências públicas e fóruns especializados. Por essas razões, o território também figura como terreno, na América Latina, para a observação de narrativas governamentais sobre a criptografia.

---

[9] Coalizão de cooperação de inteligência informacional que reúne a Austrália, Canadá, Nova Zelândia, Reino Unido e Estados Unidos.

[10] Uma linha do tempo das derrubadas de aplicações da Internet está disponível em Bloqueios.info.

[11] COSTA, Gilberto (2018).

Partindo do hipótese de que o ano de 2013 – em razão das revelações de Edward Snowden sobre abusivos programas de vigilância da NSA (Greenwald, 2014) - foi o epicentro contemporâneo para o fortalecimento das agendas pró-privacidade e das contra-narrativas aos discursos governamentais, confirmando teorias sobre a extensão do horizonte de vigilância estadunidense, foi tomado esse ano como o marco inicial temporal de análise dos discursos. O intervalo entre o ano de 2013 e a data de publicação deste estudo foi assumido, portanto, como o recorte temporal. Assume-se a hipótese de que o contexto sociopolítico tenha provocado uma sofisticação nas narrativas governamentais, as quais passaram a considerar o direito à privacidade enquanto concessão ao debate e inauguraram novos recursos argumentativos, inclusive na busca pela desqualificação de um "radicalismo" pós-Snowden (Comey, 2014).

Por fim, um recorte material priorizou uma busca documental, principalmente a partir de registros descritos, datilografias, relatórios técnicos, discursos públicos, testemunhos oficiais, entrevistas, depoimentos, debates em fóruns especializados e outros materiais disponíveis na Web que vêm refletindo narrativas governamentais das agências de interesse. Como forma de contrabalancear e referenciar posicionamentos estatais a partir de um referencial mais amplo, foi utilizada literatura especializada e contemporânea, sobretudo proveniente da sociedade civil organizada e da comunidade acadêmica. Assim, procurou-se localizar as balizas que relacionam o uso da criptografia com a garantia de direitos humanos.

3. Imaginários sociotécnicos enquanto ferramenta de análise tecnopolítica

Nos Estudos de Ciência, Tecnologia e Sociedade, a observação multidisciplinar de fenômenos que atravessam fatores sociais, políticos e tecnológicos vêm modernizando a abordagem científica sobre os fluxos de construção social (Felt et al, 2017). Artefatos, indivíduos, idéias, conhecimentos, meios de comunicação e outros elementos humanos e não-humanos, materiais e não materiais, são levados em consideração para formar uma rede de associações sociotécnicas.

O conceito de "imaginário sociotécnico" emerge dessa área do conhecimento e encontra em Sheila Jasanoff seu expoente. Abarca "visões de futuros desejáveis, coletivamente construídas, institucionalmente estabilizadas e performadas publicamente, animadas por compreensões compartilhadas de formas de vida e ordem social, alcançadas através de – e suportadas por - avanços na ciência e na tecnologia" (Jasanoff, 2015). "Imaginários" não mais se reduzem a meras fantasias, simples fugas da realidade, passatempos ou contemplações, mas se tornam áreas organizadas de práticas sociais, formas de trabalho e negociação (Appadurai, 1990), contribuindo, portanto, para a construção de projetos políticos.

Ao estabelecer um elo entre "ideias" - aqui identificada por discursos, testemunhos e outras manifestações da linguagem - e "tecnologias" - aqui percebidas pela criptografia - o conceito de imaginários sociotécnicos desempenha um importante papel na análise das narrativas que circulam a retórica do "obscurecimento" entoada por uma série de agências de investigação para enfraquecer a criptografia e facilitar o acesso ao conteúdo das comunicações. Assim, a associação entre tecnologias, política e sociedade pode ser analisada através desse quadro.

Partindo do entendimento de que a linguagem é um meio crucialmente importante para a construção de imaginários (Jasanoff e Kim, 2009) e, portanto, formações sociais e políticas, a identificação de elementos discursivos recorrentes – bem como sua conotação - se mostra importante para estabelecer um paralelo entre a performatividade dos agentes governamentais e o assentamento contínuo de imaginários adaptados às rotinas e narrativas das agências de investigação. Pretende-se contribuir, neste estudo, mais com uma coleção de peças narrativas que caracterizam os discursos e que qualificam a retórica do "obscurecimento" como um imaginário sociotécnico, e menos com uma abordagem que trabalhe ou conjecture a (im)possibilidade técnica de haver um acesso excepcional

sem que haja perda de segurança ou esvaziamento de direitos.

Nos discursos aqui explorados, a construção de imaginários não se limita à observação de casos recentes ou históricos, situando o debate em fatos concretos ou objetivamente analisáveis, mas também investem em uma projeção de cenários futuros. Encaminham-se narrativas com base em uma crise presente, de caráter processual-investigativo, mas que se inclina ao futuro, no rompimento social iminente, simbolizado pela impunidade e liberdade que aproveita uma barbárie (entre abusadores de menores, terroristas e traficantes de drogas), o que romperia com as possibilidades de segurança pública diante de uma ameaça. A sustentação de uma "crise", portanto, terá o poder de catalisar o debate.

Nesses discursos, a leitura de um dado desafio sociotécnico possível de ser observado - tal como os obstáculos/liberdades provocados pela criptografia - não basta à interpretação, mas o ato de criar, imaginativamente, também é exercitado. Logo, o futuro é chamado a compor o cenário das crises atuais, acentuando-se os conflitos através do tempo. As representações investigativas aqui exploradas teriam, supostamente, autoridade para projetar as repercussões que estariam por vir diante do "obscurecimento", já que vivem, rotineira e sigilosamente, os processos afetados negativamente pela criptografia. Ao mesmo tempo, vale notar que estatísticas apresentadas - por exemplo, sobre o número de aparelhos inacessíveis em razão da encriptação, porém necessários às investigações – são metodologicamente mal construídas, exageradas ou imprecisas[12]. Da mesma forma, não há evidências de que o uso da criptografia eleve a frequência de crimes (Lewis, Zheng e Carter, 2017), como propõe o imaginário governamental. Identificar-se com as narrativas propostas, portanto, implica em desconsiderar suas fissuras e, ao mesmo tempo, exercitar a imaginação criativa sob a regência desses atores.

Assim se organiza a montagem de uma ameaça. Certamente, a exploração desses fatos sociais geram reações políticas que podem "eleger" as ameaças enquanto tal, respaldando narrativas que objetivam influenciar o desenvolvimento tecnológico e uma determinada área do planejamento científico nacional, regulando-a. Seria possível fazer um paralelo entre a construção desses imaginários sociotécnicos e as retóricas da securitização[13], entendida como uma engenharia de "seguranças e inseguranças" públicas a partir de discursos. Essa fabricação, por sua vez, geraria energia política e contexto para motivar a construção de políticas públicas (Weaver, 1995 *apud* Williams, 2003). As ameaças, no entanto, são eleitas por atores determinados, bem como *o que* deve ser considerado uma ameaça e *como* devemos lidar com ela (Cavelty, 2013). Essas construções são utilizadas para legitimar medidas de segurança extraordinárias que, normalmente, não seriam aprovadas por uma audiência democrática na ausência de uma ameaça (Schultze, 2017), como no caso de um *backdoor.*

De toda forma, o imaginário que tange a criptografia sofreu mutações ao longo das últimas décadas. Com mais veemência a partir da década de 90, pode-se apontar que tenha assumido o sintoma das disputas sobre as liberdades civis. Isso por que, durante grande parte do século 20, o uso da criptografia era conferido, em maior parte, quase que exclusivamente a agências militares e de inteligência governamentais (Kehl, Wilson e Bakston, 2015). Nos Estados Unidos, sobretudo na esteira da Segunda Guerra Mundial e da Guerra Fria, a disputa informacional, a exemplo da corrida científica, gerava à criptografia o caráter de instrumento militar e todos os produtos que a tinham

[12]Acess Now et al. Letter to Department of Jutice Inspector General Requesting Investigation into FBI's Device Miscalculation. Human Rights Watch, 2018. Disponível em https://www.hrw.org/news/2018/06/04/letter-department-justice-inspector-general-requesting-investigation-fbis-device. Acesso em 15 de dezembro de 2019.

[13]Conceito advindo da Escola de Compenhage. Propôs uma nova abordagem às análises sobre segurança, dando ênfase à linguagem e aos discursos. "Na teoria da securitização, "segurança" é tratada não enquanto uma condição objetiva, mas como um produto de um processo social específico: a construção social dos problemas relacionados à segurança (*quem* ou *o que* está sendo assegurado *do que*) é analisada a partir do exame dos "atos-discursos 'securitizadores'". Em Williams (2003).

como recurso eram controlados pelo *International Traffic in Arms Regulations* (ITAR), além de figurarem na listagem oficial de munições (Dam e Lin, 1996). A regulação da sua exportação e as restritas regras para publicação de técnicas criptográficas objetivavam evitar o empoderamento de nações adversárias, mas também o seu uso indiscriminado no âmbito doméstico (Kehl, Wilson e Bakston, 2015).

Mas ainda partir de 1976, com a publicação do trabalho seminal de Whitfield Diffie e Martin Hellman (1976), onde foi apresentada a "criptografia de chave pública", inaugurou-se a possibilidade de pessoas e empresas comuns se comunicarem de forma segura sobre redes modernas de comunicação e superar o histórico monopólio governamental sobre as cifras de encriptação (Khel, Wilson e Bankston, 2015). A partir daí, é possível encontrar a germinação dos primórdios das "cripto guerras" e a fabricação de um novo imaginário sobre a criptografia.

A partir da década de 90, então, com a popularização da Internet comercial, com as disputas em torno do *Clipper Chip*[14] e, consequentemente, com o ganho de força das instituições e movimentos (ciber)ativistas (simbolizados pelos *cipherpunks,* para a temática aqui tratada) o imaginário se reforma e a criptografia passa a significar, a um só tempo, um obstáculo para o acesso às comunicações e um símbolo da luta pela privacidade. Através de criação de uma dicotomia - alimentada até os dias de hoje, sobretudo pelos discursos governamentais aqui explorados - pairava a ideia de um desequilíbrio sintetizado, de um lado, pela privacidade e, de outro, pela segurança pública. Sobre essa falsa correlação, o imaginário governamental acerca da criptografia irá se construir.

4. Análise de narrativas

É comum assumir que crises são, com frequência, gatilhos para mudanças em paradigmas (Danblon, 2007). Justificam a passagem de um estado social bem estabelecido a outro, já que a ordem anterior, aparentemente, não teve sucesso em lidar com a nova ordem ou configuração política. Não é difícil observar que, por exemplo, a retórica da crise está presente em discursos de polarização política que motivam personagens como Donald Trump e Jair Bolsonaro ou campanhas como o Brexit (Thompson, 2016), em um contexto mais amplo. Logo, a existência de supostas realidades críticas são a motivação ideal para políticas impopulares e para a suspensão, por exemplo, de direitos fundamentais – como a privacidade. Fundamentalmente, portanto, a criação de crises compõe o imaginário que acompanha as retóricas anti-criptografia.

Em grande parte dos discursos governamentais das agências representativas de investigação criminal, a construção argumentativa aponta para a iminência de um estado caótico social provocado por vetores como a encriptação forte, identificada como encriptação "à prova de mandados" (Rosenstein, 2017) , criando "zonas livres do alcance da lei" ou "ilimitadas áreas do mundo digital que são imunes ao escrutínio do sistema judiciário" (Rosen, 2019). Para esta linha de raciocínio, a construção desses "espaços" estaria longe de ter origem em uma cooperação legítima e democrática, mas seriam arquitetadas pela vontade única econômico-empresarial, "um espaço sem lei, criado, não pelo povo americano ou por seus representantes eleitos, mas pelos donos de grandes empresas" (Wray, 2019), "motivados pelo lucro" (Rosenstein, 2017), em uma abordagem quase avessa à mais-valia, seria possível apontar. Atualmente, estariam soterrados os meios de defesa da sociedade em troca do

[14]Propostas da *National Security Agency* - NSA - para implementação de *chips* de encriptação nos aparelhos comercializados pelas empresas de telecomunicações nos Estados Unidos. Ocorre que, além de encriptar, também inseria *backdoors* para acesso excepcional de autoridades policiais norte-americanas. O sistema, que ficou conhecido como *key escrow*, ou "custódia de chaves", sugeria que quando a autoridade policial acreditava serem os conteúdos das comunicações necessários a investigações, se dirigiam aos órgãos que possuíam a custódia das chaves e, assim, conseguiriam a decriptação daquela troca de mensagens e o acesso à comunicação de um dado usuário. O episódio gerou uma série de reações tanto de natureza mercadológica quanto sociais, reacendendo a luta pela privacidade nos Estados Unidos. Para uma análise mais detalhada, conferir Levy (1994) e Ramiro (2018).

sucesso das empresas de tecnologia. Restaria apenas a memória idílica de uma época de ordem social e eficácia jurídica: "os bons e velhos dias de aplicação da lei" (Comey, 2015a), quando a vigilância não encontrava obstáculos, "se foram" (Comey, 2015b).

Parece que quando os provedores de aplicação possuem protocolos bem estabelecidos de cooperação com as agências de investigação, a crítica ao empresariado é suspensa. Enquanto estes forem fornecedores de informações, pistas, dicas, conteúdo de comunicações ou mesmo possuam canais de acesso direto por parte dos setores da inteligência estatal (Greenwald e MacAskill, 2013), então essas plataformas cumpririam seu "dever cívico" (Rosenstein, 2017). Negligenciam, deliberadamente, a emergência d e um dever de responsabilidade dos provedores de aplicação com o desenvolvimento de sistemas e serviços cada vez mais seguros ao ecossistema tecnológico."A encriptação não é apenas um recurso técnico: é um *pitch* de mercado" (Comey, 2014)l, ou seja, é menos uma questão técnica e mais uma escolha relacionada ao modelo de negócio (Barr, 2019b). Em outras palavras, "seu negócio é vender produtos e ganhar dinheiro (...) enquanto nosso negócio é prevenir crimes e salvar vidas" (Rosenstein, 2017).

Como aponta Cory Doctorow (2018), o FBI insiste que desenvolvedores apenas não estão se esforçando ou sendo *nerds* o suficiente. Como se o debate girasse em torno de crenças pessoais ou simplesmente do auto-convencimento "Eu simplesmente não acredito na afirmação de que é impossível", afinal, "se nós podemos desenvolver carros autônomos que dão independência para que os cegos e deficientes se transportem; se nós podemos estabelecer mundos virtuais, totalmente gerados por computadores, para elevarmos ao próximo patamar o entretenimento e a educação de forma segura (...) certamente nós devemos ser capazes de fabricar dispositivos que, a uma só vez, ofereçam segurança e permitam acessos legais com ordem judicial" (Wray, 2018). Respaldando a retórica do solucionismo (Morozov, 2013) tecnológico, reinante no Vale do Silício, que promete um futuro brilhante e soluções impossíveis, segue o DOJ ao afirmar que "provedores de tecnologia estão trabalhando para construir um mundo com exércitos de drones e frotas de carros autônomos, um futuro de inteligência artificial e realidade aumentada. Certamente essas empresas podem fabricar produtos que forneçam segurança enquanto permitem o acesso por meio de ordem judicial" (Rosenstein, 2017).

Encontra eco no debate brasileiro a crença de que uma solução de acesso à encriptação ponta a ponta apenas não é alcançada pois não há vontade suficiente: "esses instrumentos foram criados por homens. E, se foram criados por homens, podem ser desenhados de forma diferente" (Aras, 2017), reduzindo a possível saída a uma questão eminentemente humana. O imaginário reforçado por essas agências parecem fazer acreditar que soluções tecnológicas, sobretudo aquelas que encontram limites na própria matemática, podem se curvar a uma insistente vontade humana e a uma "certeza" que não leva em conta décadas e décadas de pesquisa em segurança da computação (Pfefferkorn, 2017a).

Crises causadas por uma "implementação tecnológica irresponsável" parecem não se limitar a uma dimensão técnica – ou de viés meramente comercial - da criptografia, mas se estendem a um aspecto cultural, afetando também a razoabilidade, a boa fé e o senso crítico daqueles que advogam pela privacidade. Em um mundo pós-Snowden, onde "o pêndulo parece ter ido longe demais" (Comey, 2014) o ceticismo exercitado pela sociedade civil em relação ao poder estatal parece ter cedido lugar a um cinismo (Comey, 2015b) provocado por um sopro de radicalismo que induz ao medo e à desconfiança. Assim, são marginalizadas as obrigações dos provedores com as agendas da sociedade civil, como o devido processo legal - espaço esse confundido com a crise jurídico-criminal ocasionada pela popularização da criptografia. E infantilizam aqueles que se opõem: "É tempo de termos um debate aberto e honesto sobre liberdade e segurança" (Comey, 2014), "Deve ser um conversa séria e adulta (...) Espero que você participe" (Comey, 2016a). Especialistas avessos às soluções de acesso excepcional ou "advogados da privacidade absoluta" (Rosenstein, 2017) parecem sofrer de uma crise da razão.

Outras engenharias percorrem o imaginário governamental, como as que procuram ressignificar termos já estabelecidos na literatura através da repetição de novas chaves terminológicas. Enquanto convencionou-se, no setor científico-acadêmico, chamar de "encriptação forte" um sistema criptográfico computacionalmente seguro, que não prevê meios de quebra ou qualquer outro mecanismo de acesso (Schneier, 1996) (assim, um mandado judicial não surtiria efeito), a retórica do DOJ, reforça o que chama de "encriptação responsável" – ou seja, aquela que proporcionaria meios de acesso excepcional. Assim, resta à encriptação forte ser "à prova de mandados" ou, por dedução, ser *irresponsável*. Ao substituir a *robustez* da criptografia pela *irresponsabilidade*, é animada uma disputa moral cuja responsabilidade sobre as consequências – ilustradas por estes mesmos atores governamentais - recai sobre as plataformas, aos defensores da privacidade ou, em última análise, aos criptógrafos. No que seria possível responder: responsável para quem? (Pfefferkorn, 2017b), recolocando a questão posta acima: a única responsabilidade sensata das plataformas, então, seria com a polícia, sob risco de um colapso criminal. Aqui, a linguagem é manipulada para restringir a interpretação e, por que não, o próprio acesso à informação – uma vez que cria uma tendência para a opinião pública sobre a tecnologia ao opô-la à lei desde o *nome* pelo qual é chamada - sobretudo no que se refere a um tema sobre o qual poucos têm real conhecimento: como funciona a criptografia e o que está em jogo.

Um verdadeiro exercício de *branding* é operado para reduzir a criptografia a uma "moldura" estabelecida por estes atores[15]. A forma a partir da qual a questão é enquadrada é crucial para se definir quais valores e narrativas irão se sobressair (Bennett, 2008). "Emoldurar" ou "enquadrar" o debate sobre a criptografia em termos de obstáculos, afrontas ou mesmo atentados à eficácia das investigações criminais e ao processo penal, associando-a à criação de uma zona anárquica, em um jogo binário de "presença/ausência" do Estado, é deixar de fora outras dimensões – sociais, culturais, tecnológicas, econômicas e mesmo subjetivas -, utilidades e finalidades da criptografia que não dizem respeito, por exemplo, a relação do indivíduo com o Estado ou à uma simples relação de resposta à vigilância. Uma equivocada equação onde investigações criminais estariam para a sociedade enquanto a privacidade estaria para o indivíduo, como forma de afastar seu valor social-coletivo. Logo, o enquadramento para a qual é empurrado o debate também faz parte de um esforço político provocado por um imaginário governamental em construção. "A artimanha verbal é, em si mesma, uma prática da inteligência (Donner, 1981). Para isso, novos rótulos seriam necessários.

Como aponta Phillip Rogaway (2015), as narrativas governamentais são fabricadas de forma a garantir o direcionamento do discurso exatamente para onde as autoridade querem que se encaminhe, em um movimento que aponta para o discurso do medo: medo do crime, medo de que os pais percam a proteção sobre os filhos e, inclusive, medo do escuro (Pfefferkorn, 2017a). Essa fabricação de enganos seria, em si mesma, uma tradição narrativa da inteligência estatal.

A metáfora do "obscurecimento" recebeu, ao longo dos últimos anos, atenção de acadêmicos em razão da sua dimensão apelativa a um signo do medo, o terror que acompanha o imaginário sobre o escuro, as sombras, o desconhecido. A associação encontra apoio, com frequência, no estudo seminal de George Lakoff e Mark Johnson, "Metaphors We Live By" (2003), onde sustenta-se que o papel das metáforas vão além da estética, da linguística ou das ferramentas descritivas, mas têm o poder de criar a própria realidade. Ou seja, podemos encontrar relações com as técnicas de definir *molduras* ou *enquadramentos* em razão de uma finalidade política de controle sobre a direção do debate. A estratégia de reforçar uma metáfora, inclusive, nos instiga a dar por garantida a forma sobre

[15] Da mesma forma, é interessante notar que é posta nova roupagem linguísitca a práticas iminentemente culturais da vigilância - as quais vêm carregando uma aura cada vez mais ameaçadora e ilegal - como forma de re-enquadrá-las em eufemismos. "Vigilância em massa" se torna "coleta em massa", "grampo" se torna "cobertura confidencial" e mesmo "espionagem" cai em desuso, cedendo lugar à genérica "coleta de dados". Uma melhor análise dessa reforma linguística pode ser encontrada em Murphy (2019) e Greenwald (2015).

a qual pensamos a respeito de algo (Watson, 2018) e, assim, reconfigura o próprio significado (Gill, 2018) da criptografia.

A escuridão estaria avançando: "se os desafios da interceptação em tempo real ameaça levar [o FBI] ao obscurecimento, a encriptação ameaça levar a todos nós à escuridão." "Imagine", Comey nos convida ao seu território, "que o FBI trabalha em uma sala. O canto dessa sala tem estado no escuro pelos últimos vinte anos (...) esse canto escuro começou a tomar o espaço inteiro". Uma enganosa ameaça criptográfica toma espaço e se confunde com a escuridão total: "a ubíqua encriptação por padrão nos aparelhos, a ubíqua encriptação forte nas aplicações e outras formas de comunicação tem propagado as sombras e agora está tomando mais e mais a nossa sala (Comey, 2017).

Policiais mortos, crianças desaparecidas, aumento vertiginoso do tráfico de drogas, estupros, pedofilia e drástica queda nas capacidades de solucionar crimes parecem ser imagens que percorrem o cenário apocalíptico sistematicamente ilustrado. "O tsunami de opióides, cocaína e metanfetamina que surgiu nos Estados Unidos" parece apenas ter sido possível em razão do crescente uso de ferramentas de encriptação. A rede de crimes possibilitada teria consequências diretas não apenas para a sociedade civil, mas daria margem ao extermínio de policiais pelos mesmos cartéis de drogas. Encontram associações com um "cartel que usou o WhatsApp" aplicação que parece ser central para a viabilidade e expansão de redes de organizações criminosas, "para o propósito específico de coordenar o assassinato de oficiais de polícia baseados no México" (Barr, 2019a). As investidas contra a encriptação são pinceladas com casos concretos, percentuais e estatísticas sobre emboscadas e oficiais de polícia assassinados pelos mesmos atores que fazem uso da encriptação. Ainda que nem sempre haja uma correlação direta com os dados sobre policiais mortos em serviço, a linha narrativa é construída em uma ambientação comum onde o uso da encriptação e os percentuais de mortes de oficiais convivem.

Enquanto a criptografia desorganizaria a força policial, fortaleceria o crime e comprometeria o própria modelo institucional do Estado representado pelas agências de investigação. Para James Comey, não haveria futuro para a segurança pública diante do fenômeno do "obscurecimento", situação em que "[nós] estamos perdendo de vista predadores que exploram os mais vulneráveis entre nós... perdendo de vista violentos criminosos que apontam para nossas comunidades... perdendo de vista células terroristas que estão usando mídias sociais para recrutar, planejar e executar ataques." A distopia caracterizada pela banalização dos crimes hediondos bate à porta: "caso [a criptografia forte] se torne a regra, eu sugeriria a você que casos de homicídios se estabelecerão, suspeitos andarão livremente e violadores de crianças não serão descobertos ou processados", não em razão de problemas históricos, estruturais e complexos, como a questão racial nos Estados Unidos, a desigualdade social ou mesmo a centralização da energia e do capital investigativo policial na falida guerra às drogas, mas apenas em razão de um celular bloqueado ou um disco rígido encriptado. Os valores, na construção argumentativa, não dizem respeito a uma equação complexa em que a segurança, resiliência e estabilidade da rede estão em jogo, em que a liberdade de expressão de milhões e milhões de indivíduos correm risco, profissões que dependem dos sigilo das comunicações, como para jornalistas e defensores públicos, são ameaçadas, mas "tudo em nome da privacidade e da segurança da rede" (Comey, 2014).

Ainda que os termos da disputa sobre a criptografia no Brasil sejam diferentes dos contexto norte-americano – encontram mais enfoque na jurisdição, na essencialidade dos serviços de mensageria e na constitucionalidade do bloqueio de aplicações no país (Antonialli, 2019) - a visão sobre o reinado da impunidade, causado pela criptografia, se repete e se afirma como o âmago do imaginário sociotécnico das forças investigativas. Para a Polícia Federal no Brasil, "nós temos todo o *iter criminis*: cogitação, preparação, execução, consumação, e, logo depois, o exaurimento. Todo esse *iter criminis,* todo esse leito de um rio com águas turvas de criminalidade, ele é percorrido, hoje,

por meio de aplicativos de comunicação. Não há uma investigação da Polícia Federal que, em momento oportuno, não se revela que atos de cogitação - porque não atos de preparo - ordens de execução, são feitos por meio de comunicação. (...) Então, hoje, nós temos um cenário livre na criminalidade; cenário livre!" (Leal, 2017).

Os quadros pintados na composição do imaginário anti-encriptação não apenas jogam com um cenário habitado pelos mais chocantes crimes, que passariam impunes, mas também inserem um elemento temporal crítico e urgente em seu *storytelling,* como a fabricação de uma bomba-relógio. Esse colapso se aproximaria em direção à nós e, inevitavelmente, provocará um choque. Do encontro entre a "defesa irrazoável" da privacidade e o esvaziamento da segurança pública, o resultado é uma realidade colapsada. "O relógio está contando", alerta William Barr (2019b). Além disso, a imagem de um impacto físico e mecânico, entre esses dois corpos, se apresenta. "[E]ssas duas coisas queridas para nós estão em colisão. (...) o uso da encriptação está se chocando com nossa necessidade de alcançar a segurança pública (...) todos já realizaram que estamos em colisão (...) um choque entre duas coisas que valorizamos." (Comey, 2015c). As figuras criadas parecem induzir à ansiedade ao enfatizar a urgência e a real possibilidade de uma catástrofe que virá a qualquer momento e de qualquer lugar. Para William Barr (2019a), "O tempo para atingir [soluções que fornecerão o acesso legal] é limitado (...) um grande incidente deve ocorrer a qualquer momento e irá reaquecer a opinião pública sobre essas questões (...) Enquanto o debate se arrasta e o desenvolvimento da encriptação à prova de mandado é acelerado, nossa habilidade de proteger o público contra ameaças criminais está rapidamente se deteriorando.". A falência policial estaria próxima.

Plataformas de encriptação - ou "paraísos digitais" (Aras, 2019) - passam não só a serem meios fatalmente encontrados por pessoas mal intencionadas para ocultar o conteúdo de comunicações criminosas, mas seriam *desenhadas* com a específica finalidade de impedir o acesso legal (Barr, 2019a) e se esquivar da obrigação de fornecer registros de comunicação (Ministério Público Federal do Brasil, 2016). Um "sonho que se torna realidade para predadores de crianças e pedófilos" ou, na paródia performada, “algumas empresas querem dizer ao indivíduo: ei, nós podemos te deixar invisível para as autoridades policiais" (2019b). Uma plataforma que os permite encontrar e se conectar com crianças e outros criminosos afins que não temem consequências", afinal, redes de conspiração pedófila depositam sua confiança nessas plataformas (Wray, 2019). Se James Comey, de forma comedida e razoável, é fã da privacidade e da criptografia (Comey, 2015b), hackers, terroristas e abusadores de menores a amam (Comey, 2016b) desproporcionalmente. É categórica a associação e induz à dedução: por que existiria a defesa política e técnica de algo que figuras hediondas veneram?

Especial ênfase é dada ao fato de certas aplicações encriptarem mensagens por *padrão*. Quer dizer, uma aplicação possuir a *possibilidade* de encriptar comunicações – em uma ação que podemos chamar de *opt-in,* que demande a ação positiva do usuário – não parece ser um problema considerável nessa disputa. Sobre a simples disponibilidade da criptografia ao usuário, o FBI sustenta que nunca foi um problema: "os esforços do país em alcançar um equilíbrio em mais de 200 anos não foram dificultados pela tecnologia (...) digo dessa forma por quê a encriptação sempre esteve por perto por décadas, sempre disponível a usuários sofisticados" (Comey 2015b). Em um possível contrassenso sob a ótica da segurança da informação e dos mais progressistas princípios da privacidade, da autodeterminação informativa e da proteção de dados, a quimera surge quando o recurso de segurança é implementado sem a necessidade de ação proativa do usuário – ou seja, por padrão - o que minaria, por exemplo, o resgate de crianças das mãos de abusadores e a supressão da distribuição de imagens relativas à pedofilia na rede: "o horizonte tem mudando debaixo de nossos pés. Com a disseminação da encriptação por padrão, provedores, com frequência, não tem a capacidade de identificar terríveis imagens com dados encriptados. Isso significa que pistas como as que nos permitiu resgatar as três garotas mencionadas [casos de abuso de menores] – essas pistas simplesmente não seriam enviadas. O dano não é interrompido. As vítimas – aquelas pequenas crianças – ainda estariam aí fora sofrendo abusos" (Wray, 2019) Diante do imaginário proposto, ser a favor da encriptação por padrão nas

aplicações significa ser conivente – ou, no mínimo, paciente - com a permanência das crianças nas mãos dos abusadores.

Dos mais importantes princípios do que se convencionou chamar de P*rivacy by Design* (Cavoukian, 2009) - série de fundamentos que propõem um suficiente e resiliente desenho industrial, desde fábrica, para que um produto respeite a privacidade e a autonomia do indivíduo, regras básicas para qualquer legislação de proteção de dados no mundo – a *privacidade por padrão* amadurece o entendimento de que o indivíduo não precisa realizar qualquer configuração técnica para que sua privacidade se mantenha intacta e suficientemente respeitada. Ir de encontro à padronização da proteção ao sigilo é enfraquecer a autonomia individual e chancelar uma lógica de exploração política e econômica sobre as comunicações privadas. Essa mentalidade, certamente, confirma a necessidade das agências de investigação em relação ao mercado de dados pessoais, uma vez que, enquanto houver mineração e capitalização sobre dados comportamentais dos usuários, será maximizada a potencialidade vigilantista governamental.

Os ataques à encriptação por padrão sintetizam e explicitam as estreitas relações do Estado com as engrenagens do capitalismo de vigilância (Zuboff, 2019). Caso estremecida essa relação, quedaria aleijada a capacidade policial: "a encriptação [por padrão] de comunicações e dispositivos colocam em grande risco a segurança pública *quando*[16] é parte de serviços de consumo no mercado de massa." (Rosenstein, 2017).

5. **Dissensos no imaginário governamental**

Imprimir a ilusão de consenso e unidade - mesmo que internamente a um dado setor - sobre um determinado problema, fazendo parecer que há um entendimento consolidado, é um dos efeitos políticos da criação de um imaginário. Na luta regulatória, envolvendo outros setores de interesse da sociedade, a potencial solidez de uma posição governamental pode projetar a adesão de legisladores ou mesmo insegurança a outros setores que fazem frente a culturas narrativas levadas à frente por setores do governo, como aqueles de investigação.

Não é por acaso a forte vocalidade dos líderes da força policial norte-americana, tanto em seu território, quanto em expansões de influência via coalizões geopolíticas internacionais (Five Country Ministerial, 2018). A solidez e continuidade de suas declarações, construindo um imaginário sociotécnico ao longo de quase duas décadas, raptam a narrativa de outros agentes do mesmo Estado e, ao mesmo tempo, de forças policiais e de inteligência de outros países, principalmente aqueles do sul global. Outras realidades discursivas podem ilustrar novos entendimentos governamentais que contradizem a narrativa até aqui exposta, o que podemos chamar de contranarrativas ou *contraimaginários*. Tecnicamente, a título de discursos setoriais, ainda que as citações a seguir levantadas digam respeito a personagens que, tecnicamente, não mais fazem parte da representação governamental, ajudam-nos a (des)construir ou apontar fissuras nas narrativas do setor público a partir da fala daqueles que ja representaram Estados que, atualmente, lideram a construção do imaginário governamental sobre a criptografia. Hoje, opinam a partir de um lugar de fala privado, porém foram considerados enquanto racionalidades que herdaram interesses e pensamentos estratégicos do setor público.

Ex-diretores de algumas das mais importantes agências de inteligência vêm contribuindo para a construção de um dissenso sobre as disputas em torno da criptografia. Seria possível interpretar que o peso da representação governamental, ao ser aliviado, permite genuínas manifestações da expressão e, talvez, mais realistas, ao ver o panorama tecnopolítico de fora da disputa, associando o avanço tecnológico, as liberdades fundamentais e a macro-visão dos reais riscos de segurança. Jonathan

[16]Grifo meu.

Evans, ex-chefe do MI5 (agência nacional de inteligência do Reino Unido, um dos países mais posicionados na busca por vias alternativas à encriptação forte) parece sugerir que o conhecimento prático sobre os meandros da inteligência, da vigilância e das ciber-guerras entre Estados deveria levar à busca pelo avanço da segurança - e não sua flexibilização. "Enquanto compreensivelmente existe uma legítima preocupação sobre o contra-terrorismo, essa não é a única ameaça que enfrentamos: o modo pelo qual o ciberespaço está sendo usado por criminosos e governos é uma ameaça ainda mais ampla aos interesses do Reino Unido" (Grierson, 2017). Estrategicamente, o espectro de ameaças à segurança nacional, às informações governamentais sensíveis e infraestruturas críticas se expõem a riscos quando a encriptação das comunicações se enfraquece. "Nossa infraestrutura crítica depende profundamente da Internet, nós precisamos estar realmente confiantes de que temos tornado isso seguro, pois nosso dia a dia e economia irão depender da segurança que empregamos para nos proteger de ciber-ataques."

Na contramão desse entendimento, recentemente William Barr propôs que o problema do "obscurecimento" não diz respeito à proteção de "códigos de lançamento nuclear", mas apenas à "cibersegurança do consumidor", ou seja, simplesmente às comunicações como em *smartphones* e e-mails (Barr, 2019a). Talvez seja, em parte, verdade, mas ignora o grande espaço ocupado por comunicações - relativas à segurança nacional – efetuadas por legisladores, diretores executivos de empresas, funcionários das próprias agências de investigação e inteligência, chefes de Estado, operadores de usinas elétricas, juízes e outros "meros consumidores" cuja vulnerabilidade geraria riscos que vão além da esfera individual (Schneier, 2019).

Também se constrói a contranarrativa levando em consideração o medidor econômico que gira em torno da disputa. Sustentam Mike McConell, ex-diretor da *National Security Agency* (Agência de Segurança Nacional - NSA), Michael Chertoff, ex-secretário do *Homeland Security* (Departamento de Segurança Interna dos Estados Unidos) e William Lynn, ex-Secretário Adjunto de Defesa dos Estados Unidos, que "tal sistema de encriptação [ponta-a-ponta] protegeria de ataques a privacidade individual e informações empresariais em um nível muito maior do que o que atualmente existe" (McConnell, Chertoff e Lynn, 2015). A criptografia seria fundamental para a estabilidade da influência econômica e, consequentemente, o poder político e militar delas derivariam. Inclusive a manutenção do *status quo* socioeconômico – podemos ler como "manutenção da hegemonia" -, através da influência predominante global norte-americana, se beneficiaria da segurança oferecida pela encriptação das comunicações. "Se os Estados Unidos querem manter seu papel global e influência, é essencial proteger interesses empresariais da massiva espionagem econômica. E esse imperativo deve compensar os benefícios táticos de se fazer mais acessíveis comunicações encriptadas a autoridades ocidentais" (McConnell, Chertoff e Lynn, 2015). Aqui, já é possível ver um novo perfil narrativo, o qual, ainda que mantenha o centralismo dos interesses norte-americanos, enxerga a segurança das comunicações como caminho seguro e recomendado para se alcançar metas de protagonismo econômico.

Dito de outra forma, o caráter político-estratégico da criptografia para os Estados também recebe contornos relativos à competitividade informacional, como as travadas entre Estados Unidos, Rússia, China ou Coréia do Norte, simbolizadas por outros imaginários sociotécnicos históricos que atravessam todo o século 20 - como a corrida espacial, a energia atômica (Jasanoff e Kim, 2009), e a corrida comunicacional-tecnológica. Ganha peso o receio de que outros Estados e economias rivais tenham disponíveis soluções de acesso potencialmente viabilizadas pelo governo norte-americano: "o que diremos a outros países? Quando outros países disserem 'ótimo, nós também queremos ter uma chave duplicada', em Pequim, Moscou ou qualquer outro lugar?", questiona Michael Chertoff. ″As empresas não terão uma base principiológica para se recusarem a fazê-lo. Então isso será um problema estratégico para nós" (Farivar, 2015). A perspectiva faz sentido e deve ser considerada, não a nível de rivalidade entre as nações citadas, mas de ciência política complexa em torno das decisões regulatórias sobre o acesso excepcional, situação em que não haverá dois pesos e duas medidas. As

correlações ultrapassam fronteiras nacionais, soluções objetivas, aparentemente domésticas e bilaterais entre um dado governo e uma dada empresa (Budish, Burkert e Gasser, 2018).

"A experiência nos mostra que não estamos exatamente no escuro, como, às vezes, pensamos estar", segundo Chertoff (Farivar, 2015). Se o medo impresso pelo obscurecimento - de que as investigações percam por completo seu poder de visão - reina no imaginário governamental, na prática, a *previsão* não parece também vingar ou é, no mínimo, hiperbólica. "A história nos ensina que o medo de que a encriptação ubíqua irá causar o obscurecimento é superestimado" (McConnell, Chertoff e Lynn, 2015). Resgatam a década de 90 - quando o problema do Clipper Chip protagonizou as guerras criptográficas - para dizer que a mesma linha de raciocínio foi levantada para justificar um grande programa de acesso excepcional às comunicações e violação do sigilo. Quer dizer, tanto o presente quanto o passado contradizem o imaginário governamental atual. "Quando a matemática da encriptação de 'chave pública' foi descoberta enquanto uma forma de possibilitar proteção criptográfica de forma mais ampla e por menor custo a todos os usuários, alguns oficiais de segurança nacional estiveram convencidos de que, se a tecnologia não fosse restrita, as forças policiais e as organizações de inteligência ficariam cegas e surdas." A retórica do obscurecimento se antecipava, ainda que com outra roupagem, porém "o governo Clinton e o Congresso rejeitaram o Clipper Chip baseados na reação das empresas e do público" (...) Mas o céu não caiu e nós não ficamos cegos nem surdos." Pelo contrário (Swire e Ahmad, 2011; Zittrain et al,)[17], "falando com as pessoas da área [da inteligência], sabe o que se ouve? Nós coletamos mais do que nunca. Nós encontramos uma forma de contornar essa questão" afirma Chertoff (Farivar, 2015).

Caso tornem possível o acesso excepcional, interessa pensar que os interesses da própria força policial seriam prejudicados. Atualmente, metadados das comunicações são coletados, disponibilizados e compartilhados com agências de investigação como política padrão de cooperação das mais populares plataformas do mundo. A inauguração de brechas nessas rotinas causaria uma fuga para serviços mais impopulares, desconhecidos, de difícil alcance cooperativo para as polícias, ou mesmo plataformas de fabricação própria das organizações terroristas, como já ocorre, por exemplo, com a Al Qaeda (Lewis, Zheng e Carter, 2017). "Um requerimento para que provedores norte-americanos criem uma chave duplicada não vai impedir que atores maliciosos achem outros caminhos e provedores de tecnologias que fornecerão encriptação ubíqua. Os vilões mais espertos irão encontrar caminhos e tecnologias que impeçam acesso e nós podemos ter certeza de que o mercado da 'dark web' irá oferecer uma miríade de capacidades" (McConnell, Chertoff e Lynn, 2015). Em outras palavras, para Chertoff, "Os reais vilões irão encontrar aplicações e ferramentas que os permitam encriptar tudo sem que haja um *backdoor.* Essas aplicações estão se multiplicando o tempo todo. A ideia de que você pode interromper isso, particularmente considerando a realidade global, é um apenas um sonho". Assim, nem os metadados restariam disponíveis. Os efeitos colaterais são incontáveis e os riscos imensuráveis, além de resvalar diretamente na segurança dos usuários comuns: "Isso pode levar a uma consequência perversa a partir da qual organizações que cumprem a lei e indivíduos percam a segurança de suas comunicações, enquanto atores maliciosos se aproveitarão." "Então você basicamente está deixando as coisas mais inseguras para o cidadão comum" (Farivar, 2015).

Àqueles que assumiram funções de liderança em cargos da alta inteligência nacional e superaram a falsa dicotomia entre "privacidade e segurança", a encriptação atinge sua finalidade e

[17] Uma diversidade de especialistas aponta para o fato de que a associação entre o aparto de vigilância governamental de ponta, o desenvolvimento de tecnologias de análise *big data*, e a grande quantidade de informações e dados pessoais sobre todos disponíveis online, teria levado às agências de investigação, não ao "obscurecimento", mas à era de ouro da vigilância. Mais precisamente, três aspectos apontariam para essa conclusão: os crescentes modelos de negócio baseados em coleta e tratamento de dados dos usuários; o fato de produtos serem oferecidos como serviços contínuos que implicam em permanente interface entre fornecedores e usuários e a expansão da Internet das Coisas, o que abriria uma nova fronteira para a expansão das formas de coletar informações a investigações criminais. Mais detalhes em Swire e Ahmad (2011) e Zittrain et al (2016).

fornece segurança pública quando não sofre interferência. Como afirma Michael Hayden, ex-diretor da NSA, "a segurança norte-americana é melhor servida com encriptação ponta a ponta inquebrável do que com portas da frente, dos fundos, laterais ou como você queira descrevê-lo (...) quando você observa a segurança norte-americana de uma forma macro, acho que os Estados Unidos estão mais seguros com uma encriptação que não possui uma porta que qualquer um pode explorar"[18].

Interessante notar que mesmo as contra-narrativas carregam um sentido político-histórico e pretendem manter os Estados Unidos na liderança econômica global. Assim, chamam atenção ao valor da criptografia para dar sentido a essa narrativa. Novos imaginários são agregados, como a guerra híbrida informacional entre ocidente e oriente, como a Rússia e a China. Os argumentos parecem apostar no revanchismo norte-americano que parte dos fantasmas da Guerra Fria. No entanto, fazem sentido quando apontam para a importância central da criptografia à nível de estratégia político-econômica-militar, afinal sua flexibilização significa a vulnerabilidade de um ecossistema de estruturas e valores críticos, como, para esses atores, segredos de negócio e segurança nacional.

6. Projetos políticos da narrativa anticriptográfica. A que(m) servem?

A partir de uma agência de provocações que buscam a antecipação de riscos, crises, desatualização da lei, incapacidade, fragilidade, insegurança e instabilidade social, as narrativas governamentais aqui analisadas partem de uma dificuldade técnica e avançam sobre um suposto desmonte das possibilidades de segurança pública. A aproximação do cenário caótico demanda esforço político e engajamento "antes que seja tarde". A impunidade de predadores sexuais, terroristas e outras figuras que habitam a narrativa governamental, exigiria medidas securitárias, ainda que isso seja pago com a redução da segurança na rede (Barr, 2019a).

Securitizar a criptografia tem o condão de estabelecer um precedente para que outras democracias liberais sigam o mesmo caminho (Schultze, 2017). Políticas provocadas pelo governo-norte americano excedem suas fronteiras e desdobram consequências no Reino Unido, França, Alemanha, Austrália, Canadá, Nova Zelândia, entre outros países que respondem à geopolítica global em torno do acesso às comunicações. Da mesma forma, as Filipinas, a China, a Arábia Saudita ou o Brasil, países atualmente reconhecidos por suas políticas antidemocráticas, marcante e sistemática perseguição aos jornalistas, ativistas, movimentos sociais e outras formas de organização e defesa dos direitos humanos, irão aparelhar soluções de acesso para atacar opositores.

Importante notar que, nos Estados Unidos, a prática vigilantista também têm assumido, historicamente, um caráter eminentemente político. Como extensamente documentado, a vigilância no país assumiu a missão de manter o *status-quo* (Donner, 1981) não apenas em âmbito doméstico, mas global. O monitoramento de dissidentes se tornou um pilar institucional para se manter a ordem política. Para ficar em um exemplo, universidades norte-americanas foram amplamente infiltradas com informantes, estudantes, funcionários e professores, os quais reportariam constantemente a uma extensa rede de agentes do FBI sobre qualquer manifestação política que porventura ocorresse nos centros acadêmicos. Líderes internacionais que ameaçassem a ordem ideológica liberal-econômica norte-americana eram – e ainda são – alvos de vigilância, muitas vezes com a finalidade de eliminação (Church Committee Reports, 1975).

Coalizões igualmente são estabelecidas precisamente para gerar impacto transnacional, como os esforços do G7 ou dos Cinco Olhos, os quais geram frutos como o *Access and Assistance Act* (Decreto "Anticriptografia" australiano)[19]. Analistas assumem que a Austrália foi o país perfeito para

[18]Business Insider. **Ex-NSA chief thinks the government is dead wrong in asking Apple for a backdoor.** Disponível em https://www.businessinsider.com/michael-hayden-encryption-apple-2016-2. Acesso em 15 de dezembro de 2019.

[19] Australian Government. Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018. Federal Register Legislation, 2018. Disponível em https://www.legislation.gov.au/Details/C2018A00148. Acesso em

a vanguarda das políticas públicas modernas de enfraquecimento à criptografia devido a sua falta de conjuntos abrangentes de regras de proteção aos direitos humanos, ausência de requisitos de equilíbrio com a proteção à privacidade e, por isso, abertura de espaço para a existência da iniciativa (Landau, 2018). Através de esforços conjuntos, autoridades policiais norte-americanas podem usá-la para fazer avançar sua própria agenda em linhas semelhantes.

De uma maneira geral, narrativas que esvaziam a privacidade interagem com um projeto político conservador que instrumentaliza a vigilância, não para incidência no cumprimento da lei e para a persecução penal, necessariamente, mas para sustar ou neutralizar movimentos que propõem mudanças sociais ou resistências políticas. No Brasil, por exemplo, é alimentada uma cultura de interceptação das comunicações distante de previsão legal ou justificativa plausível (Abreu e Antonialli, 2017), o que já rendeu ao país a fama de República da Escuta[20]. Em 2009, no episódio que ficou conhecido como "Caso Escher", a Corte Interamericana de Direitos Humanos condenou o Brasil a indenizar grupos de trabalhadores rurais associados ao Movimento Sem-Terra, os quais foram alvo de escutas ilegais no ano de 1999, em desrespeitando a vários aspectos da Lei de Interceptações. Ainda, partes do conteúdo das comunicações interceptadas foi ilegalmente vazada pelo poder público. Na mesma esteira, comunicações estabelecidas entre o ex-presidente Luís Inácio da Silva (Lula) e a ex-presidenta Dilma Rousseff foram grampeadas e vazadas - com intuito político de influenciar a opinião pública - pelo então juiz Sérgio Moro. Além disso, os trechos vazados foram colhidos em momento em que a autorização para a interceptação já havia expirado, o que resultou na anulação processual do conteúdo e sérias repreensões ao juiz por parte do Supremo Tribunal Federal (Borges, 2016).

O monitoramento de processos de organização e comunicação de movimentos sociais é uma constante e dialoga estreitamente com projetos de poder. Em 2013, o movimento Xingu Livre, coletivo de organizações e ambientalistas que atuam historicamente em oposição à Usina Hidrelétrica de Belo Monte no Estado do Pará, detectou a presença de um infiltrado gravando reuniões com uma "caneta espiã". O infiltrado havia sido contratado pelo consórcio de entidades responsável pela construção da Usina. O material seria analisado conjuntamente com a Agência Brasileira de Inteligência (Abin), ligada à Presidência da República (Xingu Vivo, 2013). Mais recentemente, em 2019, em Comissão Parlamentar de Inquérito (CPI) promovida pelo Congresso Brasileiro, foi revelado que o filho do presidente Jair Bolsonaro, grande influenciador do governo, pretendia criar uma "Abin paralela", com a intenção de montar uma entidade governamental específica para o monitoramento de adversários políticos através do emprego de grampos e criação de dossiês (Paduan, 2019), em um evidente aparelhamento dos serviços secretos e técnicas de vigilância para a execução de programas da extrema direita.

A abertura de possibilidades de acesso às comunicações encriptadas, somada à cultura de interceptação ilegal brasileira, daria brecha para a vigilância em massa e efetivação de planos políticos bem delineados através da eliminação de opiniões dissidentes. Sem dissenso e, consequentemente, sem liberdade de expressão, o progresso social é improvável (Rogaway, 2015).

Esse cenário se torna ainda mais patente e arriscado na realidade brasileira do governo de Jair Bolsonaro, o qual não ergue bandeiras de combate ao terrorismo, como os norte-americanos, mas de perseguição às ONGs, aos ativistas do movimento sem-terra, à militância ambientalista-indigenista contrária à indústria da mineração e ao agronegócio predatório, além de diversos outros grupos da ala progressista (Conectas, 2018; Seto, 2018). Desde a ótica da proteção aos direitos humanos e desde a histórica repressão à dissidência política, é possível supor que, caso possível o acesso excepcional às comunicações encriptadas, os alvos de interesse seriam, possivelmente, as figuras relacionadas aos movimentos por direitos políticos e sociais.

15 de dezembro de 2019.

[20] Para mais informações sobre o histórico abuso do uso de grampos ilegais no Brasil, visitar "Grampo.org".

Portanto, enxergar os propósitos do imaginário sociotécnico sobre a criptografia, para além da esfera investigativa ou técnica, implica em estabelecer um paralelo entre as narrativas e os projetos políticos hegemônicos e avessos à dissidência. A privacidade e o sigilo das comunicações inquietam, sobretudo, aqueles que buscam minar formas e forças de organização política e social. Phillip Rogaway quis chamar atenção para o "caráter moral do trabalho criptográfico" (Rogaway, 2015) – diante do aprofundamento orgânico da vigilância pública e privada, opressiva e com crescente desejo de controle, o profissional criptógrafo deveria carregar um dever moral de contribuir para a popularização da criptografia, associando-a à condição política e ao modelo democrático de sociedade. Consequentemente, é fundamental identificar o avesso: o caráter moral dos discursos que visam ao acesso às comunicações a partir do enfraquecimento da criptografia, sua ânsia de alimentar a cultura de vigilância e seu sistemático trabalho em ressignificar as tecnologias de proteção à privacidade.

7. Conclusão

Pelo menos dois caminhos, portanto, são sugeridos sob a leitura aqui proposta. Primero, de que as associações entre tecnologia e sociedade também residem nos discursos e narrativas performadas publicamente por autoridades governamentais, as quais arquitetam um imaginário sociotécnico. Segundo, que esse imaginário repercute sobre políticas públicas e está a serviço de um projeto de poder estatal que encontra alicerce em retóricas sobre a flexibilização da privacidade e no uso da tecnologia à serviço da vigilância. Tecnologias que reduzam esse potencial, portanto, são pintadas como motivadoras de desordens sociais. Os desafios que a criptografia gera carregam o poder de gravitar essas duas conclusões de forma significativa.

Isso não significa que o debate em torno da criptografia seja de fácil decifragem. Sua potência disruptiva traz, seguramente, reconfigurações para a cultura tradicional de investigações criminais, bem como para a sociedade no que significa comunicar-se em uma esfera verdadeiramente privada, o que possibilita o exercício de uma série de direitos individuais, coletivos e políticos que se associam à liberdade de expressão e à privacidade.

No entanto, em oposição a essa realidade posta, a articulação dos agentes governamentais aqui explorada sugere uma reação conservadora que procura desmontar avanços de ordem tecnológica e social. Fazem isso, muitas vezes, valendo-se de artifícios discursivos superficiais, injustos, de caráter sensibilizador e que promovem um cenário político baseado na prevenção policial diante de uma insegurança virtual[21]. Somadas aos jogos de re-significação de linguagens, às metáforas e ilustrações de cenários perturbadores, antigas figuras lançadas pra esvaziar direitos no ciberespaço são convocadas, como redes terroristas, pedófilos ou traficantes de drogas. Não se pretende negar as ameaças que esses fenômenos oferecem, mas, sim, questionar e chamar atenção quanto à precisão, peso e pertinência com os quais são utilizados, bem como seus propósitos políticos.

Ainda, riscos amplamente alertados, tanto a nível de segurança da informação (Abelson et al, 2015) quanto a nível de direitos humanos (Anistia Internacional, 2015; Schulz e Hoboken, 2016; Kaye, 2015) são deliberadamente desconsiderados. Logo, a omissão sobre esses temas, por parte dos atores aqui investigados, também é eloquente e constitui uma importante peça em suas construções narrativas. Enquanto os interesses das agências de investigação, portanto, são postos como prioridade diante de um amplo espectro de interesses, esse estudo ressalta a importância do mapeamento discursivo para a articulação e fortalecimento das agendas da sociedade civil em correlação com a comunidade científica. O desenvolvimento da rede, bem como de suas políticas, passa pela participação plural e fortalecimento das representações da população, dos usuários finais e daqueles

[21] Diferente do sentido ligado à Informática, Pierre Lévy (1999) define o virtual também em sua acepção filosófica. Aqui, o verbete se opõe ao *atual,* é aquilo que *não está presente* ou que existe apenas em potência.

setores para quem a criptografia assume função central de proteção. Reafirma-se, portanto, a importância de uma Governança da Internet (ou da Criptografia) verdadeiramente inclusiva.

Enquanto isso, novas fronteiras de possibilidades de vigilância se expandem e cada vez menos a metáfora do obscurecimento é cristalizada. A necessidade de desconstrução de metáforas "estabelecidas", portanto, carrega a função de propor uma nova leitura para uma nova realidade desafiadora e cujo resultado irá impactar de forma estrutural todo um ecossistema de comunicações, serviços e direitos baseados na Internet. Essas conexões, por fim, podem significar uma nova redistribuição de poder – e a criptografia desempenha papel central nessa missão.

8. Referência Bibliográfica

ABELSON et al. (2015). Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. Massachusetts Institute of Technology. Disponível em https://dspace.mit.edu/handle/1721.1/97690. Acesso em 19 de fevereiro de 2019.

ABREU, Jacqueline (2017). Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. Revista Brasileira de Políticas Públicas, Vol 7, nº 3.`

ABREU, Jacqueline; ANTONIALLI, Dennys (2017). Vigilância sobre as comunicações no Brasil: interceptações, quebra de sigilo, infiltrações e seus limites constitucionais. InternetLab. Disponível em http://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf. Acesso em 15 de dezembro de 2019.

Access Now et al (2018). Letter to Department of Jutice Inspector General Requesting Investigation into FBI's Device Miscalculation.. Disponível em https://www.hrw.org/news/2018/06/04/letter-department-justice-inspector-general-requesting-investigation-fbis-device. Acesso em 15 de dezembro de 2019.

Anistia Internacional (2016). Encryption: a Matter of Human Rights. Anistia Internacional. 2016. Disponível em: https://www.amnestyusa.org/reports/encryption-a-matter-of-human-rights/. Acesso em 15 de dezembro de 2019.

ANTONIALLI, Dennys (2019). Da 1ª instância ao STF: bloqueio e sanções do Marco Civil da Internet. InternetLab, 2019. Disponível em http://www.internetlab.org.br/pt/especial/da-1a-instancia-ao-stf-bloqueios-e-sancoes-do-marco-civil-da-internet/ . Acesso em 15 de dezembro de 2019.

ARAS, Vladimir (Ministério Público do Brasil) (2017). Audiência Pública sobre as Ação Direta de Inconstitucionalidade nº 5.527 e Ação de Descumprimento de Preceito Fundamental nº 403. Supremo Tribunal Federal. Brasília. Disponível em http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 15 de dezembro de 2019.

Australian Government (2018). Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018. Federal Register Legislation.` Disponível em https://www.legislation.gov.au/Details/C2018A00148. Acesso em 15 de dezembro de 2019.

BARR, William (2019a). Attorney General William P. Barr Delivers Keynote Address at the International Conference on Cyber Security. Department of Justice. New York, 2019. Disponível em https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-

international-conference-cyber. Acesso em 15 de dezembro de 2019.

BARR, William (2019b). Attorney General William P. Barr Delivers Remarks at the Lawful Access Summit. Department of Justice. Washington, 2019. Disponível em https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-lawful-access-summit. Acesso em 15 de dezembro de 2019.

BENDOR, Jathan; BENDOR, Roy (2016). Selling smartness: Corporate Narratives and the Smart Cities as a Sociotechnical Imaginary. Science, Technology, and Human Values.

BENNETT, Colin (2008). The Privacy Advocates: resisting the spread of surveillance. The MIT Press.

BENTHAM, Jeremy (2008). O Panóptico. Editora Autentica. Belo Horizonte.

BORGES, Laryssa (2016). STF anula grampo entre Lula e Dilma e envia para Sergio Moro investigações contra ex-presidente. Revista Veja, 2016. Disponível em https://veja.abril.com.br/politica/stf-anula-grampo-entre-lula-e-dilma-e-envia-para-sergio-moro-investigacoes-contra-ex-presidente/. Acesso em 15 de dezembro de 2019.

CAREY, Robert F.; BURKEL, Jacquelyn A (1999). Revisiting the Four Horsemen of the Infocalypse: representations of anonymity and the internet in Canadian newspapers. Disponível em https://www.firstmonday.org/ojs/index.php/fm/article/view/1999/1874;

CAVOUKIAN, Ann (2009). Privacy by Design: the 7 foundational principles. Information and Society Comissioner of Ontario. Disponível em https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em 15 de dezembro de 2019.

CAVELTY, Dunn (2013). From cyber-bombs to political fallout: threat representation with an impact in the cyber-security discourse. International Studies Review,.

Church Committee Reports (1975). Interim Report: Alleged Assassination Plots Involving Foreign Leaders. AARC – Assassination Archives and Research Center. 1975 Disponível em http://www.aarclibrary.org/publib/church/reports/ir/pdf/ChurchIR_0_Title.pdf . Acesso em 15 de dezembro de 2019.

COMEY, James (2014). Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? Brookings Institution. Disponível em https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course. Acesso em 15 de dezembro de 2019

COMEY, James (2015a). Addressing the Cyber Security Threat. Federal Beaureau of Investigation. International Conference on Cyber Security, Fordham University, 2015. Disponível em https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat. Acesso em 15 de dezembro de 2019.

COMEY, James (2015b). Confonting cyber threat. Federal Beaureau of Investigation. Sixth Annual Financial Crimes and Cyber Security Symposium, Federal Reserve Bank, 2015. Disponível em https://www.fbi.gov/news/speeches/confronting-the-cyber-threat. Acesso em 15 de dezembro de 2019.

COMEY, James (2015c). Standing Together Against Terrorism and Fear: Tossed by the Waves but Never Sunk. Federal Bureau of Investigation (2015). NYPD Shield Conference 2015. Disponível em

https://www.fbi.gov/news/speeches/standing-together-against-terrorism-and-fear-tossed-by-the-waves-but-never-sunk. Acesso em 15 de dezembro de 2019.

COMEY, James (2016a). Privacy, Public Safety, and Security: How We Can Confront the Cyber Threat Together. Federal Bureau of Investigation. International Conference on Cyber Engagement, Georgetown University, 2016. Disponível em https://www.fbi.gov/news/speeches/privacy-public-safety-and-security-how-we-can-confront-the-cyber-threat-together. Acesso em 15 de dezembro de 2019.

COMEY, James (2016b). Expectations of Privacy: Balancing Liberty, Security, and Public Safety. Federal Bureau of Investigation. Center for the Study of American Democracy Biennial Conference, Kenyon College, 2016. Disponível em https://www.fbi.gov/news/speeches/expectations-of-privacy-balancing-liberty-security-and-public-safety. Acesso em 15 de dezembro de 2019.

COMEY, James (2017). The FBI and Cyber Crime: New Perspectives, New Partnerships, and New Ways of Doing Business. Federal Bureau of Investigation. Intelligence and National Security Alliance (INSA) Leadership Dinner, 2017. Disponível em https://www.fbi.gov/news/speeches/the-fbi-and-cyber-crime-new-perspectives-new-partnerships-and-new-ways-of-doing-business-. Acesso em 15 de dezembro de 2019.

G7 France (2019). Combating the use of the Internet for terrorists and violent extremist purposes. G7 France, 2019. Disponível em http://www.g7.utoronto.ca/justice/2019-internet.pdf. Acesso em 15/12/2019

Conectas (2018). Cerca de 3 mil entidades repudiam bolsonaro por fala sobre o fim do ativismo no Brasil. Disponível em https://www.conectas.org/noticias/cerca-de-3-mil-entidades-repudiam-bolsonaro-por-fala-sobre-fim-do-ativismo-no-brasil. Acesso em 15 de dezembro de 2019.

COSTA, Gilberto (2018). Candidatos acionam justiça para retirar conteúdo negativo da Internet. Agência Brasil. Disponível em http://agenciabrasil.ebc.com.br/justica/noticia/2018-10/candidatos-acionam-justica-para-retirar-conteudo-negativo-da-internet. Acesso em 15 de dezembro de 2019.

DAM, Kenneth W.; LIN, Herbert S. (1996). Cryptography's Role in Securing the Information Society. National Academy Press.

DANBLON, Emmanuelle (2007). Crises in Rhetoric, Crises in Democracy. Questions de Communication nº 12. Press Universitaires de Lorraine.

DIFFIE, Whitfeld; HELMAN, Martin (1976). New directions on Cryptography. IEEE Transactions on Information Theory. Disponível em https://ee.stanford.edu/~hellman/publications/24.pdf. Acesso em 15 de dezembro de 2019.

DOCTOROW, Cory (2018). NERD HARDER! FBI Director reiterates faith-based belief in working crypto that he can break. Boing Boing, 2018. Disponível em https://boingboing.net/2018/01/12/imaginary-numbers.html. Acesso em 15 de dezembro de 2019.

DONNER, Frank (1981). The Age of Surveillance: The Aims and Methods of America's Political Intelligence System. Vintage Press 1981.

FARIVAR, Cyrus (2015). Even former heads of NSA, DHS think crypto backdoors are stupid. Ars Technica. Disponível em https://arstechnica.com/tech-policy/2015/07/even-former-heads-of-nsa-dhs-think-crypto-backdoors-are-stupid/. Acesso em 15 de dezembro de 2019.

Five Country Ministerial (2018). Statement of principles on access to evidence and encryption. Quintet meeting of Attorneys-General. Disponivel em https://www.ag.gov.au/About/CommitteesandCouncils/Documents/joint-statement-principles-access-evidence.pdf. Acesso em 15 de dezembro de 2019.

FELT, Ulrike; FOUCHÉ, Rayvon; MILLER, Clark A.; SMITH-DOERR, Laurel (2017). The Handbook of Science and Technology Studies. The MIT Press.

GILL, Lex (2018). Law, Metaphor, and the Encrypted Machine. Osgoode Hall Law Journal.

GRIERSON, Jamie (2017). Ex-MI5 chief warns against crackdown on encrypted messaging apps. The Guardian. Disponível em https://www.theguardian.com/technology/2017/aug/11/ex-mi5-chief-warns-against-crackdown-encrypted-messaging-apps. Acesso em 15 de dezembro de 2019.

GREENWALD, Glenn (2014). No Place to Hide. Edição: 1ª ed. New York: Metropolitan Books, 2014

GREENWALD, Glenn (2015). The Orwellian Re-Branding of "Mass Surveillance" as Merely "Bulk Collection". The Intercept, 3 de março de 2015 Disponível em: https://theintercept.com/2015/03/13/orwellian-re-branding-mass-surveillance-merely-bulk-collection/. Acesso em 15 de dezembro de 2019.

GREENWALD, Glenn; MACASKILL, Ewen (2013). NSA Prism Program taps in to user data of Apple, Google and others. The Guardian, 2013. Disponível em https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Acesso em 15 de dezembro de 2019.

HUGHES, Eric (1993). A Cypherpunk's Manifesto. Disponível em https://www.activism.net/cypherpunk/manifesto.html. Acesso em 15 de dezembro de 2019.

JASANOFF, Sheila (2015). Future Imperfect: Science, Technology, and the Imagination of Modernity. In Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power, University of Chicago Press.

JASANOFF, Sheila; KIM, Sang-Hyun (2009). Containing the Atom: Sociotechnical Imaginaries and Nucler Power in the United States and South Korea. Minerva, vol 47 nº 2. Springer Publishing 2009.

KAYE, David (2015). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Disponível em: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session32/Documents/A_HRC_32_38_EN.docx. Acesso em 15 de dezembro de 2019

KHAN, David (1996). The Codebreakers: the comprehensive history of secret communications from Ancient Times to the Internet. Scribner Book Company.

KHEL, Danielle; WILSON, Andi; BANKSTON, Kevin (2015). Doomed to Repeat History? Lessons from the Crypto Wars of the 1990. Open Technology Institute, New America Foundation.

KURBALIJA, Jovan (2016),. Uma Introdução à Governança da Internet. Edição: 6ª ed. São Paulo: Comitê Gestor da Internet.

LAKOFF, George; JOHSEN, Mark (2003). Metaphors we live by. The University of Chicago Press. Disnponível em http://shu.bg/tadmin/upload/storage/161.pdf . Acesso em 15 de dezembro de 2019.

LANDAU, Susan (2018). The Five Eyes Statement Encryption: things are seldom what they seem. Lawfare. Disponível em: https://www.lawfareblog.com/five-eyes-statement-encryption-things-are-seldom-what-they-seem. Acesso em 15 de dezembro de 2019.

LEAL, Felipe Alcântara de Barros (Polícia Federal do Brasil) (2017). Audiência Pública sobre as Ação Direta de Inconstitucionalidade nº 5.527 e Ação de Descumprimento de Preceito Fundamental nº 403. Supremo Tribunal Federal. Brasília. Disponível em http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInterneteBloqueioJudicialdoWhatsApp.pdf. Acesso em 15 de dezembro de 2019.

LÉVY, Pierre (1999). Cibercultura. São Paulo: Editora 34.

LEVY, Steven (1994). Battle of the Clipper Chip. The New York Times Magazine.

LEWIS, James A; ZHENG, Denise E.; CARTER, William A (2017). The Effect of Encryption on Lawful Acess to Communication and Data. CSIS – Center for Strategic and International Studies.

MCCONNELL, Mike; CHERTOFF, Michael; LYNN, William (2015). Why the fear over ubiquitous data encryption is overblown. Washington Post. Disponível em https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html. Acesso em 15 de dezembro de 2019.

MCNEIL, Mauree; ARRIBAS-AYLLON, Micheal; HARAN, Joan; MACKENZIE, Adrian (2017). Conceptualizing Imaginaries of Science and Technology. In The Handbook of Science and Technology Studies. Cambridge: MIT Press.

MAY, Timothy C. (1994). The Cyphermonicon. Disponível em http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ.

Ministério Público Federal e Conselho Nacional dos Procuradores-Gerais (2016). Nota técnica sobre o descumprimento da legislação brasileira que regulamenta o uso da internet. Ministério Público Federal. Disponível em http://www.mpf.mp.br/pgr/documentos/nota-tecnica-crimes-ciberneticos/. Acesso em 2015 de dezembro de 2019.

MOROZOV, Evgeny (2013). To save everything, click here: smart machines, dumb humans, and the myth of tecnological perfectionism. Perseus Books, Public Affairs.

MURPHY, Maria Helen (2019). Surveillance and the Law: Language, Power, and Privacy. Routledge, Taylor and Francis Group.

PADUAN, Roberta (2018). ‘Carlos Bolsonaro tentou montar uma Abin paralela’, diz Joice Hasselmann. Revista Veja. Disponível em https://veja.abril.com.br/politica/carlos-bolsonaro-tentou-montar-uma-abin-paralela-diz-joice-hasselmann/, Acesso em 15 de dezembro de 2019.

PFEFFERKORN, Riana (2017b). A Response to "Responsible Encryption". Center for Internet and Society – CIS. Stanford Law School. Disponível em http://cyberlaw.stanford.edu/blog/2017/10/response-%E2%80%9Cresponsible-encryption%E2%80%9D. Acesso em 15 de dezembro de 2019.

PFEFFERKORN, Riana (2017a). The Rheroric of Responsible Encryption. Just Security. Disponível em https://www.justsecurity.org/46102/rhetoric-responsible-encryption/. Acesso em 15 de dezembro

de 2019.

RAMIRO, André (2018). Aspectos de uma Governança da Criptografia. II Encontro da Rede de Pesquisa em Governança da Internet. Goiânia, 2018.

ROGAWAY, Phillip (2015). The Moral Character of Cryptographic Work. University of California. Disponível em http://web.cs.ucdavis.edu/~rogaway/papers/moral.pdf. Acesso em 15 de dezembro de 2019.

ROSEN, Jeffrey A. (2019). Deputy Attorney General Jeffrey A. Rosen Delivers Remarks at Justice Department's Lawful Access Summit. Department of Justice. Disponível em https://www.justice.gov/opa/speech/deputy-attorney-general-jeffrey-rosen-delivers-remarks-justice-departments-lawful-access. Acesso em 15 de dezembro de 2019.

ROSENSTEIN, Rod (2017). Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy. Department of Justice`. Disponível em https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-encryption-united-states-naval. Acesso em 15 de dezembro de 2019.

SETO, Guilherme (2018). Bolsonaro diz que pretende acabar com 'ativismo ambiental xiita' se for presidente. Folha de S. Paulo. Disponível em https://www1.folha.uol.com.br/poder/2018/10/bolsonaro-diz-que-pretende-acabar-com-ativismo-ambiental-xiita-se-for-presidente.shtml. Acesso em 15 de dezembro de 2019.

SCHNEIER, Bruce (1996). Applied Cryptography. 2ª Ed. John Wiley & Sons.

SCHNEIER, Bruce (2019). Attorney General William Barr on Encryption Policy. Schneier on Security,. Disponível em https://www.schneier.com/blog/archives/2019/07/attorney_genera_1.html. Acesso em 15 de dezembro de 2019.

SCHULTZE, Matthias (2017). Clipper Meets Apple vs. FBI—A Comparison of the Cryptography Discourses from 1993 and 2016. Media and Communication, Vol. 5.

SCHULZ, Wolfgang; HOBOKEN, Joris van (2016). Encryption and Human Rights. Paris: UNESCO - United Nations Educational, Scientific and Cultural Organization.

SOLOVE, Daniel (2011). Nothing to Hide: the false tradeoff between privacy and security. Yale University Press.

SWIRE, Peter; AHMAD, Kenesa (2011). "Going Dark" versus a "Golden Age of Surveillance. Center for Democracy and Technology. Disponível em https://fpf.org/wp-content/uploads/Going-Dark-Versus-a-Golden-Age-for-Surveillance-Peter-Swire-and-Kenesa-A.pdf . Acesso em 15 de dezembro de 2019.

THOMPSON, Mark (2016). From Trump to Brexit Rhetoric: how today's politicians have to gota away with words. The Guardian. Disponível em https://www.theguardian.com/books/2016/aug/27/from-trump-to-brexit-rhetoric-how-todays-politicians-have-got-away-with-words. Acesso em 15 de dezembro de 2019.

WATSON, Sara (2018). Data is the new "___". Dis Magazine. Disponível em http://dismagazine.com/blog/73298/sara-m-watson-metaphors-of-big-data/. Acesso em 15 de dezembro de 2019.

WILLIAMS, Michael (2003). Words, Images, Enemies: Securitization and International Politics. International Studies Quaterly.

WHITE, James Merricks (2016). Anticipatory logics of the smart city's global imaginary. Urban Geography, Vol. 37.

WRAY, Christopher (2018). Raising Our Game: Cyber Security in an Age of Digital Transformation. Federal Bureau of Investigation. Fordham University - FBI International Conference on Cyber Security, 2018. Disponível em https://www.fbi.gov/news/speeches/raising-our-game-cyber-security-in-an-age-of-digital-transformation. Acesso em 15 de dezembro de 2019.

WRAY, Christopher (2019). Finding a Way Forward on Lawful Access: Bringing Child Predators out of the Shadows. Federal Beureau of Investigation. Lawful Access Summit. Disponível em https://www.fbi.gov/news/speeches/finding-a-way-forward-on-lawful-access. Acesso em 15 de dezembro de 2019.

Xingu Vivo (2019). Funcionário de Belo Monte é flagrado espionando Xingu Vivo para informar ABIN. Disponível em http://www.xinguvivo.org.br/2013/02/25/funcionario-de-belo-monte-e-flagrado-espionando-reuniao-do-xingu-vivo-para-informar-bin/. Acesso em 15 de dezembro de 2019.

ZIMMERMAN, Phil (1999). Why I Wrote PGP. Disponível em: https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html. Acesso em 19 de fevereiro de 2019

ZITTRAIN, Johnatan et al (2016). Don't Panic: Making progress on the "Going Dark" debate. Berkman Klein Center, Harvard University. Disponível em https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf. Acesso em 15 de dezembro de 2019.

ZUBOFF, Shoshana (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.