Rio de Janeiro, 2018

Não Entre em Pânico:

Avançando no debate sobre “obscurecimento” (*Going Dark*)

DON'T PANIC:
Making Progress on the "Going Dark" Debate

ITS
Instituto
de Tecnologia
& Sociedade
do Rio

Berkman
The Berkman Center for Internet & Society
at Harvard University

Berkman Klein Center for
Internet & Society at
Harvard University

Não Entre em Pânico:

Avançando no debate sobre "obscurecimento" (*Going Dark*)

Tradução brasileira

Por Instituto de Tecnologia e Sociedade do Rio (ITS Rio)

Prefácio

Há pouco mais de um ano, com o apoio da William and Flora Hewlett Foundation, o Centro Berkman para Internet e Sociedade da Universidade Harvard convocou um grupo diversificado de especialistas em segurança e políticas públicas da área acadêmica, da sociedade civil e dos serviços de inteligência americanos para começar a enfrentar alguns dos problemas mais desafiadores e persistentes na vigilância e na segurança cibernética.

O grupo se reuniu com o entendimento de que não havia escassez de debates. Tínhamos como objetivo promover um diálogo franco, para além dos tópicos de sempre, entre pessoas que não costumam ter a chance de interagir e, com isso, contribuir de formas significativas e concretas para o discurso sobre essas questões.

Um debate público se deu em paralelo aos nossos encontros: as alegações e questionamentos sobre o fato de o governo estar se deparando com um cenário que está "ficando no escuro" como resultado de novas formas de criptografia introduzidas em serviços e produtos de amplo consumo pelas empresas que os oferecem. Buscamos condensar nossas conversas e algumas conclusões aqui. Os participantes do nosso grupo que assinam este relatório, listados na página seguinte, endossam "os pontos de vista e opiniões alcançados pelo grupo em geral, mas não necessariamente cada uma das conclusões e recomendações.

Os participantes que trabalham atualmente em regime integral para órgãos do governo estão impedidos de assinar o relatório, e nada pode ou deve ser inferido sobre suas perspectivas a partir dele. Apenas agradecemos suas contribuições para as discussões do grupo.

– Matt Olsen, Bruce Schneier e Jonathan Zittrain
Organizadores do projeto

Signatários

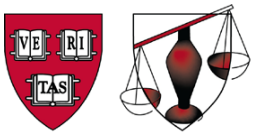
Urs Gasser
Nancy Gertner
Jack Goldsmith
Susan Landau
Joseph Nye
David R. O'Brien
Matthew G. Olsen
Daphna Renan
Julian Sanchez
Bruce Schneier
Larry Schwartztol
Jonathan Zittrain

Tradução

Gabriela Baptista

Revisor

Eduardo Magrani



Berkman
The Berkman Center for Internet & Society
at Harvard University

Não entre em pânico

Avançando no debate sobre "obscurecimento" (Going Dark)

1º de fevereiro de 2016

Introdução

No ano passado, as conversas sobre vigilância giraram em torno do uso de criptografia em tecnologias de comunicação. O debate foi impulsionado pelas decisões da Apple, do Google e de outros grandes fornecedores de serviços e produtos de comunicação em favor de habilitar a criptografia de ponta-a-ponta em certos aplicativos nos sistemas operacionais de smartphones, assim como a criptografia padrão em dispositivos móveis, enquanto grupos terroristas usam esse mesmo recurso para ocultar sua comunicação.

A inteligência e as forças policiais americanas veem essa tendência com diferentes graus de preocupação, alegando que suas capacidades de interceptação estão "ficando obscurecidas" (*going dark*). De acordo com seus relatos, as empresas cada vez mais adotam arquiteturas de informação que inibem a capacidade de o governo obter acesso a comunicações, mesmo em situações que se adequam às exigências da Quarta Emenda. A criptografia é a marca dessas arquiteturas. Agentes do governo demonstram preocupação, pois sem acesso às comunicações, temem perder a capacidade de evitar ataques terroristas e de investigar e processar atividades criminosas. Para eles, a solução é forçar as empresas a manter o acesso às comunicações e dados dos usuários e proporcionar esse acesso às forças policiais mediante solicitação, de acordo com o devido processo legal. No entanto, o setor privado tem resistido. Críticos temem que arquiteturas equipadas para esse acesso possam comprometer a segurança e a privacidade de usuários ao redor do mundo, ao mesmo tempo em que prejudicam a viabilidade econômica de empresas americanas. Discute-se também até que ponto as soluções propostas poderiam de fato evitar que terroristas e criminosos se comuniquem por meios resistentes à vigilância.

À frente de boa parte do debate, em nome do governo americano, está o Departamento de Justiça, que inclui a Agência Nacional de Investigação (o FBI, na sigla em inglês), cujos líderes têm comentado a questão em diversas declarações públicas, discursos e depoimentos no Congresso, ao longo de 2014 e 2015. Depois de quase um ano de discursos, em que foram feitas numerosas críticas à posição do governo por parte de ex-agentes da inteligência americana e

especialistas em tecnologia da segurança, a Casa Branca declarou em outubro de 2015 que não buscaria uma solução legislativa no futuro próximo.[1]

A decisão, porém, não encerrou o debate. Desde então, o FBI tem se concentrado em estimular empresas a buscar soluções para as necessidades de investigação de forma voluntária. Mais recentemente, os ataques terroristas em San Bernardino, Paris e outros lugares do mundo, somados a crescentes preocupações com o grupo terrorista Estado Islâmico (EI), têm chamado cada vez mais atenção para questões de vigilância e criptografia. Esses desenvolvimentos têm levado a renovados apelos, inclusive entre candidatos à presidência, para que o governo e o setor privado colaborem para enfrentar a questão de "obscurecimento" e para que o governo Obama reconsidere sua posição.

Conclusões

Apesar de não termos chegado a um consenso sobre o escopo do problema ou sobre a solução que poderia alcançar o melhor equilíbrio em termos de políticas, encaramos os alertas do FBI sem maiores questionamentos: as mudanças tecnológicas, em certa medida, têm dificultado certos tipos de vigilância. Ainda assim, nos perguntamos se a metáfora "obscurecimento" é adequada para descrever a situação atual. Estaríamos mesmo caminhando para um futuro no qual não seremos capazes de exercer uma vigilância efetiva sobre criminosos e pessoas perigosas? Não acreditamos nisso.

Com exceção de uma intervenção estatal na tecnologia que não parece ser contemplada por nenhum país além dos regimes mais despóticos, sempre existirão canais de comunicação que resistem à vigilância, principalmente devido à natureza gerativa da Internet atual, na qual novos serviços e aplicativos podem ser disponibilizados sem um processo de triagem centralizado. Entretanto, a questão que exploramos é o impacto dessa falta de acesso à comunicação sobre interesses legítimos do governo. Argumentamos que, no futuro, a comunicação não será eclipsada pela escuridão nem iluminada sem sombras. É provável que as forças do mercado e os interesses comerciais limitem as situações nas quais será oferecida criptografia que oculte os dados dos usuários da própria empresa, e a trajetória do desenvolvimento tecnológico aponta para um futuro com dados não encriptados abundantes, alguns dos quais podem preencher as lacunas deixadas pelos mesmos canais de comunicação que as forças policiais temem ficar "no escuro" ou fora de alcance.

Em resumo, chegamos às seguintes conclusões:

- Não é provável que a criptografia de ponta-a-ponta e outras arquiteturas de tecnologia voltadas para ocultar dados de usuários sejam adotadas de forma generalizada, pois a maioria das empresas que fornecem serviços de comunicação dependem do acesso a esses dados para fluxos de receitas e para garantir a funcionalidade de produtos, o que inclui a recuperação de dados, caso uma senha seja esquecida.
- Ecossistemas de software tendem a ser fragmentados. Para que a criptografia se tornasse amplamente disseminada, seria necessário muito mais coordenação e padronização do que temos atualmente.
- Estima-se que a presença de sensores em rede e da Internet das Coisas crescerá substancialmente, e isso tem o potencial de trazer mudanças drásticas para a vigilância. As imagens estáticas e em movimento e os áudios capturados por esses dispositivos podem permitir interceptações em tempo real e gravações para acesso posterior. Assim,

a incapacidade de monitorar um canal encriptado poderia ser mitigada pela capacidade de monitorar uma pessoa de longe, por meio de um outro canal.

- Metadados não são encriptados, e a grande maioria deve continuar assim. Tais dados precisam permanecer não encriptados para que os sistemas operem: dados de localização de celulares e outros aparelhos, registros de ligações telefônicas, informações de cabeçalho em e-mails, e assim por diante. Essa informação proporciona uma enorme quantidade de dados de vigilância que não estariam disponíveis se esses sistemas se disseminassem.
- Essas tendências suscitam novas questões sobre como a privacidade e a segurança dos indivíduos serão protegidas no futuro. O debate de hoje é importante, mas apesar dos esforços para levar em conta todas as tendências tecnológicas, está sendo desenvolvido em grande parte sem referência ao contexto geral.

Um catalisador: Apple, Google e outras empresas introduzem encriptação embutida (*Built-in Encryption*) e fácil de usar

Em setembro de 2014, cerca de um ano e meio depois das revelações de Edward Snowden, ex-colaborador da Agência de Segurança Nacional dos Estados Unidos (NSA, na sigla em inglês), a Apple anunciou a decisão de embutir a criptografia dos conteúdos protegidos por senha em seus aparelhos na então futura versão de seu sistema operacional móvel, o iOS 8.[2] Em verdade, os dados gerados por muitos dos aplicativos do sistema iOS 8 e versões posteriores são encriptados quando estão armazenados no próprio aparelho, em trânsito e nos servidores da Apple.[3] As chaves de desencriptação são atreladas à senha do aparelho e são armazenadas apenas nele.

Pouco depois do anúncio, o Google seguiu o exemplo ao divulgar que o Lollipop, a nova versão do sistema operacional Android, permitiria a criptografia padrão.[4] Depois, em novembro de 2014, o popular serviço de mensagens instantâneas WhatsApp, que agora pertence ao Facebook, anunciou que suportaria o protocolo de criptografia de ponta-a-ponta TextSecure.[5] Em março de 2015, o Yahoo introduziu o código-fonte para uma extensão que encripta mensagens no Yahoo Mail, embora exija que os usuários executem uma troca de chaves.[6] Esses passos trazem ao mundo dos aparelhos móveis um pouco das tecnologias que estão disponíveis há muito tempo – se não embutidas – em sistemas operacionais de computadores desktop, como o File Vault da Apple e o Bitlocker da Microsoft.

O que há de mais significativo desses anúncios é que a criptografia acontece por meio de chaves às quais apenas o usuário do respectivo aparelho tem acesso e é habilitada por padrão.

Embora o problema de obscurecimento englobe uma gama de mudanças de arquitetura que impedem o acesso do governo, a adoção de criptografia de dados em repouso e de ponta-a-ponta em alguns aplicativos comuns de comunicação tem se tornado um ponto central no debate atual, especialmente nos casos em que os prestadores de serviço não têm acesso às chaves. Por exemplo, o termo "criptografia de ponta-a-ponta" tem sido usado para descrever situações em que a informação está sendo encriptada nas duas pontas de um canal de comunicação, e apenas o emissário e o destinatário originais possuem as chaves necessárias para desencriptar a mensagem. Em outras palavras, a informação (em teoria e como é vendida pela publicidade) não pode ser lida por alguém que a veja atravessar uma rede entre o emissário e o destinatário, nem por um prestador de serviço intermediário, como a Apple. De forma semelhante, a criptografia

de *dispositivos* – em que as chaves só existem em aparelhos bloqueados – impede que os conteúdos sejam lidos por qualquer outra pessoa além daquelas que possuem as chaves.

A distinção é importante porque uma maioria esmagadora de usuários da Internet se comunica por meio de serviços *online*, como *webmail*, mensagens instantâneas e redes sociais, que não são encriptados de ponta-a-ponta. Ao longo de uma investigação, agentes do governo podem interceptar comunicações e buscar ter acesso a comunicações armazenadas por esses intermediários ao obter um mandado, uma ordem judicial ou uma intimação, desde que a empresa seja capaz de apresentar a informação desejada. No entanto, sem acesso às chaves, uma empresa como a Apple não é capaz de dar acesso a comunicações em trânsito ou armazenadas em seus serviços, mesmo que as forças policiais apresentem um mandado ou uma ordem judicial.[7]

As opções padrão e *native support* para encriptação também têm um papel importante. Assim como o Filevault e o Bitlocker protegem seus dados em repouso, os indivíduos têm tido a possibilidade de enviar e receber mensagens encriptadas há muito tempo. Por exemplo, o primeiro software de criptografia de chave pública, chamado *Pretty Good Privacy* (PGP), foi disponibilizado ao público no início dos anos 1990. No entanto, o usuário médio tem tido dificuldades em usar a criptografia em e-mails, especialmente quando a mesma não é embutida no software de comunicação.[8] O uso desses softwares requer uma curva de aprendizado bem documentada e acrescenta vários passos no envio de mensagens: tanto o emissário quanto o destinatário precisam entender o processo de criptografia, possuir o software, gerar o par de chaves, compartilhar as chaves públicas e encriptar e desencriptar as mensagens. Tudo isso traz uma complexidade e uma fricção que fazem muitos usuários desistirem.

A complexidade é reduzida de forma considerável quando a criptografia é embutida no software de comunicação. Quando está perfeitamente integrada, o usuário não precisa realizar nenhuma ação para encriptar ou desencriptar as mensagens, e boa parte do processo é realizado pelo software. Na verdade, um usuário médio pode não ser capaz de diferenciar mensagens encriptadas ou não. Quando essas opções são habilitadas por padrão em dispositivos e plataformas populares, como o iPhone, uma grande parcela das comunicações é encriptada.[9] Até agora, o governo não precisou se preocupar com o uso disseminado desse tipo de criptografia, mas o fato de esse esquema passar a ser padrão pode mudar a situação. Certamente, no passado havia menos dados para serem buscados pelas autoridades: o volume de comunicação digital na era da hegemonia dos computadores pessoais, de 1977 a 2007, mesmo com o surgimento da Internet, é ínfimo em comparação com as trocas facilitadas pelos dispositivos móveis.

Apesar de todo o alarde, poucas das ações midiáticas e preocupantes (pelos menos para o governo) dos fabricantes de sistemas operacionais em 2014 se materializaram em criptografia padrão fora do alcance de agentes do governo.[10] Além disso, como exploramos a seguir, por uma série de motivos, não está claro se a onda de criptografia introduzida nos últimos anos permanecerá.

Começa o debate sobre "obscurecimento" (Going Dark) (mais uma vez)

Este não é o primeiro debate sobre o público ter a capacidade de usar a criptografia e o governo ter acesso a comunicações. Em embates muitas vezes descritos como "criptoguerras", o acesso das autoridades a mensagens encriptadas tem sido objeto de discussões acalorados e políticas restritivas desde os anos 1970, tendo o governo afrouxado muitas restrições para o controle de exportações de software com algoritmos criptográficos fortes em 2000.[11] O papel e as obrigações

de empresas de telecomunicação em permitir que agentes do governo interceptem comunicações por voz – em especial, no antigo sistema telefônico que antecede a era dos PCs e da Internet – também têm sido amplamente debatidos ao longo das últimas décadas. Nos Estados Unidos, isso foi enquadrado pela Lei de Auxílio das Comunicações para a aplicação do Direito (CALEA, na sigla em inglês), que obrigava empresas de telefonia e outras instituições a garantir que suas redes pudessem ser interceptadas, mediante o devido processo legal, à medida que as tecnologias de rede passavam do sistema analógico para o digital.[12]

O FBI tem capitaneado a participação do governo no debate atual. Em 2010, a agência de investigação começou a demonstrar publicamente preocupação sobre sua capacidade de interceptar comunicações *online*.[13] Valerie Caproni, a então Diretora jurídica da instituição, em uma declaração diante da Comissão de Justiça do Senado dos EUA, usou a frase "*going dark*" para caracterizar tais preocupações, citando uma crescente discrepância entre o privilégio jurídico das forças policiais para interceptar comunicações eletrônicas e a capacidade de colocar essa interceptação em prática.[14] O depoimento enfatizou que muitos serviços de comunicação via Internet estão se tornando não apenas mais complexos, mas também são usados em modalidades que não estão sujeitas à CALEA.[15] Outros relatórios com declarações semelhantes surgiram durante aquele período, inclusive um relatório situacional do FBI sobre segurança cibernética que deixou de ser confidencial e descrevia como dados podem ser "ocultados" das forças policiais com o uso de criptografia e como os emissários e destinatários dos canais de comunicação podem ser escondidos por meio de um servidor *proxy*, como a rede Tor.[16]

Embora o FBI tenha sido a agência governamental que mais se manifestou sobre a questão,[17] agências de inteligência internacional, como a Agência Central de Inteligência (CIA, na sigla em inglês) e a NSA também enfrentam obstáculos decorrentes da criptografia e de outras arquiteturas que impedem seu acesso. O governo não é uma organização monolítica, e o debate sobre a criptografia não é visto da mesma forma pelas diferentes organizações governamentais, nem pelos indivíduos que fazem parte delas. As necessidades e recursos variam, assim como o âmbito jurisdicional. Por exemplo, os recursos do FBI para combater a criptografia podem ser menores do que aqueles da NSA. Da mesma forma, autoridades estaduais e locais têm acesso a menos recursos do que as forças policiais da esfera federal. No entanto, embora o grau de preocupação e o valor operacional atribuídos a essa questão possam não ser compartilhados pelas diferentes agências e instâncias governamentais, há um consenso geral entre agentes tanto das forças policiais quanto dos serviços de inteligência de que, caso todas as condições fossem as mesmas, seria uma vantagem se as arquiteturas tecnológicas não oferecessem barreiras para investigações. (Certamente, as condições não são as mesmas; por exemplo, se todas as comunicações fossem desencriptadas de forma rotineira, os cidadãos estariam expostos à vigilância de uma variedade de fontes, muitas das quais poderiam ser consideradas ameaças à segurança nacional pelos governos desses cidadãos.) Ao mesmo tempo, certas agências, entre elas o Departamento de Estado, o Laboratório de Pesquisa Naval dos Estados Unidos e a Agência de Projetos de Pesquisa Avançada de Defesa (DARPA, na sigla em inglês), têm apoiado o desenvolvimento da rede Tor, que oculta a informação transacional de comunicações via Internet. Tal apoio do governo é motivado por razões de segurança, além de interesses de direitos humanos.

Desde que Valerie Caproni invocou a metáfora "obscurecimento" em 2010, o problema continua a piorar, segundo agentes do governo. A criptografia se tornou uma preocupação central. James Comey, o Diretor do FBI, que talvez tenha sido a voz mais enfática sobre o assunto entre as autoridades ao longo do ano passado, deu destaque a essa apreensão em outubro de 2014, pouco depois dos anúncios da Apple e do Google:

> "Infelizmente, a lei não acompanhou o ritmo da tecnologia, e essa desconexão tem criado um significativo problema de segurança pública. Nós o chamamos de "obscurecimento" e o que significa é o seguinte: aqueles que têm a responsabilidade de proteger nosso povo nem sempre têm acesso às provas necessárias para processar crimes e prevenir o terrorismo. Temos autoridade legal para interceptar e acessar comunicações e informações de acordo com ordens judiciais, mas muitas vezes não temos a capacidade técnica para isso."[18]

Em outras declarações públicas e depoimentos no Congresso, o Diretor Comey e outros, inclusive a procuradora-geral adjunta Sally Yates, continuaram a chamar atenção para o problema. Segundo eles, o problema de obscurecimento está sendo impulsionado pelo "avanço das configurações de criptografia padrão e dos padrões de criptografia mais fortes, tanto em dispositivos quanto em redes,"[19] e pode ter uma série de implicações. Por exemplo, de acordo com agentes do FBI, "se não há meios de acessar dados (...) podemos não ser capazes de identificar aqueles que buscam roubar nossa tecnologia, nossos segredos de estado, nossas propriedades intelectuais e nossos segredos comerciais".[20]

Segundo agentes do governo, o uso de criptografia pode inibir a capacidade das forças policias e dos serviços de inteligência para investigar e impedir ataques terroristas. Mais especificamente, Comey afirmou que operadores do EI na Síria estão "recrutando dezenas de americanos problemáticos para matar pessoas, [usando] um processo que cada vez mais acontece por meio de aplicativos de mensagens para celular que contam com criptografia de ponta-a-ponta, comunicações que não podem ser interceptadas, apesar de ordens judiciais de acordo com a Quarta Emenda."[21] Agentes do FBI também enfatizaram que a agência não tem a capacidade de derrotar a criptografia com ataques de força bruta e que não há um jeito fácil de quebrar uma criptografia forte.[22] Recentemente, em depoimento para o Congresso, Comey identificou um ataque terrorista em Garland, no Texas, como um exemplo: "antes de sair e tentar cometer um assassinato em massa, um dos terroristas trocou 109 mensagens com terroristas no exterior", disse ele a uma comissão do senado. "Não temos a menor ideia do que ele disse, porque as mensagens estavam encriptadas."[23]

Outros membros das forças policiais e dos serviços de inteligência, incluindo o Diretor da NSA, o Almirante Michael Rogers, o Secretário de Segurança Nacional Jeh Johnson e a Procuradora Geral Loretta Lynch, também manifestaram preocupação com o problema de obscurecimento.[24] Após os ataques em Paris em 2015, atribuídos ao EI, mesmo na ausência de uma afirmação registrada de que os terroristas usaram a criptografia para proteger sua comunicação, o Diretor da CIA John Brennan sugeriu que o fato de os terroristas usarem tecnologia "tornava excepcionalmente difícil, tanto em termos técnicos quanto legais, obter os indícios que os serviços de inteligência e segurança precisam para encontrá-las."[25] Qualquer que seja a avaliação do uso de comunicação encriptada para frustrar investigações do governo, um grande número de ex-agentes das forças policiais e dos serviços de inteligência discordam sobre a necessidade de intervenção por meio de políticas.[26]

Apesar de boa parte do debate na imprensa ter sido voltada para questionar se o Diretor Comey estaria pedindo para que empresas como Google e Apple preservem o acesso a dados de usuários, não surgiu nenhuma proposta oficial por parte do FBI ou de outros membros das forças policiais e dos serviços de inteligência. Em julho de 2015, diante das comissões de justiça e de inteligência do senado, ele observou que "embora não tenha sido tomada uma decisão de pleitear legislação, precisamos trabalhar junto ao Congresso, a acadêmicos da indústria de

tecnologia, a grupos de proteção à privacidade, entre outros, para elaborar uma abordagem que trate de todas as variadas e legítimas preocupações concomitantes no centro de tantos debates nos últimos meses."[27] O Diretor também convocou o setor privado para ajudar a identificar soluções que proporcionem segurança ao público, sem frustrar esforços de vigilância das forças policiais. Mais recentemente, em outubro de 2015, ele confirmou em depoimento que o governo Obama, por enquanto, não buscaria uma solução legislativa, mas "continuaria as conversas com a indústria" para encontrar soluções voluntárias.[28]

Debates semelhantes acontecem em outros países.[29] No Reino Unido, o primeiro-ministro David Cameron propôs banir completamente tecnologias de criptografia de ponta-a-ponta após os ataques ao escritório da revista *Charlie Hebdo* em Paris, em 2015.[30] Os ataques mais recentes na cidade, em novembro, também levaram as autoridades francesas a questionar políticas em relação à disponibilidade de softwares de criptografia.[31] Outros países europeus aprovaram ou estão considerando aprovar leis exigindo que empresas retenham dados de usuários de forma legível e permitam o acesso das autoridades quando requisitado.[32] E Estados-nação que reconhecem menos barreiras constitucionais ou legais para demandas do governo por dados, como a Arábia Saudita, a Rússia e os Emirados Árabes, foram pioneiros em soluções legais preventivas para a retenção de dados e a desencriptação por parte de empresas de tecnologia.

Antes de nos aprofundarmos nas questões sobre a metáfora "obscurecimento", vale ressaltar brevemente algumas observações gerais.

O debate traz para o primeiro plano um número de tensões entre segurança, privacidade, competitividade econômica e acesso do governo à informação. Há uma vasta e rica literatura especializada que explora essas questões em detalhe.[33] Muitos dos aspectos tecnológicos e políticos do debate foram o foco do relatório *Keys Under Doormats* ("Chaves embaixo do tapete"), publicado recentemente e assinado por muitos daqueles que endossam este documento.[34] Embora essas perspectivas estejam fora de nosso escopo aqui, reconhecemos sua importância para a compreensão de muitas dimensões do debate sobre obscurecimento.

Vale enfatizar o cenário global no qual o debate está sendo desenvolvido. Muitos parceiros geopolíticos dos EUA estão engajados em discussões sobre a promoção da segurança cibernética e os limites adequados para a vigilância através de fronteiras. Por exemplo, o tratado de proteção de dados entre os EUA e a União Europeia conhecido como Safe Harbor, que proporcionou um enquadramento jurídico para fluxos comerciais de dados através de fronteiras desde a virada do século, foi recentemente decretado inválido pela Corte de Justiça da União Europeia, devido a preocupações sobre a capacidade dos serviços de inteligência americanos de acessar dados.[35] A ONU também deu uma limitada contribuição para o debate, ao declarar que a criptografia "é necessária para o exercício do direito à liberdade de expressão."[36]

Ao mesmo tempo, muitas empresas americanas também precisam responder aos governos de outros países onde operam. Nesse sentido, desempenham um papel quase soberano ao enfrentar decisões difíceis diante da pressão de órgãos governamentais estrangeiros para que apresentem dados sobre cidadãos no exterior. Muitas empresas se recusam a mudar a arquitetura de seus serviços para permitir tal vigilância. Entretanto, se o governo americano ordenasse mudanças em arquiteturas de informação, isso facilitaria a vigilância tanto para autoridades americanas quanto estrangeiras, até regimes autocráticos conhecidos por reprimir dissidentes políticos. As doutrinas jurídicas, os requisitos processuais e os mecanismos de reparação relativamente bem desenvolvidos, que servem para conter as atividades de vigilância do governo americano não são reproduzidas em todo o mundo.

Sobre a questão das ferramentas e técnicas de vigilância, muita coisa mudou ao longo dos últimos 20 anos. A revolução digital se mostrou vantajosa: tornou-se possível rastrear e obter informações sobre indivíduos de forma extremamente detalhada.[37] Embora a criptografia possa oferecer barreiras para a vigilância, talvez não seja impenetrável. Há muitas maneiras de implementar a criptografia de forma incorreta e outras fragilidades além dela podem ser exploradas.[38] Por exemplo, a técnica não impede invasões nas pontas das trocas de mensagens, o que tem sido cada vez mais usado pelas forças policiais.[39] Normalmente, a criptografia não protege metadados, como endereços de e-mail e informações de localização em dispositivos móveis, que precisam ser mantidas em texto simples, não formatado, para servir seus propósitos funcionais. Dados também podem ser vazados em meios não encriptados, através de *backups* na nuvem e sincronização em vários dispositivos.[40]

Obscurecimento é a metáfora errada

A metáfora "obscurecimento" sugere que as comunicações estão ficando fora de alcance de forma inexorável: uma abertura está se fechando e quando fechar, estaremos cegos. Essa imagem não retrata a situação atual e a trajetória do desenvolvimento tecnológico.

Certamente, serviços de criptografia e aqueles que ocultam o provedor dificultam a vigilância em alguns casos, mas o cenário é muito mais variado do que sugere a metáfora. Há, e sempre haverá, bolsões de penumbra e alguns pontos cegos – canais de comunicação que resistem à vigilância – , mas isso não significa que estamos ficando completamente "no escuro". Algumas áreas estão mais iluminadas agora do que no passado e outras estão ficando mais claras. Em particular, três tendências facilitam o acesso do governo. Primeiro, o modelo de negócios de muitas empresas depende do acesso a dados de usuários. Segundo, cada vez mais, produtos são oferecidos como serviços, e as arquiteturas se tornaram mais centralizadas por meio de computação em nuvem e centros de processamento de dados. Um serviço, que implica uma relação contínua entre fornecedores e usuários, se presta muito mais ao monitoramento e ao controle do que um produto, em que a tecnologia é comprada uma vez e usada sem outras interações com o fornecedor. Por fim, a Internet das Coisas promete abrir uma nova fronteira para conectar em rede objetos, máquinas e ambientes, de formas que ainda estamos começando a entender. Quando, digamos, uma televisão tem um microfone e uma conexão em rede e é reprogramável pelo vendedor, pode ser usada para ouvir um dos lados de uma conversa por telefone no mesmo cômodo, por mais encriptado que seja o serviço telefônico. Essas forças estão em trajetória rumo a um futuro com muito mais oportunidades para a vigilância.

Nesta seção, esperamos elucidar essa contranarrativa. Não estamos sugerindo que o problema identificado pelo FBI e outros estaria necessariamente resolvido com a disponibilidade de outras fontes de dados, nem que associamos essa disponibilidade à capacidade do governo de obter acesso. Acreditamos que as forças que estão abrindo novas oportunidades para a vigilância estatal significam que, qualquer que seja a situação da criptografia no iOS 8 em relação a seu antecessor, "obscurecimento" não descreve adequadamente o cenário a longo prazo. Qualquer debate sobre a capacidade de vigilância que possa resultar em políticas duradouras deve levar em conta essas tendências mais abrangentes.

A criptografia é contrária aos interesses comerciais de muitas empresas

Os atuais modelos de negócios desestimulam a implementação de criptografia de ponta-a-ponta e outros impedimentos técnicos ao acesso da empresa e, portanto, do governo.

Nos últimos 15 anos, empresas de Internet voltadas para o consumidor têm recorrido à publicidade como modelo de negócios dominante. É frequente o uso de anúncios para subsidiar conteúdos e serviços gratuitos. Mais recentemente, as empresas têm migrado para o marketing orientado por dados, e a tecnologia que permite veicular publicidade passou a depender muito mais de dados de usuários para direcionar anúncios com base em informações demográficas e comportamentos. As empresas buscam fazer avaliações de comportamento para associar anúncios a usuários ao longo do processo. Produtos do Google exibem anúncios determinados por padrões de comportamento, buscas e outras informações coletadas pela empresa.[41] De forma semelhante, o Facebook alega ser capaz de alcançar públicos específicos para campanhas publicitárias com "89% de precisão", com base em localização, dados demográficos, interesses e comportamentos.[42] Os produtos do Yahoo também são sustentados pela publicidade.[43] E a lista continua.

Para impulsionar esse lucrativo mercado, as empresas normalmente desejam ter livre acesso a dados de usuários, sendo a privacidade garantida ao se restringir a disseminação de informações identificáveis do cliente fora dos limites da empresa (com exceção das autoridades, caso solicitem os dados por vias legais). Implementar a criptografia de ponta-a-ponta como padrão para todos, ou mesmo para a maioria, dos fluxos de dados de usuários entraria em conflito com o modelo de publicidade e provavelmente reduziria as receitas. Até agora, as tendências do mercado refletem o fato de que as empresas têm poucos incentivos para desviar desse modelo, o que faz com seja improvável que criptografia se torne onipresente em aplicativos e serviços. Como resultado, muitas empresas de Internet continuarão a ter a capacidade de responder às ordens do governo para permitir o acesso às comunicações dos usuários.

A computação em nuvem faz com que o movimento de dados e software se encaminhe para locais centralizados e operados por empresas, e não para o armazenamento direto dos usuários. Essa tecnologia, possibilitada pela conectividade amplamente disponível, permite que empresas e indivíduos espalhem seus recursos computacionais pela Internet em centros de processamento de dados, como um serviço de utilidade pública.[44] Como resultado, produtos são cada vez mais oferecidos como serviços, o que, por sua vez, marca uma virada de noções mais tradicionais de propriedade e controle para repositórios centralizados de dados de usuários. Softwares e dados não precisam mais estar instalados e armazenados localmente nos computadores dos indivíduos – podem ser entregues por meio de um serviço de nuvem, como o Google Apps, ou armazenados remotamente em serviços como o Dropbox, onde podem ser acessados convenientemente de qualquer lugar por meio de um navegador ou aplicativo de smartphone.[45] *Webmail*, redes sociais, editores de texto e outros aplicativos comuns são agora oferecidos como serviços em rede.[46] Tais serviços proporcionam conveniência e vantagens significativas, tanto para indivíduos quanto para empresas, e muitas vezes são gratuitos, em modelos subsidiados por anúncios ou em esquemas pré-pagos.[47]

A criptografia de ponta-a-ponta, no momento atual, não é prática para empresas que precisam oferecer funcionalidades em serviços de nuvem que exigem acesso a dados em texto simples. Por exemplo, o Google oferece um número de funcionalidades em serviços *online*, incluindo pesquisas de texto completo em documentos e arquivos armazenados na nuvem, e para que funcionem, a empresa precisa ter acesso a dados em texto simples. Embora a Apple afirme encriptar comunicações de ponta-a-ponta em alguns dos aplicativos que desenvolve, não estende a criptografia para todos os serviços. Isso inclui principalmente o serviço de backup do iCloud,

que permite a usuários recuperar seus dados nos servidores da empresa. O iCloud é habilitado por padrão nos aparelhos da Apple. Apesar de encriptar os *backups*,[48] a empresa retém as chaves, para que usuários que perderam tudo não fiquem sem recursos. Então, embora os dados sejam protegidos de ataques externos, ainda podem ser desencriptados pela Apple.[49] Como a empresa retém as chaves, pode ser compelida a apresentar dados armazenados no iCloud mediante processo jurídico.

Há muitos outros motivos pelos quais uma virada em direção à criptografia e outras arquiteturas do tipo não interessam as empresas. Esquemas de criptografia muitas vezes tornam a experiência do usuário mais complexa. Joe Sullivan, ex-Diretor de segurança do Facebook, observou que a rede social "tem sido capaz de empregar a criptografia de ponta-aponta há muito tempo", mas adiou seu uso devido à complexidade adicional e porque "quando a criptografia de ponta-a-ponta é feita da forma correta, é difícil para uma pessoa comum se comunicar."[50] O Google também teria adiado a implementação de criptografia padrão em dispositivos Android bloqueados por questões de desempenho, apesar de ter anunciado que faria isso em 2014.[51] Até o presente momento, a versão mais recente do sistema operacional ainda não habilitou a criptografia padrão.

A fragmentação em ecossistemas de software também pode dificultar a disseminação de novas convenções e mudanças arquitetônicas, especialmente aquelas que permitiriam a criptografia de ponta-a-ponta em diferentes dispositivos e serviços. Nesses ecossistemas, podem existir múltiplos pontos de controle que influenciam os tipos de aplicativos e as atualizações de sistema operacional que acabam chegando aos usuários finais.

Por exemplo, no ecossistema Android, os smartphones são controlados por empresas de telecomunicação e fabricantes, que criam versões customizadas do sistema operacional para os aparelhos que vendem. Essas empresas têm poucos incentivos para atualizar aparelhos mais antigos com as versões mais recentes do Android, pois isso exigiria investimentos para tornar compatíveis as características customizadas.[52] De fato, muitos aparelhos Android mais antigos nunca são atualizados com versões mais recentes do sistema operacional. De acordo com o Google, no momento em que este texto foi escrito, cerca de 32% dos dispositivos Android usavam a versão mais recente do Lollipop, que foi lançado em novembro de 2014.[53] Além disso, embora a próxima versão a ser lançada possa conter aplicativos que suportem criptografia de ponta-a-ponta, um fabricante ou uma empresa de telecomunicação pode modificar o software para incluir seu próprio conjunto de aplicativos que não a suportam. Algumas dessas empresas podem ter interesse comerciais em manter o acesso a comunicações em texto simples.[54] O Google Play também disponibiliza uma ampla variedade de aplicativos de mensagens de terceiros, e os usuários finais podem instalar e usá-los no lugar de aplicativos pré-instalados em seus aparelhos. Para que a criptografia de ponta-a-ponta funcione adequadamente, precisa ser suportada tanto pelo aplicativo de mensagens do emissário quanto do destinatário, o que não é o caso de todos os aplicativos. Se o ecossistema for fragmentado, é muito menos provável que a criptografia se torne dominante.

A Internet das Coisas e os sensores em rede abrem caminhos para a vigilância nunca antes navegados

Atualmente, há um enorme número de sensores em rede embutidos em objetos cotidianos. São mecanismos muito propícios para a vigilância, vetores alternativos para coleta de informações que poderiam suprir em muito as lacunas deixadas pelas fontes que ficaram no escuro, tanto que suscitam questões preocupantes sobre como o público pode ficar vulnerável a ter suas

comunicações interceptadas. Traçar um quadro geral do que é obscurecimento com base no fato de que um grande número de aplicativos e produtos amplamente usados têm introduzido a criptografia padrão, pode ofuscar essa tendência mais ampla.

Segundo analistas e comentaristas que representam o senso comum, a Internet das Coisas será a próxima revolução na computação. Observadores especialistas têm sugerido que "a Internet das Coisas tem o potencial de trazer uma mudança fundamental na forma como interagimos com nossos ambientes", no trabalho, em casa, em espaços comerciais, em carros e nas vias públicas.[55] A previsão é que esse se tornará um mercado de trilhões de dólares nos próximos dez anos,[56] e de acordo com uma pesquisa entre especialistas, terá "efeitos benéficos e amplamente disseminados até 2025."[57] Isso trará mudanças significativas na forma como os membros da sociedade interagem uns com os outros e com os objetos inanimados ao seu redor.[58]

Utensílios e produtos, desde televisões e torradeiras até lençóis, lâmpadas, câmeras, escovas de dente, fechaduras, carros, relógios e outros dispositivos vestíveis estão sendo equipados com sensores e conectividade sem fio.[59] Muitas empresas estão desenvolvendo plataformas e produtos nessas áreas.[60] Para citar apenas algumas, Phillips, GE, Amazon, Apple, Google, Microsoft, Tesla, Samsung e Nike estão desenvolvendo produtos com essa funcionalidade, com sensores como giroscópios, acelerômetros, magnetômetros, sensores de proximidade, microfones, alto-falantes, barômetros, sensores infravermelhos, leitores de impressões digitais e antenas de radiofrequência, com o propósito de captar, coletar, armazenar e analisar informações minuciosas sobre seu entorno. Todos esses dispositivos estarão conectados uns aos outros via Internet, transmitindo dados de telemetria a seus respectivos vendedores para serem processados na nuvem.[61]

Os sensores de áudio e vídeo em produtos equipados com a Internet das Coisas abrirão muitas possibilidades para que agentes do governo exijam acesso a comunicações gravadas e em tempo real. Um caso que dura mais de dez anos envolvendo um sistema de assistente pessoal para carros pode ser uma indicação de como isso pode se desenrolar. O serviço permite que a empresa monitore remotamente e reaja aos ocupantes de um carro por meio de conexão via celular e uma variedade de sensores. Ao apertar um botão, o motorista pode falar com um representante que indica o caminho ou diagnostica problemas no carro, por exemplo. Durante uma investigação, o FBI tentou usar o microfone em um carro equipado com o sistema para capturar conversas entre dois supostos integrantes do alto escalão do crime organizado. Em 2001, um tribunal federal no estado de Nevada determinou, em decisão *ex parte,* que a empresa auxiliasse o FBI na interceptação. A empresa recorreu e, embora o Tribunal de Apelações do Nono Circuito tenha proibido a interceptação por outros motivos, deixou aberta a possibilidade de usar dispositivos de comunicação instalados em carros para vigilância, desde que as funcionalidades de segurança do sistema não fossem desabilitadas no processo.[62] Hoje, esse auxílio pode ser solicitado a qualquer empresa capaz de gravar conversas ou outras atividades à distância, seja por meio do smartphone da própria pessoa, um Amazon Echo, um monitor de bebê, uma câmera de segurança conectada à Internet, ou um boneco futurista equipado com sensores de imagem e áudio em rede.[63]

Em fevereiro de 2015, vieram à tona relatos de que as televisões inteligentes da Samsung estariam captando conversas por meio de um microfone embutido e as transmitindo para a empresa para discernir automaticamente se os usuários estariam tentando dar instruções ao aparelho.[64] Uma declaração publicada nas políticas de privacidade da empresa orientava os usuários a "estarem cientes de que informações pessoais ou delicadas incluídas em suas conversas faladas estariam

entre os dados capturados e transmitidos para terceiros por meio do uso de reconhecimento de voz."[65]

Todos os passos do processo da Samsung para oferecer as funcionalidades da televisão fazem sentido. O reconhecimento de voz é uma tarefa que exige muita capacidade computacional, e o processamento de dados de uma televisão moderna não seria suficiente para fazê-lo funcionar. Esse é um desafio comum para dispositivos equipados com Internet das Coisas que têm capacidade limitada de processamento e bateria. A solução, nesse caso, foi usar uma infraestrutura de nuvem por meio de uma conexão de rede para enviar os dados de voz a um servidor remoto para serem processados, interpretados e transmitidos de volta como comandos acionáveis pelo aparelho. Comandos simples, como "mudar para o canal 13", poderiam ser processados localmente, mas aqueles mais complexos, como "mostre um filme de ficção científica como o da semana passada, mas sem a Jane Fonda", precisariam ser enviados à infraestrutura de nuvem, e no caso da Samsung, a terceiros para processamento.

De forma semelhante, o navegador Chrome, do Google, suporta comandos de voz por meio do microfone embutido em um laptop ou desktop. A funcionalidade é ativada quando um usuário pronuncia a frase "OK Google", e o processamento de voz, que exige muitos recursos, acontece nos servidores remotos da empresa.[66] Até os brinquedos de criança estão começando a contar com essas funcionalidades. Em abril de 2015, a Mattel lançou a boneca interativa "Hello Barbie", capaz de manter diálogos, por meio da gravação das interações da criança com o brinquedo, que são processadas na nuvem, e do envio de respostas verbais a um alto-falante embutido.[67] A popularidade de câmeras de vídeo IP também tem crescido nos últimos anos. Dispositivos como a Nest Cam gravam vídeo em alta resolução com lente grande angular e o transmite ao proprietário.[68] Os usuários podem acessar a gravação pelo site da Nest ou por um aplicativo no celular, e a câmera envia alertas ao detectar movimentos ou barulhos atípicos. A Nest Cam também pode trocar dados e interagir com outros dispositivos, como os termostatos e detectores de fumaça da própria empresa, que também contam com sensores e microfones.

As forças policiais e os serviços de inteligência podem começar a buscar meios legais que obriguem a Samsung, o Google, a Mattel, a Nest ou fornecedores de outros dispositivos em rede a fazer uma atualização ou girar uma chave digital para interceptar as comunicações no ambiente de um alvo de investigação. Todos esses produtos são uma realidade agora. Se a Internet das Coisas tiver o impacto previsto, o futuro será cada vez mais repleto de sensores que podem ser requisitados pelas forças policiais, e esse é um mundo muito diferente daquele onde as oportunidades de vigilância ficariam obscurecidas. É vital reconhecer essas tendências e tomar decisões ponderadas sobre o quanto nossos ambientes construídos devem ser abertos à ampla vigilância, tanto de governos nacionais e internacionais quanto das empresas que oferecem os produtos que estão transformando nossos espaços pessoais.

Considerações finais

O debate sobre a criptografia suscita questões difíceis sobre segurança e privacidade. Do ponto de vista da segurança nacional, precisamos considerar se o acesso a comunicações encriptadas para ajudar a impedir o terrorismo e investigar crimes pode também aumentar nossa vulnerabilidade à espionagem cibernética e outras ameaças, e se as nações que não adotam o estado de direito poderiam tirar proveito desse mesmo acesso. Ao mesmo tempo, do ponto de vista das liberdades civis, precisamos considerar se impedir as autoridades de ter acesso a comunicações de acordo com as exigências previstas em lei e na Quarta Emenda atingiria o

equilíbrio certo entre privacidade e segurança, especialmente quando terroristas e criminosos usam a criptografia para escapar da vigilância do governo.

Ao examinar essas questões, nosso grupo se concentrou na trajetória da vigilância e da tecnologia. Concluímos que a metáfora "obscurecimento" não descreve plenamente a futura capacidade do governo de acessar as comunicações de suspeitos de terrorismo ou crime. A crescente disponibilidade de tecnologias de criptografia certamente impede a vigilância do governo em algumas circunstâncias, e nesse sentido, o governo está perdendo algumas oportunidades. No entanto, chegamos à conclusão de que a combinação de desenvolvimentos tecnológicos e forças de mercado provavelmente suprirá essas lacunas e, de forma mais ampla, garantirá novas possibilidades para que o governo colete informações críticas para a vigilância.

Pensando no futuro, a prevalência de sensores em rede e da Internet das Coisas traz novas e difíceis questões sobre privacidade a longo prazo. Isso significa que devemos pensar agora sobre as responsabilidades das empresas que desenvolvem novas tecnologias e em novas regras e procedimentos operacionais para ajudar as forças policiais e os serviços de inteligência a navegar o emaranhado de questões que certamente acompanharão essas tendências.

Notas

[1] Ver Ellen Nakashima e Andrea Peterson, "Obama administration opts not to force firms to decrypt data – for now", *The Washington Post*, 8 de outubro de 2015,

https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

[2] David Sanger, "Signaling Post-Snowden Era, New iPhone Locks Out NSA", *The New York Times*, 26 de setembro de 2014, http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html.

[3] Apple, Inc., "iOS Security Guide: iOS 8.1 or later", outubro de 2014.

[4] *Ibid.*

[5] Craig Timberg, "Newest Androids will join iPhones in offering default encryption, blocking police", *The Washington Post*, 18 de setembro de 2015, http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

[6] Andy Greenberg, "WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users", *WIRED*, 18 de novembro 2014, http://www.wired.com/2014/11/whatsapp-encrypted-messaging/.

[7] Alex Stamos, "User-Focused Security: End-to-End Encryption Extension for Yahoo Mail", *Yahoo Blog*, 15 de março de 2015, http://yahoo.tumblr.com/post/113708033335/user-focused-security-end-to-end-encryption.

[8] Charlie Savage, "U.S. Tries to Make It Easier to Wiretap the Internet", *The New York Times*, 27 de setembro de 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html.

[9] Ver registros relacionados à decisão In Re Order Requiring Apple, Inc. To Assist In The Execution Of A Search Warrant Issued By This Court, No. 15-MC-1902 (E.D.N.Y, 9 de outubro de 2015).

[10] Alma Whitten e J.D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0". In: Lori Cranor e Simpson Garfinkel. *Security and Usability: Designing Systems that People Can Use*. Sebastapol: O'Reilly, 2005.

[11] No começo de 2014, estimava-se que mais de 600 milhões de pessoas em todo o mundo usavam iPhone e mais de 1,9 bilhões usavam celulares com Android. Ver Dawiderpal Sahota, "Android Domination to continue in 2014; iPhone loses ground", *Telecoms.com*, janeiro de 2014, http://telecoms.com/210391/android-domination-to-continue-in-2014-iphone-loses-ground/.

[12] Ver, por exemplo, Nathan Freitas, "6 Ways Law Enforcement Can Track Terrorists in an Encrypted World", *MIT Technology Review*, 24 de novembro, 2015, http://www.technologyreview.com/view/543896/6-ways-law-enforcement-can-track-terrorists-in-an-encrypted-world/; Nicholas Weaver, "iPhones, The FBI, and Going Dark", *Lawfare*, 4 de agosto de 2015, https://www.lawfareblog.com/iphones-fbi-and-going-dark; Jan Willem Aldershoff, "Users shouldn't trust WhatsApp's end-to-end encryption", *MYCE.com*, 1 de maio de 2015, http://www.myce.com/news/users-shouldnt-trust-on-whatsapps-end-to-end-encryption-75939/.

[13] Para uma história completa, ver Whitfield Diffie e Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge: MIT Press, 2007.

[14] Ver Ben Adida, Collin Anderson, Annie Anton, et al., "CALEA II: Risks of Wiretap Modifications to Endpoints", 17 de maio de 2013.

[15] Charlie Savage, "U.S. Tries to Make It Easier to Wiretap the Internet", *The New York Times*, 27 de setembro de 2010, http://www.nytimes.com/2010/09/27/us/27wiretap.html.

[16] "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies," audiência perante a Subcomissão de Justiça para Crimes, Terrorismo e Segurança Nacional da Comissão de Justiça do Senado, Câmara dos Representantes dos Estados Unidos, 112º Congresso. (2011), http://judiciary.house.gov/_files/hearings/printers/112th/112-59_64581.PDF.

[17] Promulgada em 1994, a CALEA determinava que empresas de comunicação deveriam modificar sua infraestrutura digital para que as forças policiais pudessem conduzir atividades de vigilância dentro da lei. Pub. L. 103-414, 108 Stat. 4279 (5 de outubro de 1994) (codified at 47 USC §§ 1001-1010).

[18] Agência Nacional de Investigação, Relatório Situacional, Alerta sobre Atividades Cibernéticas, "Going Dark: Law Enforcement Problems in Lawful Surveillance", 29 de junho de 2011, http://info.publicintelligence.net/FBI-GoingDark.pdf.

[19] Órgãos governamentais estaduais e regionais também apresentaram relatórios e declarações sobre o debate. Ver, por exemplo, "Report of the Manhattan District Attorney's Office on Smartphone Encryption and Public Safety", novembro de 2015, http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

[20] James B. Comey, Diretor do FBI, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?", discurso na Brookings Institution, outubro de 2014, http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

[21] Amy Hess, Diretora-executiva assistente para ciência e tecnologia do FBI, "Encryption and Cyber Security for Mobile Electronic Communication Devices", Encryption Technology and Potential U.S. Policy Responses, Before the House Oversight and Government Reform Committee, Subcommittee on Information Technology, 29 de abril de 2015, http://www.fbi.gov/news/testimony/encryption-and-cyber-security-for-mobile-electronic-communication-devices.

[22] Amy Hess, Diretora-executiva assistente para ciência e tecnologia do FBI, "Encryption and Cyber Security for Mobile Electronic Communication Devices," Encryption Technology and Potential U.S. Policy Responses, Before the House Oversight and Government Reform Committee, Subcommittee on Information Technology, 29 de abril de 2015.

[23] James B. Comey, "Counter Intelligence and the Challenges of Going Dark", depoimento para a Seleto Comitê de Inteligência do Senado, 8 de julho , 2015, https://www.fbi.gov/news/testimony/counterterrorism-counterintelligence-and-the-challenges-of-going-dark; https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy; James Comey, "Encryption, Public Safety, and 'Going Dark'", *Lawfare*, 6 de julho 2015, https://www.lawfareblog.com/encryption-public-safety-and-going-dark. Ver também Michael Steinbach, "ISIL in America: Domestic Terror and Radicalization", Statement Before the House Judiciary Committee, Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, 26 de fevereiro de 2015, https://www.fbi.gov/news/testimony/isil-in-america-domestic-terror-and-radicalization.

[24] James B. Comey, Diretor do FBI, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?", discurso na Brookings Institution, outubro de 2014.

[25] James Comey, depoimento perante a Comissão de Justiça do Senado, "Oversight of the Federal Bureau of Investigation", 9 de dezembro de 2015.

[26] John Reed, "Transcript: NSA Director Mike Rogers vs Yahoo! on Encryption Backdoors", *Just Security*, 23 de fevereiro de 2015, http://justsecurity.org/20304/transcript-nsa-director-mike-rogers-vs-yahoo-encryption-doors/; Nick Gass, "Jeh Johnson warns of post-Snowden encryption frenzy", *Politico*, 15 de maio de 2015, http://www.politico.com/story/2015/05/jeh-johnson-edward-snowden-fallout-117986.html.

[27] Ver Damian Paletta, "Paris Attack Reopens U.S. Privacy vs Security Debate", *The Wall Street Journal*, 16 de novembro de 2015, http://blogs.wsj.com/washwire/2015/11/16/paris-attack-reopens-u-s-privacy-vs-security-debate/.

[28] Mike McConnell, Michael Chertoff e William Lynn, "Why the fear of ubiquitous data encryption is overblown", *The Washington Post*, 28 de julho de 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html.

[29] James B. Comey, "Going Dark: Encryption, Technology, and the Balances Between Public Safety and Encryption", depoimento em conjunto com a Procuradora-Geral Adjunta Sally Quillian Yates para a Comissão de Justiça do Senado, 8 de julho de 2015, https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy.

[30] Ellen Nakashima e Andrea Peterson, "Obama administration opts not to force firms to decrypt data – for now", *The Washington Post*, 8 de outubro de 2015, https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

[31] Cyrus Vance, Fraçois Molins, Adrian Leppard e Javier Zaragoza, "When Phone Encryption Blocks Justice", *The New York Times*, 11 de agosto de 2015, http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html.

[32] Ver Rowena Mason, "U.K. spy agencies need more powers, says Cameron", *The Guardian*, 12 de janeiro de 2015, http://www.theguardian.com/uk-news/2015/jan/12/uk-spy-agencies-need-more-powers-says-cameron-paris-attacks; Rob Price, "The U.K. government insists it's not going to try and ban encryption", *Business Insider*, 14 de julho de 2015, http://www.businessinsider.com/uk-government-not-going-to-ban-encryption-2015-7.

[33] Ver David Sanger e Nicole Perlroth, "Encrypted Messaging Apps May Face New Scrutiny Over Possible Role in Paris Attacks", *The New York Times*, 16 de novembro de 2015, http://www.nytimes.com/2015/11/17/world/europe/encrypted-messaging-apps-face-new-scrutiny-over-possible-role-in-paris-attacks.html.
[34] Hal Abelson et al., "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications", *Journal of Cybersecurity*, v.1 n.1, 2015.
[35] Maximillian Schrems v. Data Protection Commissioner, C-362/14 (CJEU 6 de outubro de 2015), http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.
[36] David Kaye, Conselho de Direitos Humanos das Nações Unidas, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", 22 de maio de 2015. Ver também David Kravets, "U.N. says encryption 'necessary for the exercise of the right to freedom'", *Ars Technica*, maio de 28 de 2015, http://arstechnica.com/tech-policy/2015/05/un-says-encryption-necessary-for-the-exercise-of-the-right-to-freedom/.
[37] Ver Peter Swire e Kenesa Ahmad, "'Going Dark' Versus a Golden Age of Surveillance", Center for Democracy & Technology, novembro de 28, 2011.
[38] Nathan Freitas, "6 Ways Law Enforcement Can Track Terrorists in an Encrypted World", *MIT Technology Review*, 24 de novembro de 2015, http://www.technologyreview.com/view/543896/6-ways-law-enforcement-can-track-terrorists-in-an-encrypted-world/; Nicholas Weaver, "iPhones, The FBI, and Going Dark", *Lawfare*, 4 de agosto de 2015, https://www.lawfareblog.com/iphones-fbi-and-going-dark.
[39] Ver Steven M. Bellovin, Matt Blaze, Sandy Clark e Susan Landau. "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet", *Northwestern Journal of Technology and Intellectual Property*, v. 12 n. 1, abril de 2014.
[40] Ver, por exemplo, Nathan Freitas, "6 Ways Law Enforcement Can Track Terrorists in an Encrypted World", *MIT Technology Review*, 24 de novembro de 2015, http://www.technologyreview.com/view/543896/6-ways-law-enforcement-can-track-terrorists-in-an-encrypted-world/; Nicholas Weaver, "iPhones, The FBI, and Going Dark", *Lawfare*, 4 de agosto de 2015, https://www.lawfareblog.com/iphones-fbi-and-going-dark.
[41] Ver, por exemplo, Google, "Showing Gmail ads", https://support.google.com/adwords/answer/6105478.
[42] Facebook, "How to target Facebook Ads", https://www.facebook.com/business/a/online-sales/ad-targeting-details.
[43] Yahoo, "Advertising", https://advertising.yahoo.com/.
[44] Michael Ambrust et al., "Above the Clouds: A Berkeley View of Cloud Computing", https://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf
[45] Ver, por exemplo, Dropbox, http://dropbox.com/.
[46] Ver, por exemplo, Janna Anderson e Lee Rainie, "The future of cloud computing," Pew Research Center, junho de 11, 2010, http://www.pewInternet.org/2010/06/11/the-future-of-cloud-computing/.
[47] Ver Quentin Hardy, "The Era of Cloud Computing", *The New York Times*, junho de 11 de 2014, http://bits.blogs.nytimes.com/2014/06/11/the-era-of-cloud-computing/.
[48] Apple, "iOS Security", setembro de 2015, https://www.apple.com/business/docs/iOS_Security_Guide.pdf
[49] Nicholas Weaver, "iPhones, the FBI, and Going Dark", *Lawfare*, 4 de agosto de 2015, https://www.lawfareblog.com/iphones-fbi-and-going-dark.
[50] Zach Miners, "End-to-end encryption needs to be easier for users before Facebook embraces it", *PC World*, março de 19 de 2014, http://www.pcworld.com/article/2109582/end-to-end-encryption-needs-to-be-easier-for-users-before-facebook-embraces-it.html.
[51] Andrew Cunningham, "Google quietly backs away from encrypting new Lollipop devices by default", *Ars Technica*, 2 de março de 2015, http://arstechnica.com/gadgets/2015/03/google-quietly-backs-away-from-encrypting-new-lollipop-devices-by-default/; Timothy J. Seppala, "Google won't force Android encryption by default", *Engadget*, 2 de março de 2015, http://www.engadget.com/2015/03/02/android-lollipop-automatic-encryption/.
[52] Alex Dobie, "Why you'll never have the latest version of Android", *Android Central*, 6 de setembro de 2012, http://www.androidcentral.com/why-you-ll-never-have-latest-version-android.
[53] Android Developer Dashboards, acesso em 27 de janeiro de 2016. http://developer.android.com/about/dashboards/index.html

[54] Ver, por exemplo, Anton Troianovski, "Phone Firms Sell Data on Customers", *The Wall Street Journal*, 21 de maio de 2013, http://www.wsj.com/articles/SB10001424127887323463704578497153556847658; Julianne Pepitone, "What your wireless carrier knows about you", *CNN Money*, 16 de dezembro de 2013, http://money.cnn.com/2013/12/16/technology/mobile/wireless-carrier-sell-data/; Declan McCullagh, "Verizon draws fire for monitoring app usage, browsing habits", *CNET*, 16 de outubro de 2012, http://www.cnet.com/news/verizon-draws-fire-for-monitoring-app-usage-browsing-habits/.
[55] McKinsey, "Unlocking the Potential of the Internet of things", junho de 2015. http://www.mckinsey.com/insights/business_technology/The_Internet_of_Things_The_value_of_digitizing_the_physical_world.
[56] Ver McKinsey, "Unlocking the Potential of the Internet of things", junho de 2015.
[57] Ver Janna Anderson e Lee Rainie, "The Internet of Things Will Thrive by 2025", Pew Research Center, março de 14, 2014, http://www.pewInternet.org/2014/05/14/Internet-of-things/.
[58] Ver Kelsey Finch e Omer Tene, "Welcome to the Metropicon: Protecting Privacy in a Hyperconnected Town", *Fordham Law Review*, v. 41 n. 1581, outubro de 2014.
[59] Ver, por exemplo, "Discover the Internet of things," http://iolist.co.
[60] Ver, por exemplo, https://aws.amazon.com/iot/; http://www.apple.com/ios/homekit/; https://developers.google.com/brillo/.
[61] Ver David Linthicum, "Thank the cloud for making big data and IoT possible", *InfoWorld*, 16 de janeiro de 2015, http://www.infoworld.com/article/2867978/cloud-computing/thank-the-cloud-for-making-big-data-and-Internet-of-things-possible.html.
[62] The Company v. United States, 349 F.3d 1132 (9th Cir. 2003). Ver também Adam Liptak, "Court Leaves the Door Open For Safety System Wiretaps", *The New York Times*, 21 de outubro de 2003, http://www.nytimes.com/2003/12/21/automobiles/court-leaves-the-door-open-for-safety-system-wiretaps.html; Jonathan Zittrain. "Tethered Appliances, Software as Service, and Perfect Enforcement". In: ____, *The Future of the Internet – And How to Stop It*. New Haven: Yale University Press, 2008. http://yupnet.org/zittrain/2008/03/14/chapter-5-tethered-appliances-software-as-service-and-perfect-enforcement/.
[63] Há um grande número de produtos de consumo – incluindo monitores de bebê, câmeras de segurança e até brinquedos de criança – com sensores em rede que transmitem telemetria e outros dados a intermediários para processamento e outros fins. Ver, por exemplo, "Amazon Echo," http://www.amazon.com/gp/product/B00X4WHP5E/; Nest, "Meet Nest Cam," https://nest.com/camera/meet-nest-cam/; Phillips, "In.Sight Wireless HD Baby Monitor," http://www.usa.philips.com/c-p/B120_37/in.sight-wireless-hd-baby-monitor.
[64] Ver Shane Harris, "Your Samsung SmartTV Is Spying on You, Basically", *The Daily Beast*, 5 de fevereiro de 2015, http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spying-on-you-basically.html.
[65] Samsung, "Samsung Privacy Policy – SmartTV Supplement," acesso em 26 de outubro de 2015 http://www.samsung.com/sg/info/privacy/smarttv.html (accessed Oc.
[66] Samuel Gibbs, "Google eavesdropping tool installed on computers without permission", *The Guardian*, junho de 23, 2015, http://www.theguardian.com/technology/2015/jun/23/google-eavesdropping-tool-installed-computers-without-permission.
[67] Ariella Brown, "Smart Barbie Puts Child's Play in the Cloud", *Information Week*, 5 de abril de 2015, http://www.informationweek.com/cloud/smart-barbie-puts-childs-play-in-the-cloud/a/d-id/1319779.
[68] Nest, "Meet Nest Cam," https://nest.com/camera/meet-nest-cam/.