DEMOCRACIA, DISPUTA DE NARRATIVAS E CONFLITOS DE SEGURANÇA NAS POLÍTICAS DE CRIPTOGRAFIA

ENTREVISTA COM RIANA PFEFFERKORN

INSTITUTO DE PESQUISA EM
DIREITO E TECNOLOGIA DO RECIFE - IP.REC

APRESENTAÇÃO

A presente entrevista foi realizada pelo Instituto de Pesquisa em Direito e Tecnologia do Recife – IP.rec, centro independente de pequisa e atuação política focado nos impactos sociais, éticos e jurídicos relativos ao desenvolvimento tecnológico.

O trabalho do Instituto teve início em 2017 e, desde então, sua equipe atua na elaboração de estudos científicos, análises de caso, campanhas, eventos e ações que contribuam para a construção de conhecimento e de senso crítico sobre o funcionamento das redes digitais.

A entrevista com Riana Pfefferkorn foi conduzida por André Ramiro, diretor do Instituto de Pesquisa em Direito e Tecnologia do Recife – IP.rec, entre os meses de junho e agosto de 2020.

Recife, outubro de 2020.

IP.rec
INSTITUTO DE PESQUISA EM
DIREITO & TECNOLOGIA DO RECIFE

RIANA PFEFFERKORN

Riana Pfefferkorn, atualmente, é uma das principais vozes na defesa da criptografia e na análise de políticas de vigilância que ponham em risco a segurança da rede e os direitos fundamentais. É Diretora Associada de Vigilância e Cibersegurança do Center for Internet and Society, da Universidade de Stanford, onde investiga políticas públicas e práticas do governo norte-americano que buscam decriptar dados e comunicações ou influenciar, por vias técnicas, legislativas ou judiciais, a arquitetura de plataformas e serviços no que se refere à criptografia.

Riana Pfefferkorn tem sido uma grande opositora das investidas anti-criptografia de setores do governo norte-americanas. Tem publicado análises, white papers, relatórios e participado de consultas e audiências públicas no âmbito de projetos de lei e casos judiciais em temas que vão desde propostas de backdoors, exploração de vulnerabilidades em aplicações e serviços tecnológicos por agências policiais e a busca de garantias por direitos fundamentais no âmbito de investigações criminais.

Os temas que orbitam as políticas de criptografia, abordados na entrevista, percorrem o papel central que a segurança tecnológica assume, atualmente, para a economia global e para a resiliência da rede. Também foram endereçadas questões sobre a abordagem legislativa de caráter policial quando o tema é política de tecnologia, bem como a centralidade de criptografia forte para o exercício de direitos políticos e fundamentalmente democráticos. E, com certeza, muito mais. Boa leitura.

ENTREVISTA

Pergunta: *Riana, muito obrigado por aceitar nosso convite. Sua visão sobre o tema é referência para tomadores de decisão, provedores de serviços e defensores da criptografia em uma variedade de regiões. Acreditamos que sua experiência é bastante valiosa para que a gente contextualize, a partir de uma perspectiva geopolítica, os debates que estão ocorrendo no Brasil e na América Latina, inclusive considerando as disputas de longa data em torno da criptografia nos Estados Unidos.*

Então comecemos com algumas questões básicas. A criptografia está na linha de frente da segurança da informação para comunicações eletrônicas há, pelo menos, meio século. Com a proliferação dos serviços de Internet e aplicações, em paralelo ao crescimento exponencial no número de usuários e dispositivos, a criptografia é, como nunca antes, uma pedra de toque para a segurança e confiança das redes. Ao mesmo tempo, a liberdade de expressão, assim como o exercício de um amplo espectro de direitos políticos e uma realidade conectada, depende consideravelmente da privacidade fornecida por protocolos de criptografia. Por isso, podemos assumir que a criptografia é diretamente relacionada com a democracia, atualmente. Mesmo assim, deparamo-nos com políticas públicas em alguns países que buscam enfraquecer a segurança da criptografia em nome de mais poderes investigativos e de vigilância. Certamente, há uma série de camadas nas ciências políticas em torno das políticas de criptografia, mas você acredita que essas políticas estão sendo propostas em razão de uma falta de conhecimento técnico ou há uma escolha consciente sobre segurança que está sendo feita por esses representantes do poder Estado? Como você vê esse cenário?

Riana Pfefferkorn: Obrigada por este excelente resumo da situação. Acredito que essas políticas têm várias motivações. Muitos agentes da aplicação da lei e legisladores provavelmente não têm conhecimento técnico para entender como a criptografia funciona ou os riscos de enfraquecê-la, como você sugere. Sempre que os legisladores voltam sua atenção para a tecnologia, a falta de conhecimento técnico pode ser um problema. No entanto, alguns legisladores têm assessores altamente versados e podem explicar a tecnologia e os riscos para eles. Da mesma forma, as agências de aplicação da lei também podem ter membros de sua equipe que são tecnicamente competentes e cujo trabalho é tentar desbloquear telefones, decriptar dados etc. Portanto, embora a falta de conhecimento técnico seja certamente um problema, não é a única explicação para por que os legisladores e membros da polícia continuam a fazer propostas de políticas para enfraquecer a criptografia.

Para aqueles que entendem as razões técnicas para não enfraquecer a criptografia, mas de toda forma fazem essas propostas, acredito que há várias motivações. Uma significa que eles compreendem os riscos de enfraquecer a criptografia, mas acreditam que, na balança, isso compensa. Eles sabem que enfraquecer a criptografia põe os dados de todo mundo em risco e que um “backdoor para os bons mocinhos” também será descoberto e explorado pelos “vilões”. Mesmo assim, quando pesam esses danos colaterais em contraposição com os benefícios esperados diante do enfraquecimento da criptografia, em termos de detectar e investigar atividades criminais e coletar evidências, eles decidem que estão de acordo com essa troca.

Agentes das forças de aplicação da lei, particularmente, também podem estar de acordo com essa troca por que sua função é combater o crime.

> *Legisladores têm que pensar de forma mais ampla: não apenas sobre crimes, mas sobre economia, sobre segurança nacional, sobre os direitos fundamentais das pessoas - tudo aquilo que a criptografia protege*

Mas, também, toda escolha política envolve trade-offs; alguns vão perder e alguns vão ganhar. O trabalho dos legisladores em construir políticas significa que eles estão sempre pensando em trade-offs e em chegar a difíceis decisões sobre elas. E, enquanto isso, eles estão sempre sob pressão para serem reeleitos, o que influencia o posicionamento deles nessas escolhas políticas. Se acreditam que têm uma melhor chance de serem reeleitos se são “duros contra o crime”, então poderão decidir que os prejuízos consequentes de enfraquecer a criptografia são aceitáveis, pois pensam que votar para enfraquecer a criptografia vão fazê-los parecer duros contra o crime (não importa se enfraquecer a criptografia vai gerar mais crimes, talvez mais do que preveniria ou resolveria).

Portanto, pode haver legisladores por aí que entendem os riscos e olhem para a criptografia como uma escolha de "segurança versus segurança": facilitando as investigações policiais por um lado e, por outro, fortalecendo as proteções para informações de segurança nacional, econômica e segurança dos indivíduos (por exemplo, para evitar que cônjuges abusivos acessem seus telefones), etc.

E, talvez, um lado desse “versus” seja simplesmente mais convincente. Os tipos de crimes de um dos lado podem parecer mais importantes do que os tipos de crimes do outro. Por exemplo, "não podemos entrar no telefone desta vítima de assassinato ou deste suspeito de terrorismo" parece absolutamente terrível, enquanto "a criptografia é necessária para proteger as informações bancárias das pessoas" pode, talvez, simplesmente não parecer tão importante quando comparado a um assassinato. Acho que quando a polícia pode contar histórias sobre crimes realmente terríveis que eles podem, de alguma forma, vincular a mensagens ou dispositivos criptografados, isso se torna muito persuasivo. Portanto, parte do que está acontecendo nessas escolhas políticas pode dizer respeito a formuladores de políticas entenderem as compensações de segurança, mas as agências de aplicação da lei contam histórias mais convincentes.

E, finalmente, acho que entre alguns policiais e também alguns legisladores, eles realmente não acreditam que as pessoas devam ter privacidade e realmente acreditam que a polícia deve ter uma quantidade muito maior de poder. Ainda esta semana *[entre 21 e 27 de junho de 2020]*, houve um novo Projeto de Lei apresentado no Senado dos EUA que basicamente tornaria ilegal a criptografia forte. Um dos seus patrocinadores, o senador Tom Cotton, publicou recentemente um artigo de opinião no New York Times, o principal jornal dos EUA, onde dizia que os militares deveriam ser enviados para reprimir os protestos que vêm acontecendo nos EUA há semanas contra a brutalidade policial e o racismo sistêmico.

Para ele, os manifestantes pacíficos merecem ser tratados como inimigos no campo de guerra! Não é nenhuma surpresa que alguém assim apoiaria uma política para tornar ilegal a criptografia forte. Para ele, os manifestantes e as pessoas que exercem seus direitos constitucionais são criminosos, e a polícia e os militares são os heróis.

> *Alguém assim, que favorece um Estado de polícia, não dá importância às desvantagens de segurança do enfraquecimento da criptografia. Ele se preocupa em impedir que os cidadãos tenham real privacidade e em dar mais poder à polícia*

P: *Quando você fala sobre as ações do senador - e eu gostaria de voltar, depois, para as interseções entre backdoors e desigualdades sociais - não posso deixar de notar outra semelhança de seus apontamentos com o contexto brasileiro em termos de agendas punitivistas dos dois países. Com a eleição de um presidente de extrema-direita em ambos os casos, essas vozes estão mais altas do que nunca e, portanto, o enquadramento criminal dos direitos políticos por esses atores se reflete em políticas de tecnologia. Por exemplo, nos últimos três anos, dois dos últimos ex-Ministros da Justiça, ambos ligados ao setor conservador e abertamente comprometidos com serem "duros com o crime" (um deles agora juiz do Supremo Tribunal Federal e outro ex-juiz), têm feito lobby por projetos de lei de backdoors junto ao parlamento. Seria possível traçar padrões entre as cruzadas por backdoors e uma tendência conservadora nas políticas públicas nos EUA (e no exterior)?*

Ou também aparecem a partir de perspectivas políticas mais progressistas?

É interessante quando você fala sobre legisladores voltando sua atenção para a tecnologia. Eu acrescentaria que, quando isso acontece, as políticas resultantes, incluindo propostas de backdoor, muitas vezes aparecem na pressa e no calor de sensibilidades sociais. Caso contrário, acredito, as pessoas provavelmente não aceitariam uma mais vigilância ao custo de romper os direitos constitucionais. Foi o que aconteceu, por exemplo, com o episódio de Suzano no Brasil (tiroteio em uma Escola, em 2019, que fez com que atenção fosse lançada à dark web). O caso aparecerá, por exemplo, como uma das motivações para um Projeto de Lei brasileiro que propõe a obrigatoriedade de monitoramento constante de conteúdo e comunicações por parte dos provedores de aplicação. Como os episódios de San Bernardino e Pensacola, por exemplo, foram usados como recursos narrativos para propostas de backdoor? Como as autoridades estão lidando com esses tipos de crimes em termos de pressionar o parlamento a interferir na criptografia?

RP: Acredito que o que o "conservadorismo" parece, agora, nos Estados Unidos é muito mais de extrema direita e extremista do que o que "conservadorismo" costumava significar, por exemplo, sob o presidente Ronald Reagan nos anos 1980. Alguns dos temas conservadores mais "clássicos" são (1) liberdade individual e (2) para que as empresas sejam livres da regulamentação governamental. Esses ideais parecem se traduzir enquanto suporte para criptografia forte, pois a criptografia forte ajuda a preservar as

liberdades individuais (privacidade, liberdade de expressão) e porque regulações sobre a criptografia restringiriam empresas, como o Facebook ou Signal, que a oferecem, e prejudicariam sua competitividade econômica no exterior. Esses valores conservadores mais tradicionais são o motivo de termos alguns membros republicanos no Senado dos EUA, como o senador Mike Lee, de Utah, que são pró-criptografia. Eles são raros, mas existem!

E, no entanto, há outro valor de conservadorismo, tanto na América quanto, eu suspeito, em outros lugares - que seria uma força policial forte, “a lei e a ordem", geralmente uma forma muito paternalista e, em última análise, pautada pela violência, de organizar a sociedade. Este slogan da "lei e a ordem" tem sido o tema do conservadorismo americano desde o presidente Richard Nixon, nos anos 70, e isso significa que os políticos de ambos os lados sentem que devem agir de forma "dura contra o crime". Portanto, esse tipo de conservadorismo - que valoriza a capacidade da polícia de se intrometer na vida das pessoas a fim de fazer cumprir as leis e manter a ordem pública - é o que vemos em jogo nas posturas anti-criptografia e pró-aplicação da lei.

Essa atitude é uma marca registrada do conservadorismo americano. Vemos isso no recém-proposto Projeto de Lei "Lawful Access to Encrypted Data Act", patrocinado por um grupo de senadores republicanos, sem co-patrocinadores democratas. Mas, a postura "lei e ordem", anti-criptografia e pró-backdoor também pode aparecer no que se passa por política "progressista" na América, o que significa nosso Partido Democrata.

Como disse, até mesmo muitos democratas têm, tradicionalmente, temido ser vistos como "brandos com o crime" - embora talvez isso esteja mudando em uma época de protestos em massa contra a brutalidade policial e demandas para acabar com a forma como atualmente fazemos o policiamento no Estados Unidos. Essa mudança é, em grande parte, impulsionada por pessoas mais jovens. Para acompanhar a opinião popular, o Partido Democrata pode precisar começar a agir a partir de posturas menos pró-polícia. Mesmo assim, o impopular "EARN IT Act" foi apresentado por um grupo bipartidário de senadores republicanos e democratas. No entanto, pelo menos um dos co-patrocinadores, o senador Blumenthal, costumava ser o procurador-geral de seu estado - portanto, não é uma surpresa que ele co-patrocinasse esse projeto.

No geral, a política norte-americana se inclinou para a direita nos últimos 40 anos. A agenda do Partido Republicano de 1980 soaria quase à esquerda para os padrões atuais. Portanto, no geral, parece muito "esquerdista" para um político se levantar e dizer: "Ei, a privacidade é um direito humano fundamental e isso significa que as comunicações privadas que não podem ser policiadas também são um direito fundamental." Tenho esperança de que o movimento juvenil de hoje, os protestos da polícia e o movimento Black Lives Matter possam ajudar a direcionar as políticas públicas mais para a esquerda nos EUA. As pessoas mais atingidas pela vigilância policial nos Estados Unidos são negras, marrons, pobres etc.

> *Eles entendem em primeira mão o quão violenta é a postura da "lei e da ordem" em sua implementação e eles entendem em primeira mão o valor das comunicações e dispositivos privados e seguros*

Se os formuladores de políticas os ouvirem e se precisarem responder às preocupações dessas comunidades para ganhar seus votos, talvez veremos uma pequena mudança nessa postura conservadora em relação à criptografia. Até agora, porém, é realmente difícil encontrar muitos políticos no Congresso dos Estados Unidos que defendam a criptografia.

2 - O Procurador-Geral/ (chefe do Departamento de Justiça) e o Diretor do FBI [Federal Bureau of Investigation] no momento do ataque de Pensacola não são os mesmos que o Procurador-Geral e o Diretor do FBI no momento do ataque de San Bernardino. Mas todos eles responderam da mesma maneira, ou seja, usar esses ataques como justificativas para argumentar em público a favor de backdoor nos dispositivos das pessoas. Mas os pedidos do procurador-geral e do diretor do FBI por backdoors após o ataque a Pensacola não tiveram tanta popularidade ou atenção da imprensa quanto o episódio de San Bernardino teve. Acho que é porque o FBI, de fato, levou a Apple à justiça na situação de San Bernardino, mas, pelo que sabemos, não fez o mesmo com o ataque de Pensacola. Em ambos os casos, terminou-se por conseguir crackear os telefones dos atiradores, o que enfraquece o argumento de que backdoors são necessários.

Mas, de toda forma, o fato das agências de aplicação da lei terem essas capacidades não impede o Procurador-Geral ou o Diretor do FBI de pedirem por backdoors.

Acho que foi uma surpresa para o Departamento de Justiça e para o FBI o fato de que o ataque terrorista de San Bernardino não tenha feito com que o público americano tomasse uma opinião uniforme e instantânea do lado da polícia e contra a Apple no que diz respeito aos iPhones encriptados. Houve previsões de altos membros do governo de que, se um ataque terrorista acontecesse, ele poderia ser atribuído à criptografia e, então, a postura do público se tornaria muito mais hostil à criptografia. Isso não necessariamente aconteceu com a opinião pública depois de San Bernardino. Infelizmente, eu diria que isso aconteceu até certo ponto com o Congresso. As agências de aplicação da lei têm a atenção de congressistas; as pessoas comuns, que se beneficiam da criptografia, não têm, então os congressistas só ouvem as pessoas comuns quando recebem muitos telefonemas ou e-mails sobre um determinado problema ou projeto de lei, ou quando pensam que precisam fazer o que as pessoas comuns desejam para obter seu voto, como eu disse antes. De qualquer forma, logo após o FBI conseguir abrir o iPhone do atirador de San Bernardino, em 2016, dois senadores, Dianne Feinstein (um democrata) e Richard Burr (um republicano) apresentaram um projeto de lei que penalizaria os fabricantes de smartphones que não incorporassem um backdoor para permitir o acesso das agências mediante ordem judicial. Esse projeto de lei não foi a lugar nenhum.

Mas acho que o ataque de San Bernardino e o ataque de Pensacola foram fatores motivadores para a atual legislação anti-criptografia que vemos pendente agora no Senado.

Dito isso, acho que o terrorismo de extremistas islâmicos não necessariamente assusta o público americano hoje como costumava, quase duas décadas após os ataques de 11 de setembro, enquanto nossa "Guerra ao Terror" se arrasta para sempre. Embora tenha havido episódios terroristas como San Bernardino, Pensacola etc,

> *muito do terrorismo que vimos nos últimos anos nos Estados Unidos foi cometido por supremacistas brancos nascidos no país. Acho que esse fato é muito constrangedor para o Procurador-Geral e o FBI, porque eles não podem usar a carta do nacionalismo, racismo, xenofobia, islamofobia como forma de convencer o público de que a criptografia é ruim*

porque os terroristas a usam. Portanto, não os ouvimos muito mais falar sobre terrorismo, exceto em casos como Pensacola.

Agora, desde meados de 2019, tudo se resume ao abuso sexual infantil online. Este tem sido um problema constante desde que a Internet existe; não há um "11 de setembro de abuso sexual infantil". Não é um incidente individual chocante como foram San Bernardino ou Pensacola.

Mas o terrorismo é raro, enquanto a imagética do abuso sexual infantil online é um problema contínuo. Isso é algo que as autoridades federais têm utilizado para fortalecer suas demandas por backdoors. Em vez de dizer "devemos criptografar a porta dos fundos por causa de um problema raro (ataques terroristas)", a polícia pode dizer "aqui está um problema contínuo". Além disso, o abuso infantil é algo que todo mundo despreza, não importa quais sejam suas tendências políticas. É uma questão bipartidária. Portanto, agora vemos a Procuradoria-Geral e o FBI se concentrando muito mais no abuso infantil ao invés do terrorismo como a razão para as propostas de backdoors. Honestamente, é uma surpresa para mim que tenham demorado tanto para usar o abuso infantil como justificativa. Eu me pergunto o porquê de não terem feito isso antes.

Dito isso, esqueci se mencionei antes, mas minha experiência de viajar para o Brasil e outros países e me envolver em debates sobre criptografia de outros países, é que sempre haverá algum tipo de crime que o governo usará para racionalizar sua demanda para backdoors.

> *Para o Brasil, tem sido a Lava Jato, corrupção e eleições. Aqui nos Estados Unidos, tem sido o terrorismo e o abuso infantil. O objetivo em todos os lugares é o mesmo: backdoors. É apenas o raciocínio que varia*

As pessoas que querem backdoors descobrirão qualquer motivo que chame a atenção da opinião pública - ou, mais importante, a opinião dos legisladores - para o seu lado, e é esse motivo que usarão. Depois que o terrorismo deixou de ter tanta influência sobre o público norte-americano, de repente era no abuso infantil que os defensores de backdoors estavam focando. Mesmo que a Lava Jato esteja sempre no background, algum acontecimento especial, como uma eleição, pode ser usado como uma ocasião para pedir backdoors no WhatsApp. São simplesmente variações da mesma melodia.

P: *É interessante porque quando o acesso a um aparelho é viabilizado por um serviço contratado, como os oferecidos pela Cellebrite ou Grayshift, parece-me que há um custo adicional, em termos de devido processo legal, para os órgãos de segurança pública e, talvez, eles perdem parte do potencial de escalabilidade (em outras palavras: poder de vigilância em massa) em comparação com a possibilidade de um uso sistêmico de backdoors. Mas, falando sobre o devido processo legal e legalidade do "cracking", o debate, em algum nível, está se movendo gradualmente em direção às práticas de hacking governamental? Como podemos analisar essas práticas em termos de políticas públicas e em relação à proteção dos direitos humanos, criptografia e, em última análise, aos riscos à segurança da informação como um todo?*

RP: Sim, concordo que o uso de dispositivos da Cellebrite/Grayshift - ao invés de backdoors - significa que a polícia está restrita a crackear telefones apenas em casos específicos. Poderíamos chamar isso de "vigilância sob medida" em vez de "vigilância em massa". E, quando falamos de dispositivos da Cellebrite e da Grayshift, estamos falando de equipamentos para invadir um determinado smartphone, o que exige que as autoridades tenham a posse do dispositivo. Mas o outro lado do hacking governamental é o hacking remoto - em que as autoridades (ou as empresas com as quais contratam) usam um exploit para obter acesso remoto ao alvo. O hack pode ser de um telefone, como quando o NSO Group (com contrato com vários governos ao redor do mundo) hackeava os telefones das pessoas, usando seu próprio software, o Pegasus, ou, em alguns casos, usando uma vulnerabilidade no WhatsApp. Ou pode ser de um navegador da web, como nos casos em que, para descobrir o verdadeiro endereço IP do usuário ou outras informações de identificação, a polícia dos Estados Unidos explorou uma falha no navegador Tor, invadindo os navegadores de milhares de pessoas por meio de um ataque "watering hole"[1] a visitantes de um servidor, do qual a polícia havia tomado poder, que administrava um “Tor Hidden Service” para imagens de abuso sexual infantil.

[1] Espécie de ataque em que um website é modificado, para para fins maliciosos, enquanto o atacante espera as vítimas entrarem e as infecta com um malware ou explora suas informações.

Portanto, parte do debate é sobre hacking governamental, que alguns especialistas e comentaristas consideram ser uma alternativa preferível aos backdoors mandatórios, porque sempre haverá falhas no software/hardware e porque o uso personalizado de tais falhas é menos prejudicial à privacidade, segurança e outros interesses além de um backdoor mandatório, o que, como você diz, abre a possibilidade de vigilância em massa sistêmica. E, no entanto, como já escrevi, o hacking governamental vem com seu próprio conjunto de riscos de segurança, sem mencionar o impacto sobre os direitos humanos quando os governos hackeiam seus próprios cidadãos, como revelou a saga do Grupo NSO.

> *Mas a prática de hacking do governo ultrapassou as restrições legais ao uso dessa ferramenta pela autoridades. A tecnologia se moveu mais rápido do que as políticas públicas, como costuma ser o caso quando falamos de novas tecnologias*

O Relator Especial da ONU para a Liberdade de Expressão David Kaye pediu uma moratória global sobre o uso de malware por governos, precisamente porque há um uso generalizado e sem muitas restrições legais - e muitas vezes em segredo, com governos negando qualquer envolvimento quando, digamos, as campanhas do Grupo NSO contra ativistas de direitos humanos, jornalistas ou dissidentes são descobertas. Nos EUA, temos o "Vulnerabilities Equities Process", que o governo federal usa para decidir se deve ou

não divulgar uma vulnerabilidade que tenha descoberto. Se divulgado, o fornecedor faria o reparo quanto à vulnerabilidade e o governo não poderia mais usá-la ofensivamente. Este é um processo útil de se ter em vigor e espero que outros governos adotem algo semelhante. Mas minha preocupação ainda é que esses processos não estejam levando em consideração todos os diferentes setores, especialmente os direitos humanos. Os governos tenderão a priorizar os direitos de seu próprio povo em detrimento dos de outros, além de priorizar a segurança nacional, e temo que os direitos humanos não sejam levados tão a sério como deveriam nessas discussões. Temos disponíveis frameworks internacionais de direitos humanos que os governos devem aplicar ao regulamentar o uso de práticas de hacking pelas autoridades policiais.

P: *Acredito que você levanta alguns fatos que envolvem, fundamentalmente, a geopolítica sobre a criptografia entre os Estados e o setor privado, bem como entre diferentes governos que estão relacionados a redes internacionais para fins de vigilância. Essas cooperações às vezes são mais sutis (mas muito eloqüentes), como declarações do G7, dos Five Eyes, ou mesmo entre os EUA e o Brasil (este último realizou um Simpósio "Going Dark" [sic] ano passado). Parece que, embora os Estados Unidos não tenham sucesso em aprovar uma legislação de backdoor, eles se envolvem e encorajam outros países a fazê-lo. Como você vê essas engrenagens de "soft power" em torno das políticas anti-criptografia, especialmente depois de cobrir durante anos a formulação de políticas nos Estados Unidos?*

RP: Não tenho conhecimento específico se os formuladores de políticas e autoridades policiais dos EUA realmente se reuniram com seus colegas de outros países e os encorajou ativamente a aprovar uma lei de backdoor. No entanto, não ficaria surpresa em saber que houve tal ação, já que, como você mencionou, vimos "declarações conjuntas" sobre criptografia às quais os Estados Unidos aderiram. Acho que o "soft power" dos Estados Unidos pode funcionar de várias maneiras. Uma dificuldade, aqui, é que o governo dos Estados Unidos não é uma entidade monolítica e diferentes partes dele têm opiniões muito diferentes sobre criptografia. Embora as agências federais de aplicação da lei dos EUA sejam anti-criptografia, as agências de inteligência são muito obstinadas contra backdoors porque vêem como os riscos superam os benefícios. Além disso, você deve se lembrar que o "Bureau de Direitos Humanos, Democracia e Trabalho", do Departamento de Estado dos EUA, ajudou a financiar o Tor. Historicamente, o Departamento de Estado dos EUA tem tentado ajudar a promover a democracia em todo o mundo como parte do exercício do “soft power” dos EUA, e você pode ver como o financiamento de tecnologias resistentes à censura contribui para isso.

Portanto, aqui temos várias partes do governo dos Estados Unidos cujos interesses não estão todos alinhados quando se trata de como exercer o “soft power” dos Estados Unidos na questão da criptografia. Mas essas partes não estão todas em pé de igualdade agora. Sob a administração atual, os Estados Unidos perderam muito de sua posição no mundo como um “farol da democracia”.

O Departamento de Estado foi praticamente desmontado, por isso exerce menos influência. Então resta as agências de inteligência e agências de aplicação da lei dos EUA, cujas abordagens quanto à criptografia estão em tensão. Compreensivelmente, as agências de inteligência geralmente não estão por aí dando entrevistas coletivas. Não sei como eles exercem o “soft power”, mas entre eles e os órgãos de segurança pública, é óbvio que os últimos são a voz mais chamativa, pelo menos no que diz respeito à criptografia.

Com a voz das agências de segurança pública dominando e o Departamento de Estado reduzido a um mero sussurro, os EUA não estão mais dando um bom exemplo de valores democráticos e abdicamos muito de nossa posição moral para contestar quando outros países aprovam leis - como as de backdoor - que sejam incompatíveis com as liberdades democráticas. A diminuição da influência dos EUA no exterior também significa que outros países podem ser os únicos a dar o exemplo para o mundo, seja esse exemplo bom ou ruim. Então,

> *quando a Austrália aprovou sua lei anti-criptografia em 2018 (modelando-a na "Snooper’s Charter”" de 2016, do Reino Unido), eles poderiam dizer "nós somos uma democracia, então esta é uma lei democrática." E agora, todos os outros países - sejam os EUA ou a China - podem apontar para a Austrália e dizer, "olhe, eles são uma democracia e aprovaram uma lei de backdoor, então isso deve significar que está tudo bem com as leis de backdoor"*

A abdicação total da liderança dos Estados Unidos no cenário global nos últimos 4 anos me parece ser um resultado negativo para o resto do mundo, mesmo que, nesta questão específica de criptografia, o DOJ esteja provavelmente contente com o resultado. Agora, parece mais normal e aceitável apresentar um projeto de lei de backdoor aqui: o Projeto de Lei “Lawful Access to Encrypted Data Act”, apresentado no Senado dos EUA em junho. O DOJ agora poderá dizer "é claro que está tudo bem com essa lei. É como as leis aprovadas por nossos aliados próximos, como a Austrália e o Reino Unido." No passado, você pensaria que seria constrangedor para o governo dos Estados Unidos (que, é claro, é muito presunçoso e egoísta) imitar o que outros países estão fazendo ao invés de ser o líder. Mas parece que é uma política dos Estados Unidos não ser mais um líder.

P: *Riana, por fim, gostaria de voltar ao valor social da criptografia para a democracia. Como você mencionou, as pessoas mais visadas pela vigilância policial são aquelas vítimas de desigualdades históricas e sistêmicas, como setores politicamente mal representados, como o movimento negro, minorias étnicas ou dissidentes políticos. Tem sido bastante documentada a cultura de escutas telefônicas ilegais e a criação de perfis de organizações e indivíduos, como jornalistas e ativistas, por governos em todo o mundo, mesmo aqueles considerados democráticos. É correto dizer, em sua opinião, que há interseções entre a lógica da vigilância em massa e a vontade de evitar qualquer mudança social substancial no status quo por meio da espionagem de movimentos sociais?*

Onde você acha que a criptografia se posiciona, historicamente, na luta pelos direitos humanos? E, por fim, você seria capaz de fazer alguma previsão para esse cenário em um futuro próximo?

RP: Acredito que a espionagem de movimentos sociais é uma tática que os governos, pelo menos nos EUA, vêm implantando há décadas como forma de monitorar o que consideram uma ameaça ao Estado. Em última análise, o estado existe não para proteger e servir a sua própria população, mas, em vez disso, para se proteger e perpetuar e estender seu próprio poder. Qualquer movimento popular por mudança social é, como você diz, uma ameaça ao status quo da existência do Estado, à forma que assume e ao escopo de seus poderes. Portanto, sim, acredito que a vigilância em massa ocorre, em parte, para que o Estado fique de olho nessas "ameaças" em potencial.

> *Acredito que isso seja parte do motivo pelo qual governos odeiam tanto a criptografia: porque ela dá mais poder à população e distancia o poder do Estado, além de tornar mais difícil, para o Estado, espionar a população*

Podemos ver mesmo agora, com os protestos populares nos Estados Unidos, que membros do governo - desde policiais até mesmo os presumíveis candidatos democratas à presidência - equiparam movimentos políticos (como o Black Lives Matter, o antifascismo e o anarquismo) à criminalidade e ao terrorismo.

Na opinião deles, não há diferença e, portanto, se backdoors são necessários para controlar criminosos e terroristas, faz sentido que o governo também queira backdoors para monitorar esses grupos políticos que representam uma ameaça para o status quo.

Por todas essas razões, acredito que a criptografia é uma ferramenta sem precedentes, na história moderna, no auxílio à luta pelos direitos humanos. Ao ameaçar a criptografia, governos estão ameaçando os direitos humanos. Tenho certeza de que eles estão bem cientes disso e, ainda assim, estão deliberadamente prosseguindo com suas agendas anti-criptografia. Precisamos de criptografia forte em conjunto com outras ferramentas que se mostraram altamente úteis: uma grande parte da população global agora tem uma câmera de vídeo no bolso e há uma grande quantidade de espaço de armazenamento na nuvem que pode ser acessada facilmente. O armazenamento deixou de ser caro, gravar vídeos e fotos deixou de ser difícil; todas essas ferramentas foram democratizadas. Isso ajuda a documentar e preservar evidências de violações dos direitos humanos. E a existência de plataformas de comunicação globais gratuitas também tornou mais fácil para que pessoas que lutam pelos direitos humanos entrem em contato, se organizem, compartilhem suas experiências e troquem dicas entre elas - ao passo que, anteriormente, ligações telefônicas, até mesmo para outras partes do país, eram dispendiosas, sobretudo para outro país, e o correio tradicional é muito lento.

Mas, é claro, muitas dessas ferramentas para proteger os direitos humanos - incluindo aplicativos de mensagem e dispositivos - existem porque as empresas do setor privado as fornecem. Dependemos dessas empresas para continuar a fornecer essas ferramentas, o que significa que somos vulneráveis à suas tomadas de decisões e políticas - seja em caso de criarem essas políticas por conta própria ou para cumprir as leis locais (como leis de backdoor). Mesmo quando pequenas organizações sem fins lucrativos criam e produzem ferramentas - lembre-se, o Signal é feito por uma organização sem fins lucrativos - ainda corremos o risco de perdê-las porque é muito fácil para as organizações sem fins lucrativos perderem financiamento, perder seu ímpeto e parar de apoiar as ferramentas que criaram. Vimos isso acontecer com ferramentas para documentar violações de direitos humanos. Isso também pode acontecer com ferramentas de criptografia.

No futuro, acredito que, ao redor do mundo, governos que são inimigos da criptografia forte farão avanços em termos de aprovação de leis para enfraquecer a criptografia, e prevejo que as empresas (principalmente americanas) que fornecem produtos e serviços fortemente criptografados se curvarão sob devido à pressão e cumprirão com essas leis. Isso não significa que a tecnologia vai desaparecer, mas será mais difícil de encontrá-las e as pessoas que precisam da proteção da criptografia terão que ser mais intencionais ao procurar e baixar essas ferramentas. Não será fácil, pois empresas como a Apple e o Google irão retirar os aplicativos de suas lojas, país por país, que não cumpram as leis aplicáveis.

E quem procura e faz o download dessas ferramentas, fora das lojas de aplicativos, corre maior risco de ser notado e visado pelo estado. Haverá riscos para você se não mais buscar e usar criptografia forte, assim como haverá riscos se ainda a usar.

Portanto, não acho que o futuro pareça particularmente promissor para a criptografia em termos de legislação e formulação de políticas globais. Mas

> *Eu acredito nas pessoas e no poder das pessoas. Encontraremos maneiras de nos proteger e a nossas comunidades, mesmo que os governos se tornem ainda mais hostis contra nós*

Enquanto isso, continuo fazendo o que posso para tentar proteger a criptografia de más leis e políticas.

IP.rec

INSTITUTO DE PESQUISA EM
DIREITO & TECNOLOGIA DO RECIFE

https://ip.rec.br

https://www.facebook.com/InstitutoIP.rec/

https://www.instagram.com/ip.rec

https://twitter.com/institutoiprec