ASPECTOS DE UMA GOVERNANÇA DA CRIPTOGRAFIA

André Ramiro[1]

RESUMO

Baseado em uma teorização sobre a governança da internet, explorando seu aspecto e abordagem multissetoriais, este trabalho propõe a observação das dimensões políticas da encriptação a partir de uma “governança da criptografia”, levando em consideração os direitos humanos, aspectos atinentes às empresas de tecnologia, demandas do Estado e, finalmente, as proporções sociais e éticas do desenvolvimento científico, em especial o criptográfico. Serão observados, igualmente, os efeitos colaterais das políticas de encriptação, os quais extrapolam o âmbito nacional de um dado Estado. Pretende-se ampliar o olhar sobre os atuais embates acerca da possibilidade de acesso excepcional ao conteúdo encriptado, à luz de uma possível ideia de “governança”. Para tanto, serão exploradas as relações entre a geopolítica internacional, as ameaças ao desenvolvimento tecnológico e a necessidade de preservação de direitos fundamentais. Assim, será possível abrir um mosaico interpretativo que pode servir de ferramenta à observação dos fatos políticos que dizem respeito ao desenvolvimento da criptografia.

PALAVRAS-CHAVE

governança; criptografia; multissetorialismo; ética; direitos humanos.

1 Mestrando em Ciências da Computação no CIn-UFPE. Bacharel em Direito na UFPE. Diretor do Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec. Email: andrebramiro@gmail.com; andreramiro@ip.rec.br

ABSTRACT

Based on theorization about internet governance, exploring its aspects and multistakeholder approach, this work proposes the observation of political dimensions of encryption found on a “cryptography governance”, taking into account human rights, aspects related to technology companies, government's requests and finally, the social and ethical proportions of scientific development, specially what concerns to cryptography. The side effects of the encryption policies, which extrapolates the national scope of a given country, will also be observed. This research intendeds to broaden the view on debates over the possibilities of exceptional access to encrypted content, in light of a possible ideia of “governance”. To achieve this, will be explored the relations between international geopolitics, threats to technological developments and the need to preserve fundamental rights. Thus, it will be possible to open an interpretative mosaic that can serve as a tool to observe the polical cases that are related to the development of cryptography.

KEY-WORDS

governance; cryptography, multistakeholderism; ethics; human rights.

INTRODUÇÃO

Enxergar a sustentabilidade do desenvolvimento de soluções tecnológicas, aplicações e dispositivos passa pela consideração dos métodos que garantem a segurança e a confiabilidade destes sistemas. Relações entre tecnologias e seus reflexos sociais se estreitam de forma que a implementação de novos serviços deste caráter passa, cada vez mais, por escrutínio público e críticas provenientes de diversos setores de interesse. Para além das dimensões técnicas, o status da encriptação das informações que trafegam pelas aplicações é um eixo crítico neste debate e carrega uma série de questões mercadológicas, sociais e, sobretudo, políticas.

A encriptação moderna vem acompanhando o desenvolvimento tecnológico, de forma a estar presente de maneira cada vez mais fundamental e robusta na construção de serviços de comunicação, comércio online, transações financeiras, dispositivos conectados e, finalmente, é vista como método garantidor e protetivo de posicionamentos políticos e das defesas da liberdade de expressão e da privacidade. Porém, como quaisquer outras soluções tecnologias disruptivas, a encriptação de mensagens também é utilizada com finalidades ilícitas, como ocultar informações e

conteúdos relativos ao planejamento de crimes ou tornar indisponíveis informações sequestradas através de *malwares*[2].

Esta última perspectiva serve de justificativa ao posicionamento de alguns dos mais importantes órgãos nacionais e internacionais de *law enforcement* para a construção de políticas públicas que procuram burlar o que se convencionou chamar de *encriptação forte,* ou seja, aquela que possui uma chave de encriptação considerada grande o suficiente para que seja difícil o acesso mesmo via ordem judicial. Além disso, ocorre que o atual estado da arte da encriptação permite que as comunicações sejam feitas sem que haja intermediários. Ou seja, dois pólos de uma conversa podem encriptar suas comunicações ponta-a-ponta sem que seja possível o acesso ao conteúdo por parte do intermediário que administra o serviço. Este acesso apenas é concedido ao emissor da informação e ao receptor.

Órgãos estatais de investigação sustentam que este cenário inviabiliza investigações, uma vez que impede que o conteúdo de mensagens seja acessado e, assim, desenvolvida uma busca por provas criminais. Nos últimos 30 anos, investidas sistemáticas para garantir o acesso a estas comunicações vêm sendo feitas, ora a nível tecnológico, ora a nível de políticas públicas. Na realidade, quaisquer das duas investidas abrange a outra, pois as relações entre políticas e tecnologias são, essencialmente, imbricadas.

Vale pontuar, ainda, que a criptografia, essencialmente, procura garantir a confidencialidade, a autenticidade e a integridade das comunicações. Porém, a nível de *disclaimer* deste trabalho, será aqui problematizado, sobretudo, aquilo que diz respeito à confidencialidade, justamente por esta ser a dimensão alvo de disputas políticas ao longo das últimas décadas.

GOVERNANÇA DA INTERNET: CONSTRUÇÃO POLÍTICA PLURAL E MULTISSETORIAL

2 O *ransomware,* por exemplo, é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, criptografando-os, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário.

Problematizar a possibilidade de acesso excepcional ao conteúdo encriptado não se resume a uma dualidade entre viabilidade técnica *versus* riscos à segurança das aplicações. Lançar uma visada a essa questão, partindo de uma abordagem multissetorial típica de um modelo de "governança da Internet" que vem ganhando força há cerca de quinze anos (KURBALIJA, 2016), não somente é saudável, mas também necessário para a formação de políticas públicas que levem em consideração um complexo que envolve infraestruturas físicas e lógicas, desenvolvimento econômico, demandas sociais, estratégias governamentais, entre outras variantes críticas à sustentabilidade de uma Internet descentralizada, plural e livre.

Se em uma floresta tropical coexistem inumeráveis plantas e animais, em uma alta biodiversidade que se mantém saudável devido à manutenção desta própria complexidade, a governança da internet possui incontáveis redes, serviços, aplicações, protocolos e usuários que devem cooperar entre si de forma coordenada e sustetável (KLEINWACHTER; ALMEIDA, 2015). Esse ecossistema – a partir de uma perspectiva político-legal – possibilita um processo dinâmico em que uma ampla variedade de regulações, co-regulações ou autorregulações coexistem e se complementam. Como resultado, é possível enxergar a possibilidade de uma rede que não possua uma autoridade única ou, não se identifique com uma política nacional específica.

Estabelecer um modelo de governança que acompanha o grau de complexidade de uma sociedade é natural, se o que se quer é alargar a participação dos setores de interesse e a formação de políticas que se sustentem por consenso comunitário. O modelo que ficou conhecido como "multissetorial" pode e deve ser aplicado na medida em que a quantidade de *players* - desde usuários finais a desenvolvedores e provedores de conexão e aplicação - também se expande e se diversifica. Quando tratamos do *status* da criptografia, seu grau de robustez, possibilidades de burlar a confidencialidade total das informações ou de fornecer acesso excepcional ao conteúdo aos órgãos policiais, essa perspectiva multissetorial também deve ser observada, dado o amplo impacto causado por comportamentos de um setor específico, como, por exemplo, do Estado. Como será descrito mais

adiante, ações independentes, sejam políticas públicas ou privadas, carregam o potencial de abalar outras políticas públicas e privadas nacionais e internacionais.

Como veremos, quatro são os principais setores que devem ser observados enquanto agentes participativos em uma governança da Internet e, consequentemente, da criptografia. São eles o governamental, o privado, o acadêmico/científico e a sociedade civil. Ainda que se considere, nos estudos mais recentes relativos à governança da internet, a participação mais capilarizada de outros setores de especial interesse, como os jovens, populações periféricas, mulheres, entres outros, consideraremos aqui estes quatro como pilares para o desenvolvimento de argumentações.

Segundo a Cúpula Mundial sobre a Sociedade da Informação – CMSI – a governança da internet diz respeito ao

> desenvolvimento e aplicação, pelos governos, pelo setor privado e pela sociedade civil, em seus respectivos papéis, de princípios, normas, regras, procedimentos de tomada de decisão e programas em comum que definem a evolução e o uso da Internet. (KURBALIJA, 2016)

O problema da regulação de questões críticas à rede é suficientemente complexo para que a abordagem seja estabelecida no centro dos diálogos diplomáticos. Questões relativas à cibersegurança, à neutralidade de rede, à proteção de dados pessoais, à inclusão digital ou, finalmente, à criptografia, são tocadas por uma transversal necessária que procura observar os potenciais impactos e efeitos colaterais que a formulação de políticas setoriais (sejam da sociedade civil, das empresas privadas ou do setor público) pode ocasionar em um ecossistema fundamentalmente abrangente e amplo como a Internet. Logo, capacitar um olhar horizontal que estabeleça mecanismos que considerem uma pluralidade de agentes de interesse na Internet se torna cada vez mais necessário. É o que uma abordagem multissetorial propõe.

A questão da regulação do ciberespaço ou de seus recursos essenciais não é uma inovação trazida e desenvolvida exclusivamente no âmbito da CMSI e ao longo dos Fóruns de Governança da Internet. A rede de inter-relações políticas e os meandros que devem ser encarados quando da construção de mecanismos de

controle sobre a Internet foram explorados de forma paradigmática pelo professor Lawrence Lessig (2006). Forças regulatórias jogam naturalmente de forma a refletir conflitos observados sobre outros problemas sociais em uma base diária.

Drogas, remédios, política de refugiados, direitos autorais ou a exploração de recursos naturais são questões que geram, por exemplo, conflitos quando são postos, frente a frente, posicionamentos de setores distintos. Empresas encaram de uma forma, governos de outra forma. A opinião da sociedade civil pode se distinguir dos interesses comerciais e assim por diante. As interfaces que podem ser traçadas exemplificam o complexidade que questões cotidianas podem carregar quando da criação de uma eventual política pública.

Com a Internet, então, não é diferente: essas inter-relações carregam níveis de disputa ainda mais profundos. Devido ao caráter pluri-participativo e descentralizado do ciberespaço, qualquer mudança no funcionamento de algum recurso crítico à rede gera um efeito em cadeia que pode descarrilar efeitos colaterais a todos os atores. A criptografia, mecanismo básico e fundamental à segurança das informações e comunicações, deve ser encarada como objeto de análise sob este prisma. Caso a balança de medição pese, desmedidamente, para um lado específico, este recurso assumirá uma faceta indesejada para os demais eixos e pode por em risco a confiabilidade da rede.

Digamos, para ilustrar, que os entes Estatais decidam pôr restrições à fabricação e implementação de soluções criptográficas. Ou seja, apenas as fabricações que carreguem a possibilidade de serem decriptadas pela agência de inteligência nacional possuam a permissão de serem desenvolvidas em dado país. Se, por um lado, a medida pode garantir acesso irrestrito às comunicações de um povo, por outro lado potencializaria as restrições à vida privada de uma sociedade, na medida em que nenhuma comunicação seria verdadeiramente confidencial. Enfraqueceria, ainda, a liberdade de expressão nessa localidade, uma vez que o receio pessoal diante da observação constante de uma entidade estatal termina por fragilizar a potência de um posicionamento político. Além disso, os serviços comercializados que necessitassem de criptografia robusta, como transações bancárias, compras online ou bancos de dados, com informações sensíveis, de uma

dada coletividade, perderiam sua confiabilidade, criando um colapso no número de usuários, o que impactaria o enriquecimento e a pluralidade de serviços via Internet.

Se partirmos dessa abordagem, assumimos que políticas públicas nacionais impactam, diretamente, o mercado nacional. Porém, os serviços de internet que requerem uso de criptografia forte não se restringem a um dado território. As maiores empresas de tecnologia do mundo possuem usuários dos cinco continentes e essa é a ambição da grande maioria das *start-ups.* Sendo assim, uma política nacional gera consequências para o mercado internacional de tecnologias. Se esse raciocínio for perseguido, pode-se assumir que uma empresa internacional, com a base do seu funcionamento na internet, carregará as restrições à fabricação e implementação de criptografia para todas as localidades em que funciona devido ao caráter transnacional da rede. Vendo o espraiamento da medida, um Estado internacional que sofreu essas consequências em seu território pode querer editar norma pelo uso protetivo e ilimitado da criptografia, a fim de gerar segurança à sua população (BUDISH; BURKERT; GASSER, 2018).

GOVERNOS: CRUZADA AO ACESSO EXCEPCIONAL

Recortar historicamente os momentos em que autoridades nacionais questionaram ou propuseram alternativas à encriptação das comunicações não se reduz ao momento presente, *pós-snowden*, quando as problematizações atinentes à vigilância ganham nova roupagem e impulsionamento, mas se dá em uma linha histórica de décadas. Aqui, estabeleceremos três janelas temporais modernas que poderão servir de cenário às disputas entre os setores envolvidos, a começar pelos posicionamentos governamentais.

Momento importante ao debate sobre limites à criptografia dizem respeito às

propostas da *National Security Agency* - NSA - para implementação de *chips* de encriptação nos aparelhos comercializados pelas empresas de telecomunicações nos Estados Unidos. Ocorre que o *Clipper Chip* (CLIPPER CHIP, 2019), como ficou conhecido, além de encriptar, também inseria *backdoor*[3] para acesso excepcional de autoridades policiais norte-americanas. O sistema, que ficou conhecido como *key escrow*, ou "custódia de chaves", sugeria que quando a autoridade policial acreditava serem os conteúdos das comunicações necessários a investigações, se dirigiam aos órgãos que possuíam a custódia das chaves e, assim, conseguiriam a decriptação daquela troca de mensagens e o acesso à comunicação de um dado usuário. À época, o acesso se dava por "autorização legal", termo vago que foi questionado, como veremos mais adiante, pelas entidades da sociedade civil.

A estratégia representava uma tentativa de proteger, o que será a tônica dos discursos governamentais nesta matéria, a segurança nacional, pois enxergavam paralelos entre uma "desordem informacional" e o desenvolvimento da criptografia (THE WHITE HOUSE, 1994). Supostamente, este cenário dava ensejo ao terrorismo, ao tráfico de drogas e a outras atividades criminais. Assim, sugeriam que a encriptação blindava as comunicações ilegais, impossibilitando investigações e a aplicação da lei criminal, bem como paralisava os esforços para proteger o bem público (LEVY, 1994). O governo norte-americano, então, protegeria a privacidade nas comunicações, via encriptação, exceto quando autoridades policiais requisitassem a exceção.

A impopularidade da medida gerou reações das organizações da sociedade civil, acadêmica (CRYPTO MUSEUM, 2019) e empresarial, restando barrada a iniciativa do *Clipper Chip* em 1996. Direitos fundamentais relativos à privacidade sobre as comunicações dos cidadãos deram importantes contornos para que houvesse o recuo do governo norte-americano. Porém, mais tarde, em 2001, o fato político necessário para impulsionar uma agenda de vigilância em massa veio à tona com o 11 de setembro, com isso, novas tentativas de dar limites à encriptação.

Após os atentados ao World Trade Center, em 2001, foi decretado o Patriot

3[ri] *Backdoor,* ou "porta dos fundos", é uma "falha" propositalmente adicionada a um sistema de segurança, como a criptografia, para que seja possível o acesso remoto a um sistema e ao conteúdo trafegado. Na maioria das vezes, não é documentado ao usuário.

Act pelo então presidente George Bush, com o propósito de alargar permissões investigativas e dar amplos poderes a órgãos de investigação com o emprego de ferramentas que tornaram possíveis programas de vigilância em massa, sobretudo nas comunicações eletrônicas. Como de praxe, ocasiões que tensionam a segurança pública nacional em larga escala “justificam” medidas governamentais energéticas que, em contrapartida, esvaziam, em grande escala, garantias às liberdades individuais em nome do combate a um “mal maior”, nesse caso, o terrorismo. O Patriot Act respaldou a execução de programas de vigilância promovidos pela NSA por meio da investida em infraestruturas físicas e por meio de acordos políticos de cooperação com empresas de telecomunicações e internet.

Ainda que o Patriot Act não atacasse os meios de encriptação especificamente, demandava que entidades privadas, corporações e indivíduos cedessem informações caso mandado judicial fosse expedido com essa finalidade. Percebe-se que, indiretamente, o decreto limitava a existência de encriptação ponta a ponta, uma vez que obrigava que provedores possuíssem meios de acesso às comunicações. O receio de responder judicialmente, devido à impossibilidade de entrega das informações, dá margem a inseguranças jurídicas, as quais reconfiguram o uso de encriptação ponta a ponta. O *trade off,* provocado via legislação, pode enfraquecer a privacidade e a segurança dos sistemas de informação.

Na esteira das políticas de vigilância empregadas pela NSA, o clímax é alcançado no que irá desaguar no, talvez, fato político mais notório do começo deste século no que diz respeito às pautas de privacidade e das liberdades fundamentais na Internet. Em 2013, Edward Snowden, ex-funcionário à serviço da NSA, veio a público denunciar detalhes de programas como o *PRISM* e o *Bullrun* – este específico para decriptar mensagens -, se tornando o *whistleblower* de maior projeção dos últimos tempos. Denunciou abusos vigilantistas, empregados de forma indiscriminada a toda a coletividade de norte-americanos e, muitas vezes, de cidadãos estrangeiros (GREENWALD, 2014). Autoridades políticas internacionais chegaram a ser alvos de vigilância, a exemplo da ex-presidenta Dilma Rousseff e da chanceler alemã Angela Merkel. Maiores consequências sobre o caso serão

exploradas ao longo deste trabalho.

SOCIEDADE CIVIL: REAÇÃO E MOBILIZAÇÃO

Abrindo um leque de perspectivas, as ações e posicionamentos políticos variam de acordo com a época e com o setor. Vamos explorar com mais detalhes cada um desses episódios a partir do ponto de vista dos setores não-governamentais, a fim de criar um mosaico interpretativo que pode servir de ferramenta de interpretação aos fatos políticos.

Movimentos e reações sociais aos momentos narrados foram fundamentais para o desenvolvimento de políticas sobre criptografia e para o amadurecimento sobre sua função pública. A década de 1990 foi simbólica nesse sentido, fazendo surgir uma rede de mobilizações civis que iria fazer o contraponto às movimentações governamentais.

No contexto do *Clipper Chip*, a tomada de consciência sobre as estratégias governamentais para o acesso às comunicações eletrônicas fez ganhar força a necessidade de criptografia para uso “popular”. O movimento *cypherpunk* surge, então, como forma de articulação social-ativista, com o mote da encriptação como forma de proteger direitos fundamentais. Para Eric Hughes (1993),

> Cipherpunks deploram regulações à criptografia, pois a encriptação é um ato fundamentalmente privado. O ato de encriptar, na realidade, retira informações do espaço público. Até mesmo leis contra a criptografia alcançam apenas uma dada fronteira nacional e a violência ali contida.

Interessante notar como a mobilização promove a conscientização sobre as repercussões do *chip* e chama atenção para a importância da confidencialidade nas comunicações e para o risco estrutural que potencialmente poderia ser causado por programas de vigilância em massa.

À possibilidade de haver uma “custódia das chaves” de decriptação em poder de autoridades governamentais, a Electronic Frointier Foundation – EFF – chamou de “renúncia das chaves”, o que ilustra uma inversão de perspectiva quando

observada sob a ótica do terceiro setor. As relações entre o direito à privacidade e a encriptação das comunicações formaram uma importante linha de atuação “ciberativista” na década de 1990, representada, entre outros, por John Gilmore, Eric Hughes e Timothy May (LEVY, 1993).

Ainda na década de 1990, emerge outra resposta a um “controle” da encriptação. Se não era possível confiar nas relações de serviços tecnológicos com o governo, novas aplicações foram fabricados para que a encriptação ganhasse maior aderência (ZIMMERMAN, 1999). Phil Zimmerman cria, ainda em 1991, o PGP - *Pretty Good Privacy*, programa de encriptação de e-mails e de arquivos armazenados em disco. A medida fortaleceu uma postura proativa, no âmbito particular, para que cada usuário, em seu computador pessoal, se empoderasse com tecnologias pró-privacidade.

À medida em que a agenda da privacidade vem ganhando força, a encriptação segue ganhando status de território de disputas políticas. Várias entidades representantes da sociedade civil organizada e de caráter social vêm vocalizando posicionamentos institucionais a respeito da possibilidade de haver acessos excepcionais ao conteúdo encriptado.

Mais recentemente, a disputa judicial envolvendo o *Federal Bureau of Investigation* – FBI – e a Apple mobilizou algumas entidades a emitirem estudos e relatórios a respeito do tema em uma tentativa de sensibilizar tomadores de decisão e mobilizar a sociedade civil. Em 2016, o FBI, por meio de ordem judicial, exigiu que a Apple desenvolvesse um sistema operacional específico para um aparelho, no qual recursos de segurança fossem enfraquecidos de modo a permitir a decriptação de inforamções. Este celular pertencia a um cidadão que supostamente esteve envolvido em ataques terroristas ocorridos na Califórnia, em 2015. A Apple, então, não possuía habilidades para quebrar a encriptação do aparelho, frustrando mandados judiciais para que houvesse o acesso. O caso ganhou notoriedade, reascendendo disputas entre as empresas que fazem uso de criptografia, os governos que demandam pelas informações protegidas e a sociedade civil.

Não por acaso, no mesmo ano, importantes relatórios e estudos fomentaram o

debate, lançando luz à criptografia em suas relações com os direitos humanos e os riscos trazidos pela possibilidade do acesso excepcional. O estudo *Encryption: a Matter of Human Rights* (ANISTIA INTERNACIONAL, 2016) explorou a formação de políticas que atentam contra a liberdade criptográfica. Ganha novos contornos a tese de que a proibição de certo uso de encriptação, seu desenvolvimento e a mera necessidade de licenças governamentais para uso privam os cidadãos do seu poder e autonomia para conferir segurança às suas comunicações, bem como impedem que indivíduos acessem livremente a própria Internet. A UNESCO se debruça sobre o tema na publicação *Encryption and Human Rights* (2016), chamando atenção para as relações entre as políticas de encriptação, a perspectiva plural da governança da Internet, as funções sociais, os valores humanos fundamentais e a ampla variedade de usos da rede. É possível encontrar a perspectiva multissetorial deste estudo, quando afirma que, da formulação de políticas dessa natureza,

> todos os setores devem estar envolvidos. A questão não se mostra relevante somente à indústria e aos governos, mas também deve incluir todos os membros da sociedade civil, representantes das comunidades mais vulneráveis, tais como as minorias, bem como as mídias e as instituições educacionais. (SCHULZ; HOBOKEN, 2016)

O Relator Especial da ONU para a Promoção e Proteção da Liberdade de Expressão e Opinião, David Kaye, em seu relatório anual, tematiza as tensões envolvendo a encriptação, o anonimato e os direitos humanos. Aqui, ganha força a afirmação de que a encriptação é ferramenta fundamental ao empoderamento da navegação, leitura, desenvolvimento e compartilhamento de informações e opiniões sem que haja interferência indesejada. A encriptação é vista, portanto, como necessária à categoria dos jornalistas, a membros de grupos étnicos e religiosos, àqueles perseguidos por orientações sexuais e políticas, artistas, ativistas, entre tantos outros, para que exercitem plenamente o direito à liberdade de expressão e opinião (KAYE, 2015).

É possível perceber que a leitura que parte das entidades de defesa da sociedade civil alcança um aspecto não assimilado pelas ordens judiciais e pelas formulações de políticas *top-down* de encriptação. Esse aspecto envolve a

consciência sobre o funcionamento de uma engrenagem social que se pauta pelo exercício de direitos políticos básicos do dia a dia. Entender a governança da criptografia também significa explorar as dualidades possíveis sobre um mesmo fato político e o impacto colateral que medidas setoriais solitárias podem causar. Contemplar a perspectiva civil e dos usuários finais da encriptação elucida uma possível base comum para o início da construção de medidas regulatórias.

SETOR PRIVADO: (IN)SEGURANÇA JURÍDICA E O MERCADO DE USUÁRIOS

Para os rumos dos debates sobre encriptação, a postura assumida pelas empresas é determinante. O grau de dedicação do setor privado quanto à privacidade dos usuários dá a tônica das disputas entre o acesso excepcional ao conteúdo encriptado e a proteção do sigilo das comunicações.

Talvez seja possível dizer que disputas ocorridas em torno de políticas de Internet, na maioria das vezes, se pautam em torno das tensões entre interesses dos Estados e das entidades representativas da sociedade civil. Porém as escolhas de cooperação, funcionamento e políticas privadas (a exemplo das políticas de privacidade) dos provedores de serviços moldam fortemente as espécies de regulação, economia e cultura do ecossistema online. Lawrence Lessig (2016) assume que o mercado é uma força reguladora determinante para o “aspecto” que o ciberespaço assume. Portanto, é necessário limitar seu poder de ditar regras (autorregular o ambiente em que se insere) e, ao mesmo tempo, inseri-lo nos diálogos públicos. A natureza regulatória dessas organizações lança efeitos colaterais que extrapolam um mercado nacional e influenciam realidades judiciais de outros países. Atualmente, isso se torna cada vez mais verdade quando é notável, por exemplo, o papel das companhias privadas no mercado global de dados pessoais e os contornos ultraliberais que esse mercado assume. Apenas recentemente regulações estatais vêm surgindo na tentativa de estabelecer molduras mais robustas e protetivas à proteção dos dados pessoais.

Para explorar esse aspecto, volte-se ao contexto do *Clipper Chip.* Apesar do

caráter governamental inicial do programa, a colaboração de entidades privadas foi fundamental para que fossem tiradas do papel as manobras que eram feitas no âmbito interno do governo. Inicialmente, o FBI, alerta à disseminação de celulares que fortaleciam o sigilo dos telefonemas através de encriptação, busca a assistência da NSA para compor uma solução alternativa que conseguisse burlar o avanço da proteção ao sigilo. Nesse momento, o *chip* surge como solução caso implementado com sucesso nos aparelhos. A AT&T*,* peça central na fabricação de telefones móveis com encriptação de voz (PEDNEKAR-MAGAL; SHIELDS, 2003) colabora com a proposta de inserção do chip em seus aparelhos. Dada a magnitude do mercado de telecomunicações à controle da AT&T, o apoio da empresa chancelou a política e deu margem para que o modelo de “custódia das chaves” se tornasse realidade.

A responsabilidade e a colaboração empresarial sobre uma realidade de vigilância é mais transparente em programas como o PRISM. Documentos revelados em uma série de furos de reportagem em 2013 (NSA, 2013) apontam para uma ampla variedade de empresas, como Google, Apple, Facebook, Verizon, Yahoo, Skype, e AOL, que concediam acesso direto às informações de seus usuários à NSA, em uma continuidade das medidas possibilitadas pelo *Patriot Act*, o que pode sugerir a existência de *backdoors* nos servidores destas organizações para uso exclusivo dos serviços de inteligência (não somente os norte-americanos).

Não é de se esperar que o discurso oficial de algumas dessas companhias corrobore as revelações - feitas com base em extensa documentação. Ainda em 2013, o discurso oficial da Apple testemunhava jamais ter ouvido falar do programa *PRISM* e que a empresa apenas cede informações a agências do governo mediante ordem judicial. Já o *Google* nega veementemente a existência de qualquer espécie de acesso direto, via *backdoor*, às informações de seus usuários.

Com o fortalecimento de organizações da sociedade civil, da agenda da privacidade, da proteção de dados pessoais e dos direitos digitais em geral, o discurso das companhias privadas passa a incorporar uma narrativa protetiva das liberdades fundamentais, com claro aceno ao seu mercado de “clientes”. O caso FBI *versus* Apple e, mais recentemente, o escândalo da *Cambridge Analytica* colocaram as empresas em uma berlinda que as leva a assumir essa postura perante a

sociedade. Companhias como o *Facebook* assinalam (HARD, 2018), por exemplo, que remover a encriptação ponta a ponta do *Whatsapp* compromete centenas de milhares de usuários que fazem uso da ferramenta com boa fé, além de que burlar a encriptação não impede criminosos de fazer uso de encriptação ponta a ponta em outros serviços. Então o giro cooperativo de ceder informações pessoais a entidades policiais de governos incorpora discursos libertários que ganharam força no ciberativismo.

Independente do veredicto sobre a existência de um acesso direto, a postura do setor privado intermedia os conflitos entre políticas governamentais e respostas provenientes da sociedade. O respeito a uma política de privacidade pró-usuário passa pelas relações intrínsecas entre empresas e governos, o que sugere serem as plataformas dos provedores de serviços campos de disputa de poder. Estes espaços também devem ser observados por uma ótica regulatória e multissetorial, sob risco de setores mais vulneráveis, como o social, serem comprometidos por acordos e cooperações que esvaziam direitos individuais e coletivos. A sabatina aos provedores de serviço contribui para uma cultura de segurança e confiança no uso da Internet. Como lidam com a privacidade e, consequentemente, com o uso de encriptação é, portanto, um fator chave para a governança da rede.

Disputas judiciais encaradas, recentemente, pelo *Whatsapp* no Brasil demonstram que o ecossistema da criptografia não somente não pertence a um Estado único, como também reverbera em outros setores. Um fato político localizado atinge o judiciário, gera reinterpretação de legislações, mobiliza a sociedade civil e impacta a experiência do usuário na Internet de modo geral. Tudo em âmbito potencialmente global.

Este cenário ilustra, de certa forma, o que a governança da criptografia deve observar. O caráter transnacional e multissetorial da Internet é elemento central a ser observado na elaboração de estratégias que impactam ferramentas críticas aos serviços que compõem a rede. Os efeitos colaterais e indesejados devem ser sopesados, seja diante de investidas privadas ou públicas.

SETOR ACADÊMICO/CIENTÍFICO: TÉCNICA E ÉTICA

O diagnóstico do “estado da arte criptográfica”, seu estudo, desenvolvimento e auditoria não são tarefas naturais dos setores acima escalados, mas de uma comunidade especializada, que se apresenta com viés técnico, mas sobre um palco fundamentalmente político. A dimensão acadêmico-científica da governança da criptografia está relacionada à análise das medidas que, eventualmente, propõem o acesso excepcional ao conteúdo encriptado.

Ainda no contexto do *Clipper Chip*, tornou-se referência, até os dias atuais, a contribuição da comunidade científica ao debate em torno da medida sugerida pela NSA. À época, o trabalho *The Risks of Key Recovery, Key Escrow and Trusted Third-Party Encryption* (ABELSON et al, 1997) reuniu a opinião de especialistas de referência em criptografia e cibersegurança, incluindo um dos criadores da criptografia de “chave pública”[4], Whitfield Diffie. Mais recentemente, por ocasião da disputa entre a Apple e o FBI, uma atualização deste estudo veio somar ao debate público, o *Keys Under Doormats - Mandating Insecurity by Requiring Government Access to All Data and Communications* (ABELSON et al, 2015) e se tornou pedra de toque quando se tratando das suspeições aos métodos de acesso excepcional ao conteúdo encriptado sugeridos por autoridades estatais investigativas.

Em ambos os estudos, algumas conclusões são apontadas pelo time de especialistas técnicos e contribuem para a rede de inter-relações setoriais aqui construída. A primeira delas diz respeito ao grau de confiabilidade que tais “recursos excepcionais” carregariam. Não há, segundo os autores, garantias de que uma brecha inserida aos mecanismos de encriptação restaria, efetivamente, em mãos unicamente do Estado. Estas vulnerabilidades carregariam o potencial de serem exploradas por indivíduos e outras nações com intenções maliciosas. Esta brecha pode se voltar justamente contra a coletividade, a mesma que as autoridades de investigação querem proteger ao interceptar ou monitorar comunicações privadas. Em segundo lugar, proporcional à complexidade de viabilizar mecanismos de custódia de chaves é a dificuldade de administrar as relações entre serviços, aplicações e autoridades investigativas ou policiais. Enormes custos, portanto, seriam gerados ao poder público. Além disso, especialistas em segurança da

4 Método que revolucionou a forma como duas partes encriptam mensagens. Desde então, as partes não necessitam mais combinar previamente uma chave de encriptação.

informação concordam que “a complexidade é inimiga da segurança” e cada novo recurso interage com os já existentes, criando possíveis novas vulnerabilidades que devem também ser cobertas por novos recursos. Quanto maior é a complexidade da Internet e de seus recursos de seguridade, mais arriscadas se tornam as propostas de acesso excepcional. Ato contínuo, é possível concluir, maiores sendo a complexidade e o risco de recursos alternativos de acesso excepcional a mensagens privadas, maior deve ser a amplitude de setores de interesse consultados em uma dinâmica que diz respeito à governança da criptografia.

Importante notar a manifestação, à época do *Clipper,* de pesquisadores e professores da área do direito, referências em regulação da Internet, o que trouxe uma dimensão sócio-jurídica à discussão. Em carta aberta ao congresso norte-americano, juristas problematizaram o sistema de custódia de chaves e declararam que o direito de se expressar livremente inclui não apenas falar *o que* se quer, mas também *como* se quer falar (LAW, 1997). Logo, um ordenamento jurídico não pode regular através de qual software deve ocorrer uma comunicação ou influenciar como desenvolvedores devem programar, uma vez que a programação também é uma linguagem comunicativa. Exigências desta natureza extrapolariam, então, os poderes delegados ao governo na Constituição, invadindo liberdades civis

Se, por um lado, a comunidade científica prefere a nomenclatura “criptografia forte”, por outro, agências de investigação chamam atenção para o que, supostamente, vem se tornando uma “encriptação à prova de mandados”[5] devido à impossibilidade de acesso ao conteúdo encriptado. Os rótulos, no entanto, se referem à mesma questão: há espaços na sociedade que estão além do acesso policial? Atualmente, as “*guerras criptográficas”*[6] vem ganhando novos ares, principalmente em torno da retórica do “ficar no escuro”[7], frequentemente mobilizada pelas autoridades policiais para falar das impossibilidades investigativas quando lidam com encriptação.

5 *Warrant-proof encryption*, no original.
6 *Crypto wars,* no original. Há quem aponte que as guerras criptográficas tenham início na Guerra Fria, mas o termo se popularizou no contexto do *Clipper Chip.* Basicamente diz respeito à série de conflitos travados entre alguns Estado, especialmente o norte-americano, e as comunidades que não aceitavam qualquer interferência do governo sobre a encriptação das comunicações.
7 *Going dark*, no original.

A tônica desta narrativa é lançar à encriptação a responsabilidade pelo eventual fracasso em evitar ou solucionar crimes como atentados terroristas, tráfico de drogas ou redes de pedofilia. Fortalecendo estas investidas, os *Five Eyes*, coalizão de cooperação formada por agências de inteligência dos Estados Unidos, Canadá, Reino Unido, Austrália e Nova Zelândia, frequentemente apoiam, de forma mútua, políticas "anti-criptografia". A lógica é: uma vez que uma política que enfraquece a criptografia é viabilizada em um dado país, outros ganham respaldo e apoio público para aprovar suas próprias regulações que limitam o sigilo nas comunicações.

Recentemente, a Austrália aprovou, em seu parlamento, questionável lei que obriga empresas de tecnologia a prestarem "assistência técnica" às forças policiais quando estas demandem por acesso às comunicações encriptadas dos usuários destas plataformas. Ocorre que a iniciativa carrega grande potencial de descarregar consequências não previstas, como por em xeque justamente a segurança nacional, como processos típicos de transações bancárias ou até mesmo o funcionamento de redes de energia nacional, em grande parte garantidas pela encriptação das informações que trafegam nestes sistemas (LIZZIE, 2018).

Legislações como a australiana ignoram que a "excepcionalidade" destes acessos carrega grande possibilidade de não ser explorada de forma localizada ou em relação a usuários específicos unicamente. Para Pferfferkorn (2018), medidas elaboradas para prover "acesso excepcional" possuem uma escalabilidade muito provável e supõem que tais soluções invariavelmente se tornam sistêmicas, uma vez que não há capacidade técnica para que seja criada uma solução para cada aparelho. Ou seja, uma vez que "assistências técnicas" sejam elaboradas com sucesso, um crescente número de dispositivos será alvo de pedidos excepcionais. Para suprir o volume de destas demandas, um método sistêmico deverá ser criado a fim de tornar eficiente e tempestiva a colaboração com as autoridades. Além disso, vários outros governos irão alimentar forte interesse nas soluções criadas para satisfazer o caso particular da Austrália. São reflexos da propagação que vulnerabilidades em sistemas criptográficos podem proporcionar.

A criptografia, enfim, pode reconfigurar arranjos de poder. Torna possível que

informações sejam disponíveis ou indisponíveis, dados sejam transparentes ou confidenciais, conteúdos sejam abertos ou protegidos a depender de quem os deseja acessar. Pode fortalecer potências dos cidadãos, na medida em que pode aproximá-los uns dos outros, ou aprofundar fraquezas, afastando-os de conhecimentos críticos.

Por ser uma ferramenta política, a criptografia possui uma dimensão moral, sustenta Phillip Rogaway (2015). O criptógrafo norte-americano aponta que, com as revelações de Edward Snowden, foi possível enxergar um fracasso no *trabalho criptográfico*, dado que as comunicações privadas da população passaram vulneráveis a interceptações ilegais. Isso ocorreu em função do trabalho e do desenvolvimento na área da criptografia terem sido moralmente neutros, distantes da dimensão ética ou fechada em “quebras-cabeças matemáticos”.

Em momentos de grande sensibilidade social coletiva, a exemplo das grandes guerras, o medo e o receio das catástrofes geram grandes esforços para que sejam desenvolvidas tecnologias que interrompam um fluxo desastroso na história. Em meados da década de 1940, na Segunda Guerra, as forças aliadas se dedicaram, não somente em termos militares, mas na área da ciência, para que fosse sustado o avanço nazista. O físico nuclear Robert Oppenheimer, famoso por ter desenvolvido as bombas atômicas que caíram sobre Hiroshima e Nagasaki, passa a liderar o Projeto Manhattan[8] movido pelo pelo temor do crescimento nazista. No pós-guerra, o mesmo Oppenheimer, diante do poder atômico e do terror que acompanhou a destruição de toda uma civilização por meio de suas criações, declara: “Eu me tornei a morte, o destruidor de universos” (ANDERSON, 2016). Sinalizava uma revisão moral do trabalho pelo qual foi mais notável e é frequentemente lembrado.

Semelhante sensibilidade coletiva, diante dos atentados de 11 de setembro de 2001, de alguma maneira pode ter justificado esforços no campo da interceptação em massa das comunicações, fortalecendo uma realidade de monitoramento e controle, talvez ainda não completamente dimensionada no que se

8 Projeto de pesquisa e desenvolvimento que produziu as primeiras bombas atômicas durante a Segunda Guerra Mundial

refere à violação aos direitos fundamentais, às liberdades individuais e, consequentemente, à construção das personalidades e das sociedades. É possível traçar um paralelo entre esforços tecnológicos para a fabricação de armas nucleares e os esforços para a construção de uma arquitetura de vigilância em massa. Como assinala Rogaway,

> Com algumas exceções, os cientistas atômicos que trabalharam no desarmamento não foram os mesmos indivíduos que construíram a bomba. Seus colegas - companheiros físicos - o fizeram. Criptógrafos não tornaram a Internet um instrumento de vigilância total, mas seus colegas - cientistas da computação e engenheiros, o fizeram. E criptógrafos têm a capacidade de ajudar. (ROGAWAY, 2015).

CONCLUSÃO

Com o passar da Guerra, novas relações entre ética, a criação científica e modelos de sociedade foram inauguradas como forma de alimentar uma nova forma de desenvolvimento tecnológico, moralmente relacionada, diante das consequências observadas com a fabricação de armas de guerra. Possivelmente, poucos foram aqueles cientistas que incorporaram tal natureza. Da mesma forma, modelos panópticos são elaborados diariamente e cientistas, engenheiros e criptógrafos também são responsáveis pelos rumos que a arquitetura da Internet irá tomar, porém apenas uma pequena parcela assimila esse caráter.

A criptografia, a essa altura é possível afirmar, influencia as relações de poder e isso pode ser percebido no dia a dia das relações entre políticas e tecnologias. Não à toa, os maiores esforços despendidos no desenvolvimento de métodos criptográficos ocorreram justamente em períodos de guerra. De toda forma, ao passo que informações governamentais são cada vez mais confidenciais, a encriptação de comunicações privadas vem enfrentando sistemáticas investidas de regulações restritivas ao seu uso. Essa leitura sugere como a distribuição de poder quer ser arranjada por certos poderes públicos.

A construção destas políticas não escapa do crivo dos variados setores, bem como o uso da encriptação não se distancia, atualmente, da esmagadora maioria da sociedade. Por isso mesmo, essas regulações devem abarcar um modelo multissetorial de discussão e de desenho de políticas públicas que vem ganhando força com a governança da internet. Novos modelos regulatórios devem acompanhar o ineditismo de novas tecnologias e de novas formas de relações sociais, a exemplo do que a rede possibilitou. Este espírito, por fim, sugere a democratização das informações, dos meios de expressão e de dos processos participativos políticos. A governança da criptografia se põe como uma transversal aos rumos que esta nova sociedade apresentará.

REFERÊNCIAS

ABELSON et al. **Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications.** Cambridge, 2015. Disponível em **https://dspace.mit.edu/handle/1721.1/97690**. Acesso em 19 de fevereiro de 2019.

ABELSON et al. **The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption**. Columbia University Academic Commons, 1997. Disponível em **https://doi.org/10.7916/D8GM8F2W**. Acesso em 19 de fevereiro de 2019.

ANDERSON, Tim. **Oppenheimer's Dilemma.** Stanford University. 2016. Disponível em: **http://large.stanford.edu/courses/2016/ph241/anderson1/**. Acesso em 19 de fevereiro de 2019.

AOKI et al. **Law Professors' Letter Opposing Mandatory Key Escrow.** 1997. Disponível em: **http://osaka.law.miami.edu/~froomkin/lawprof-letter.htm**. Acesso em 19 de fevereiro de 2019.

BUDISH, Ryan; BURKERT, Herbert; GASSER, Urs. **Encryption Policy and Its International Impacts: a Framework for Understanding Extraterritorial Ripple Effects.** Hoover Institution, artigo n. 1804, 2018. Disponível em: https://www.hoover.org/research/encryption-policy-and-itsinternational-impacts

Crypto Museum. Clipper Chip: Cryptographic Key Escrow. Disponível em https://www.cryptomuseum.com/crypto/usa/clipper.htm. Acesso em 19 de fevereiro de 2019.

Encryption: a Matter of Human Rights. International Amnesty. 2016. Disponível em: https://www.amnestyusa.org/reports/encryption-a-matter-of-human-rights/. Acesso em 19 de fevereiro de 2019.

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

GREENWALD, Glenn. MACASKILL, Ewen. **NSA Prism Program Taps Into User Data of Apple, Google and Others.** Disponível em: **https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data**. Acesso em 19 de fevereiro de 2019.

HUGHES, Eric. **A Cypherpunk's Manifesto.** 1993. Disponível em: https://www.activism.net/cypherpunk/manifesto.html. Acesso em 19 de fevereiro de 2019.

KAYE, David. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**. Disponível em: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session32/Documents/A_HRC_32_38_EN.docx. Acesso em 19 de fevereiro de 2019.

KENT, Gail. **Hard Questions: Why Does Facebook Enable End-to-End Encryption?** 2018. Disponível em: **https://newsroom.fb.com/news/2018/05/end-to-end-encryption/**. Acesso em 19 de fevereiro de 2019.

KLEINWÄCHTER, Wolfgang; ALMEIDA, Virgílio. **The Internet Governance Ecossystem.** IEEE Internet Computing, v. 19, n. 2, pp 64-67, 2015.

KURBALIJA, Jovan. **Uma Introdução à Governança da Internet.** Edição: 6ª ed.

São Paulo: Comitê Gestor da Internet, 2016.

LESSIG, Lawrence. **CODE 2.0.** Edição: 1ª ed. New York: Basic Books, 2006.

LEVY, Steven. **Battle of the Clipper Chip.** The New York Times, 1994. Disponível em: https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html Acesso em 05 de fevereiro 2019.

LEVY, Steven. **Crypto Rebels**. 1993. Disponível em: https://www.wired.com/1993/02/crypto-rebels/. Acesso em 19 de fevereiro de 2019.

Lizzie O'Shea on the Encryption Bill. Digital Rights Watch, 2018. Disponível em: https://digitalrightswatch.org.au/2018/12/05/lizzie-oshea-on-the-encryption-bill/. Acesso em 19 de fevereiro de 2019.

PEDNEKAR-MAGAL, Vandana; SHIELDS, Peter. **The State and Telecom Surveillance Policy: The Clipper Chip Initiative**. Communications Law and Policy, vol. 8, 429-464, 2003.

PFEFFERKORN, Riana. **Comments on Exposure Draft of Assistance and Access Bill.** Stanford Law School, CIS – Center for Internet and Society. 2018. Disponível em: https://cyberlaw.stanford.edu/files/publication/files/2018-09-09%20Pfefferkorn%20Comments%20to%20Australian%20Govt%20on%20Assistance%20%26%20Access%20Bill.pdf. Acesso em 19 de fevereiro de 2019.

ROGAWAY, Phillip. **The Moral Character of Cryptographic Work.** University of California, 2015. Disponível em: **http://web.cs.ucdavis.edu/~rogaway/papers/moral.pdf**. Acesso em 19 de fevereiro de 2019.

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

The Clipper Chip. Disponível em: **https://www.epic.org/crypto/clipper/**. Acesso em 19 de fevereiro de 2019.

The White House. **Statement of the Press Secretary.** 1994. Disponível em: https://www.epic.org/crypto/clipper/white_house_statement_2_94.html. Acesso em 2019 e 03 de julho de 2019.

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

Sugestão de citação (ABNT): SOBRENOME, Nome. Título do artigo. I ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, NOVEMBRO DE 2017. Disponível em: