RELATÓRIO DO WORKSHOP "CRIPTOGRAFIA, REGULAÇÃO E DIREITOS HUMANOS"
VIII FÓRUM DA INTERNET NO BRASIL 2018

Estrutura do Workshop:

O moderador realizou a apresentação d@s painelistas, seguido de breve enunciado sobre os problemas atuais propostos pelo painel.

Em seguida, o debate foi encaminhado por provocações/perguntas (apresentadas abaixo). Cada painelista teve 7 a 8 minutos a cada rodada de respostas. Na medida do razoável e respeitando a linha de raciocínio de quem estava com a fala, outr@s painelistas puderam intervir, fazendo considerações ou contraposições em torno do tema em questão, de forma franca e horizontal.

Após as rodadas de respostas, a moderação abriu para o debate com o público. Perguntas d@s participantes presenciais e via internet foram colhidas e respondidas. A moderação abriu para considerações finais d@s painelistas, seguidas de encerramento.

O formato do painel foi de mesa redonda, portanto mais dinâmico, facilitado por perguntas e provocações sem powerpoints, apenas a força da argumentação e do debate.

Perguntas que foram direcionadas pela moderação

1. Considerando a criptografia como um dos principais métodos para a garantia da segurança em um mundo conectado através de plataformas, bem como para a proteção de direitos humanos, tais como a liberdade de expressão e a privacidade, sobretudo em atividades de caráter político, quais os riscos que podemos esperar caso o acesso excepcional ao conteúdo encriptado (*backdoor*), por parte do Estado, seja permitido no Brasil? É possível viabilizar o acesso excepcional sem que haja graves riscos à segurança nas comunicações e à garantia de direitos?

2. Autoridades policiais norte-americanas frequentemente afirmam que estão "no escuro" em razão da criptografia nas comunicações, ou seja, afirmam que a criptografia vem inviabilizando as investigações policiais. Até que ponto faz sentido a afirmação de que a criptografia forte põe em risco a segurança nacional? Já não há políticas entre o setor privado e as autoridades estatais, no âmbito de investigações, para que sejam cedidas informações?

3. Nas últimas eleições presidenciais do Brasil, o WhatsApp, foi o principal veículo de disseminação de notícias, sobretudo as falsas, segundo pesquisas. Um desafio esperado será mapear a genealogia da desinformação, sobretudo em uma plataforma com encriptação. Há quem diga que a criptografia deva ser flexibilizada em razão do risco social provocado pelas fake news em veículos como o WhatsApp. Há de haver nova regulação específica para este tipo de plataforma no que diz respeito à criptografia? E, como um todo, podemos falar em uma regulação da criptografia?

Primeira Pergunta da Moderação e Rodada de Respostas

Nathalia Sautchuk - Nic.br Graduada e mestra em Engenharia de Computação pela Escola Politécnica da Universidade de São Paulo. É professora da disciplina "Governança da Internet" no Curso de Pós-Graduação em Assessoria de Comunicação e Mídias Digitais na Universidade Anhembi Morumbi e no Curso de Pós-Graduação em Segurança da Informação no Centro Universitário SENAC. Também atua como Assessora Técnica ao Comitê Gestor da Internet no Brasil (CGI.br). Faz parte do Núcleo de Coordenação da Rede de Pesquisa em Governança da Internet.

Nathalia trouxe diversos conceitos gerais, alguns sobre segurança da informação. Um sistema é seguro quando fornece informações íntegras somente a usuários autorizados, no momento em que elas são pedidas através de requisições válidas e identificadas, não permitindo que essas informações sejam recebidas, observadas ou alteradas por terceiros não autorizados. Há diferentes aspectos que caracterizam a segurança de um sistema de computadores, conhecidos como serviços de segurança. Os serviços básicos de segurança compreendem a confidencialidade, a integridade e a disponibilidade.

A integridade de dados assegura que as informações e os programas sejam modificados somente de uma maneira especificada e autorizada, enquanto a disponibilidade assegura que os sistemas operem prontamente e seus serviços não fiquem indisponíveis para usuários autorizados. Já a confidencialidade de dados é a garantia de que qualquer informação armazenada num sistema de computação ou transmitida via rede seja revelada, acessada e manipulada somente por usuários devidamente autorizados.

A confidencialidade tem relação com a privacidade, sendo que esta última pode ser definida como a garantia de que os indivíduos controlem ou influenciem quais informações sobre eles podem ser coletadas e armazenadas, bem como por quem e para quem tais informações podem ser reveladas. Sendo assim, a privacidade, além de abranger a confidencialidade de dados, também envolve as políticas de uso por usuários autorizados. A criptografia é essencial para a garantia da confidencialidade, bem como da privacidade, já que para os demais existem outras práticas que se aplicam.

O que significa um sistema seguro dentro da segurança da informação?

Existem três tipos de serviços básicos de segurança. Tríade CID* Tem que fornecer as informações de forma integral aos usuários autorizados,no momento que elas são requisitadas , com requisições válidas e identificadas. A integridade dos dados assegura que as informações só sejam modificadas de uma maneira segura. A informação não pode ficar tão protegida ao ponto de se tornar inacessível.

Quando tratamos de criptografia, estamos falando, em grande parte, da confidencialidade dos dados. Qualquer informação só deve ser acessada ou manipulada por usuários autorizados. outros quaisquer não deveriam ter acesso.

A confidencialidade que tem uma relação direta com a privacidade dos usuários. A privacidade tem relação com a confidencialidade, mas extrapola isso. Tem a ver também com políticas de uso por usuários autorizados, como uma política de segurança da informação.

Nos outros serviços existem outras práticas para garantir integridade, disponibilidade, que não a criptografia , que garante um dos pontos da segurança da informação.

A criptografia é uma área de estudo, que aborda principios e tecnicas pela qual a informação é tratada, de um texto claro, ou texto plano, em outra forma ilegível, o texto ou conteúdo criptografado, que só pode ser conhecido pelo seu destinatário. O destinatário tem uma chave, que deve ser secreta, e essa chave dá um acesso.

O algoritmo criptográfico são equações matemáticas, que realizam cálculos computacionais para a criptografia dos dados. A criptografia é a área de estudo, e o algoritmo é a aplicação disso. Existe a criptografia simétrica, que é compartilhada entre as duas pessoas na comunicação Há também a criptografia assimétrica, que dá acessos diferentes, a chave privada e a pública.

Sobre backdoors, ou porta dos fundos, muitas vezes é algo secreto, que transpõe uma aplicação normal de um produto, os backdoors normalmente são colocados para garantir acesso não autorizado remoto por um computador. Pode estar, já constar, no programa ou código, pode ser instalado como um rootkit ou no próprio hardware.

O risco de colocação de uma backdoor num algoritmo criptográfico, segundo especialistas, fragiliza muito a aplicação de confidencialidade e a proteção dos dados. Não se pode assegurar nem afirmar que uma backdoor, mesmo que imposta por lei ou como política pública, garante proteção contra acesso de terceiros pela mesma backdoor.

A criptografia é muito mais do que apenas o whatsapp, o comércio eletrônico, o sistema bancário e diversas outras aplicações da sociedade funcionam em cima de sistemas criptográficos.

Veridiana Alimonti - advogada, analista sênior de políticas para a América Latina na Electronic Frontier Foundation e doutoranda em direitos humanos pela Faculdade de Direito da USP. Foi estudante visitante no Departamento de Proteção de Dados do Conselho da Europa em 2017, representante titular do terceiro setor no CGI entre 2011 e 2013 e representante dos consumidores no Comitê de Defesa dos Usuários de Serviços de Telecomunicações da Anatel (CDUST) até o início de 2015.

Veridiana[1] trouxe exemplos sobre acesso excepcional, como o diretor do FBI em 1995. Disse que a criptografia forte era uma necessidade tanto para o governo como para a indústria e para o mercado. Apesar disso queriam um alçapão, com uma chave mestra, ou seja, um acesso excepcional)

Segundo outro artigo do New York times mencionado, há uma linha entre a confidencialidade e a segurança pública, quando se fala de riscos.

A primeira premissa que Veridiana levanta é que que há um reconhecimento de que a criptografia precisa ser forte e que esse acesso excepcional seria necessário. Porém na criptografia de ponta a ponta, o mensageiro não tem acesso ao conteúdo dessa mensagem.

Quem tem acesso a essa tecnologia, geralmente tem implementado tecnologias de chaves trocadas em cada mensagem.

Sobre as premissas e os riscos. Hipótese: Reconhece a importância da criptografia, mas um alçapão ou porta dos fundos supostamente não comprometeria a segurança do sistema como um todo.

Resposta da painelista: Especialistas consideram que os modelos matemáticos mais complexos trazem riscos também por situações que podem não ter sido previstas pelos teóricos. Conclui dizendo que criação de um backdoor coloca uma óbvia fragilidade no sistema de segurança. As pessoas que têm acesso a essas chaves podem optar por vazá-las ou disponibilizá-las de maneira ilegal. Em 2017 a Wikileaks demonstrou que mesmo documentos internos da NSA e da CIA, vazaram por conta de um backdoor. As vulnerabilidades nem sempre seguem o roteiro de confidencialidade porque o devido processo legal nem sempre é seguido.

O comprometimento de criptografia, por conta de um acesso a um banco de dados que não tem segurança suficiente, coloca em risco todo o sistema jurídico e tem relacão com uma série de outros direitos, como liberdade de expressão, direitos humanos etc.

Fernanda Teixeira - Coordenadora do grupo de Combate aos Crimes Cibernéticos da Procuradoria da República em São Paulo. Coordenadora-Adjunta do Grupo de Apoio sobre Criminalidade Cibernética da 2ª Câmara de Coordenação e Revisão da PGR.

A criptografia ponta a ponta trouxe, na visão do Ministério público, uma série de complexidades que dificultam as investigações, especialmente para o processo criminal.

Uma das principais técnicas investigativas, segundo a painelista, é a interceptação de comunicação telefônica. Com o aparecimento dos mensageiros eletrônicos, com a

[1] **Obs : Cumpre ressaltar interrupções de ordem técnica durante as falas da palestrante Veridiana Alimonti, o que prejudicou o registro e o resgate de parte do conteúdo.**

criptografia ponta a ponta, todo o fluxo de comunicação passou para os mensageiros. Os agentes de segurança passaram a se sentir mais vulneráveis. Não existia mais a fonte de investigação da interceptação autorizada. Por isso a preocupação.

Sobre os bloqueios do whatsapp. O primeiro aconteceu quando ainda não existia no serviço criptografia de ponta a ponta. A comunicação poderia sim ter sido entregue, aconteceu por desconhecimento por agentes da lei. Aconteceu por uma desídia da empresa, que começou a atuar no país, sem suporte jurídico.

Todas as sanções foram aplicadas, mas sem resposta do serviço. Por isso a suspensão das atividades.

Os dois últimos bloqueios, o segundo e o terceiro, o advogado da empresa foi ao juízo explicar que não dava para ter acesso ao conteúdo. Nem os metadados, que são informações relevantes para a investigação, não estavam sendo entregues. Depois que a comunidade jurídica entendeu o que significava criptografia ponta a ponta, passaram a entender que também queriam a sua segurança garantida, porque também atuam na proteção da privacidade das pessoas, como um direito humano. Também entendem que devem defender essa posição, como uma questão garantidora de direito de toda a comunidade. O MP também entende que o backdoor não é a ferramenta mais adequada.

É como a empresa blackberry, que cedeu o acesso para os agentes da lei e depois faliu. No direito pátrio, toda a investigação que foi feita, tem que constar no processo. Uma vulnerabilidade dificilmente seria mantida em segredo.

Natalia Garcia - advogada especialista em direito bancário e financeiro. Diretora Jurídica da Foxbit e vice-presidente da ABCripto.

Natália aponta que, em 1992, quando surgiu o movimento Cypherpunk, dentro de um fórum de criptografia, queriam utilizar ferramentas que protegessem as informações do ponto de vista da privacidade. Por serem libertários, voltados para um estado menor, queriam “expurgar’ o mal através da criptografia. A primeira tecnologia, de fato, de criptografía simétrica, com chaves públicas e privadas, foi no blockchain do bitcoin.

Como você consegue utilizar a criptografia assimétrica, para prevenir que o sistema todo seja utilizado por maus elementos? Nao funcionou num primeiro momento. Os crypto ativos eram utilizados na *deepweb* pelo tráfico de drogas.

O FBI conseguiu apreender os principais criadores do principal site da *darkweb*, o *Silkroad.* Desde então começou-se a estudar até que ponto poderia ser monitorado esse ambiente. É uma tecnologia extremamente monitorável e rastreável. Hoje, a criptografia e a tokenização de ativos, é uma tecnologia que pode surgir completamente rastreável. A criptografia hoje é utilizada por bancos, comércios e, enfim, a maioria das empresas do Brasil e do mundo, pesquisam sobre blockchain.

Como que a sociedade lida com essas novas discussões e novos temas? Seria possível que as autoridades as rastreiem e monitorem ?

Nesse sentido, consegue-se sim fazer crescer a tecnologia, para nao ter mais as *liabilities* que se tinha antes com a relação tecnológica anterior.

A imutabilidade é um preceito ruim para a tecnologia em si. Não está de acordo com algumas leis, como a de proteção de dados, que dá direito ao esquecimento. Quando se registra no blockchain, não se pode apagar nunca mais. O sistema do bitcoin funciona a partir do consenso, num sistema imutável: se algum arquivo tivesse metadado relacionado a pedofilia, não se poderia apagar nunca mais. O preceito da imutabilidade é ruim e fere em todos os aspectos os direitos humanos.

Paulo Rená - Mestre em Direito, Estado e Constituição (UnB). Professor de Pós-Graduação (IESB), Graduação (UniCEUB) e pesquisador (Cultura Digital & Democracia - UniCEUB). Fundador da ONG Instituto Beta: Internet e Democracia. Foi gestor da elaboração do Marco Civil da Internet no Brasil (Ministério da Justiça)

A função da criptografia não é só o sigilo (o qual é um direito constitucional das democracias modernas), mas também integridade e a autenticação são valores também fortemente protegidos pela criptografia e que são essenciais. Diante desses frentes, alguma quebra da segurança criptográfica inviabiliza e compromete esses valores. É o caso da Blackberry, que teve sua tecnologia inviabilizada no mercado diante do enfraquecimento de sua criptografia.

Se o próprio Estado que detém o uso da força legítima, sabendo de uma vulnerabilidade ou mesmo, sendo responsável pela sua criação, ele próprio põe em risco os indivíduos da sociedade, além de comprometer trabalhos e funções do próprio Estado.

Para resolver crimes, inclusive crimes de corrupção, não é necessário “jogar o fora o bebê junto com a água suja”. Para perseguir um crime, qual seja a natureza, não devemos comprometer a tecnologia intermediária, ou seja, a criptografia. Cita a Electronic Frontier Foundation, quando diz que a robustez de uma corrente ela tem o grau da força do elo mais fraco, e não dos mais fortes. Não podemos então admitir nenhum elo vulnerável em uma rede de proteção de conteúdo quanto a seu sigilo, autenticidade e integridade. Isso comprometeria inclusive toda a tecnologia de transações bancárias.

Os anos noventa simbolizaram o esforço do Estado para haver um acesso excepcional às comunicações de forma sistematizada, mas foi comprovado que não haveria como garantir que terceiros mal intencionados explorassem esse excepcionalidade. Com Edward Snowden, foi revelado que foram inseridas vulnerabilidade propositalmente, por parte do Estado, e que posteriormente foram exploradas por terceiros que originalmente não tinham permissão.

O mediador considera que há uma diversidade de perspectivas sobre o acesso excepcional, passando por questões mais técnicas, questões mais atinentes aos direito fundamentais ou por questões sobre investigações criminais. Faz a segunda pergunta a respeito da questão do *going dark* e levanta o questionamento sobre a possibilidade de uma "regulação da criptografia"

Segunda Pergunta da Moderação e Rodada de Respostas

Nathalia Sautchuk - Qualquer espécie e alternativa à encriptação pode ocasionar um efeito oposto. Criminosos, diante de mudanças em encriptação como a da Whatsapp, por exemplo, migraram para plataformas mais propícias para suas atividades ou até mesmo desenvolver as suas próprias. Estaríamos "enxugando gelo."

Alguns metadados já são exigidos que sejam armazenados e podem ser requisitados no âmbito de investigações. Mesmo que não haja acesso ao conteúdo em si das comunicações, os metadados já oferecem informações que colaboram suficientemente com investigações. Não devemos esquecer que há outros métodos de investigação, como o infiltramento de agentes no meio digital, que podem ser efetivos.

Sobre regulação da criptografia, é controverso e não tem muita efetividade na prática. Temos outras técnicas como a "esteganografia", ocultar informações em outros tipos de arquivos. Ou seja, há outros métodos de burlar qualquer limitação à fabricação de algoritmos de criptografia.

Veridiana Alimonti - A criptografia serve para proteger a segurança nacional. Snowden mostrou que uma série de informações críticas de outros Estados estavam sob vigilância da NSA. Ou seja, a criptografia é fundamental para assegurar o sigilo de informações do Estado contra espionagem ou vigilância de outros Estados.

Sobre o discurso de que a criptografia dificulta investigações sobre atividades terroristas, isso se coloca em um debate de proporcionalidade. Comprometer mecanismos de segurança, como a criptografia, é o melhor meio de se garantir a segurança nacional? Deve haver um debate de adequação e proporcionalidade. Há outros meios de investigação criminal, como a interceptação telefônica, a decodificação de dispositivos quando há acesso por meio de busca e apreensão. Apesar de haver facilidade em acesso às informações através de uma vulnerabilidade na criptografia, há de se fazer um teste de proporcionalidade, inclusive se levando em consideração outros meios de investigação.

Lembra que nos Estados Unidos já houve uma regulação sobre a exportação de algoritmos de encriptação. A EFF participou de ação envolvendo a matéria, onde se afirmou que o código escrito também fazia parte da liberdade de expressão do desenvolvedor.

Aponta que a regulação da criptografia pode não ser o melhor caminho, mas pensar outros mecanismos e soluções que viabilizem investigações, em contraposição com as movimentações restritivas da Austrália.

Fernanda Domingos - em alguns casos de investigação, o conteúdo das comunicações é fundamentalmente importante. Apesar de outros meios, como a infiltração, que também gera uma burocracia que envolve ganhar a confiança do grupo de criminosos, conseguir autorização para cometer pequenos delitos, isso resolve crimes que estão sendo cometidos agora e que depende do acesso em tempo real.

Quando houve a questão do Whatsapp, o MPF foi atrás de soluções que não envolvessem a implementação de um backdoor. Com isso, surge a ideia de um *man in the middle*, com colaboração da empresa, com ordem judicial. O MPF compreende que a criminalidade migre para outros aplicativos ou até mesmo os crie caso se tenha conhecimento de colaborações do Whatsapp com a polícia. Mas nem todas as organizações criminais tem poder de construir suas próprias plataformas.

No fim, a encriptação terá que ser regulada. Todos os direitos para funcionem precisam de regulação. A sociedade e o Congresso terá que decidir isso, não é com o MPF. A Austrália tem um projeto de lei, o Reino Unido já tem lei. Outros caminhos seguiram outro caminho. A Alemanha e a Holanda já tem regulações para que o próprio governo possam hackear sites, computadores etc, quando não possível acesso direito ao dispositivo. Fatalmente irá haver algum tipo de regulação

Nathalia Sautchuk - esclareceu o conceito de *Man in the middle*. É uma forma de ataque, onde pode se guardar e repassar, ou pode alterar, "*nesse nó do meio*", algumas informações, isso é acessado no momento do fluxo da comunicação dos dados. Nao altera em si o dispositivo e o conteúdo da comunicação. Isso não é backdoor por que isso será usado durante o fluxo. Não necessariamente funcionaria, pq se os dados colhidos, em fluxo, estiverem encriptados, continua sem acesso a mensagem.

Natália Garcia - Como conciliar a segurança pública quando posto frente a frente a privacidade, em um contexto de segurança da coletividade. Complicado botar na balança. O Brasil não é totalitário, mas a partir do momento em que o Estado tem acesso a uma parte das comunicações, também irá querer todo o restante. E como proteger o indivíduo diante dessa postura do Estado? Por que hoje as autoridade tem que pedir informações ao Google, Facebook etc? Por que estas empresa são *pools* de informações. Mas e se o indivíduo for o detentor dessas informações? Vemos então, como no contexto do blockchain, por exemplo, o retorno do empoderamento do indivíduo. Isso se relaciona à realidade do mercado de dados e como o indivíduo vem relendo a forma como cede seus dados.

Em relação à regulação, a internet surgiu em 1964 e foi regulada no Brasil em 2014. O uber surgiu em 2009 e foi regulado em 2017. Para regular uma tecnologia é complexo. Como regular algo em que ao menos entendemos, como criptoativos? Como por todos os

aspectos de uma tecnologia, diante de sua complexidade. Foi preciso o escândalo da NSA para regularmos a internet no Brasil. Precisamos entender, primeiro, os aspectos da tecnologia para começarmos a pensar algo nesse sentido.

Paul Rená - Vê regulação de forma distinta. Boaventura de Souza Santos diz que se o estado só enxergar o que é quadrado, vai ignorar o que é redondo. Vai deixar de fora aquilo que não seguir padrões já compreendidos. O papel do Estado é ir atrás da diversidade de interesses da sociedade. Deve promover a diversidade. Se for esperar o entendimento completo e "estático" sobre algum fenômeno, uma regulação será defasada.

A neutralidade de rede, por exemplo, sua regulação promove a regulação. Se não garantirmos hoje uma flexibilidade de regulação que promova a diversidade, tolheremos a inovação. A regulação não deve encerrar um modelo de criptografia, temos que regular no sentido de garantir o uso. A internet tem regulação que não a limita. O entendimento jurídico de liberdade e igualdade já pode guiar um modelo de regulação. O Marco Civil da Internet regula, por exemplo, responsabilidade de provedores. Portanto há uma regulação positiva. Sobre as audiências públicas realizadas no STF, sobre criptografia, uma questão importante foi entender que na Lei de Interceptação, dissemos que os dados são efêmeros. Se o que foi dito no telefone, caso não gravado, a informação some, não é resgatada, diferente de um livro, em que o conteúdo e estático. No digital, a mensagem é permanente. É preciso observar isso. Compara a quebra da criptografia ao instrumental da tortura. Por meio da tortura podemos extrair muitas informações de um suspeito. Podemos, portanto, torturar? Existe uma regra que diz que "é melhor não".

O going dark é uma falácia. Nunca tantos dados pessoais estiveram disponíveis como hoje. Então há uma profusão de informações.disponíveis às investigações. Isso é específico da atualidade.

Abertura para participação do público.

Primeira pergunta: Será que não devemos repensar o conceito de crime? No furuto, o crime será cometido pela internet. Cita Shane Harris. Temos que repensar os crimes com reconfigurações possibilitadas pela Internet. Vulnerabilizar sistemas de segurança ajudam a essa reconfiguração criminosa e a violação de direitos.

Segunda pergunta: Será possível pensar em uma flexibilização de criptografia para a hipotese de crimes mais graves? E como garantir a privacidade em relação às pessoas que não tem envolvimento de crimes graves, a grande maioria? Muitas vezes pensamos o direito no Brasil, importamos ideias de fora, como a colaboração processual e isso levou a problemas no cenário nacional. A mesa fala muito em terrorismo e segurança nacional. Será que não temos que ter cuidado ao pensar essas questões quando nacionalizamos problemas de fora?

Terceira pergunta: No artigo 5 da Constituição Federal, temos o direito ao sigilo, salvo quando, por ordem judicial, é possível essa quebra. Essa questão também pode servir a perseguições políticas ou busca por organizações criminosas. Como trabalhar essa

dicotomia levando-se em consideração a possibilidade de abuso de autoridade. O receio que haja a flexibilização do sigilo já acontece hoje quando se quebra sigilo de ligações telefônicas ou a própria ideia de grampo.

Quarta pergunta: Qualquer forma de *man in the middle,* em uma comunicação com encriptação ponta a ponta, pressupõe colocar um backdoor no sistema?

Quinta pergunta: Temos que defende a criptografia como ferramenta para o cidadão. Recomenda o PGP e o texto de Phil Zimmerman. A EFF demonstrou que os chips da Intel possuem espécies de backdoor. Quando o governo quer quebrar criptografia, isso na verdade é um grande tiro no pé.

Natália Sautchuk - A fragilidade da criptografia não deve ser pensada de forma nenhuma. Qualquer espécie de man in the middle também traz potencial problemas de segurança e vulnerabilidades. A gente não tem absoluta certeza de que o WhatsApp implementa o algoritmo do Signal, pois não há transparência no código. Os algoritmos precisam ser abertos e estudados para se entender suas seguranças e vulnerabilidade.

Veridiana Alimonti - O PGP foi uma das tecnologias desenvolvidas no contexto do *Clipper Chip.* Uma solução de resposta ao chip da NSA. Ainda que haja obrigações ou regulações restritivas, soluções alternativas serão desenvolvidas. É difícil manter as exceções ao acesso de forma absolutamente controladas, por mais garantias que haja. Essas vulnerabilidades perdem o controle, mesmo em caso de excepcionalidades a crimes hediondos ou crimes específicos. No caso de man in the middle, o próprio usuário seria notificado com houvesse alguma alteração do safety number. Então seria possível verificar que houve mudança, o que notificaria aquele usuário que faz uso da aplicação de forma maliciosa.

Fernanda Domingos - O governo não quer quebrar a criptografia, todos já entenderam a importância da criptografia. O que agentes de segurança precisam, é algum meio de obter a comunicação. Temos que lidar com a criminalidade que está na rua, que planeja crimes, homicídios, tráfico e que se comunica, gerando mais violência. Precisamos de meios para garantir a comunicação. O man in the middle não é uma vulnerabilidade e deve ser utilizado para uma cooperação específica, ainda que a gente saiba que haja a migração dos criminosos para outras plataformas. A alternativa que o governo insira malwares também deve ser levada em consideração. Todos esses caminhos dependem de debate.

Natália Garcia - A maioria dos crimes cometidos pela internet não são novos, só assumem nova roupagem. Phishing por exemplo é roubo feito pela internet. Ransomware é extorsão. Os meios apenas são diferentes e podemos por qualificantes, pode ser uma maneira de combatê-los.

Paulo Rená - Sobre o Phil Zimmerman. O argumento central é que, antigamente, sem as comunicações eletrônicas, as informações eram privadas. A ideia do PGP é que todos tenham a possibilidade de privacidade nas comunicações eletrônicas. Se só os criminosos têm meios de tornar sigilosas suas comunicações, isso enfraquece o indivíduo. Portanto

este também tem que ter meios de proteger suas comunicações. A criptografia tem que ser total e generalizada. Impedindo, inclusive, possibilidades de man in the middle. Criptografia vulnerável é uma criptografia que não funciona. A tecnologia depende de várias camadas e é complexa. O assunto depende de diálogos, debates e conversas. Nos anos 70 a criptografia era tratada como arma de guerra nos Estados Unidos. Não é interessante que voltemos a esse cenário.