EXCELENTÍSSIMO SENHOR MINISTRO RELATOR DO SUPREMO TRIBUNAL FEDERAL

ADPF 403

O **LABORATÓRIO DE PESQUISA DIREITO PRIVADO E INTERNET DA FACULDADE DE DIREITO DA UNIVERSIDADE DE BRASÍLIA - LAPIN**, comparece, respeitosamente, à presença de Vossa Excelência, em atenção ao despacho e edital de convocação de audiência pública, para apresentar memorial de exposição de opiniões a respeito do uso de criptografia ponta-a-ponta em sistemas de mensagens eletrônicas.

1. DEFINIÇÃO DO TERMO "CRIPTOGRAFIA PONTA-A-PONTA"

A criptografia ponta-a-ponta (*end-to-end*) ou fim-a-fim é uma técnica matemática aplicada como recurso de segurança em um sistema de comunicação para garantir a confidencialidade da informação trocada. O processo de criptografia é realizado por meio de algoritmos, um conjunto de regras ou passos necessários que possibilitam a cifragem da informação, que passa a ser inteligível apenas para os usuários envolvidos na conversa (emissor e receptor). Ressalte-se que criptografia (palavra cuja etimologia remete ao termo grego *kriptos*, que significa "secreto") representa método essencial para a garantia da segurança de operações cotidianas na Internet, a exemplo de transações bancárias, garantindo a privacidade dos usuários e a integridade e autenticidade das mensagens.

Hoje, inclusive, a maioria dos aplicativos tecnológicos de troca de mensagem, tais como Whatsapp, Telegram e iMessage, oferecem um serviço de mensagem protegido por criptografia ponta-a-ponta, utilizando um protocolo de troca de chaves (valores numéricos utilizados por um algoritmo para alterar uma informação). A cada mensagem, um par de chaves matematicamente relacionadas, uma pública (usada para cifrar) e outra privada (usada para decifrar) são geradas por um algoritmo criptográfico e trocadas entre os usuários. Por esse motivo, a criptografia ponta-a-ponta é um tipo de criptografia assimétrica, uma vez que a chave de cifragem é distinta da chave de decifragem.

Assim, uma vez aplicada a criptografia ponta-a-ponta, o conteúdo das mensagens torna-se cifrado, inacessível a terceiros interessados em intervir no processo comunicativo, denominados “adversários” na literatura sobre o tema, pelo fato de não possuírem a chave privada utilizada para decifrar e permitir a leitura da mensagem no seu destino. Ademais, apesar de esse processo impedir que o provedor de aplicações, ou algum outro terceiro presente na transmissão da informação, tenha acesso ao conteúdo das mensagens, a criptografia não cifra outros dados relevantes nesse processo comunicativo, a exemplo do dia e horário da mensagem, do seu remetente e destinatário.

2. O USO DE BACKDOORS: VULNERABILIDADES E OUTROS EFEITOS COLATERAIS

A principal solução sugerida por autoridades legais para que possam ter acesso ao conteúdo de mensagens criptografadas trocadas entre usuários é a instalação de *backdoors*, falhas de segurança propositalmente criadas durante o desenvolvimento do software, para facilitar a intervenção de terceiros. Por exemplo, poderia ser criado um mecanismo de "depósito de chaves" (em inglês, *key escrow*), que permitiria às autoridades investigativas a recuperação das chaves utilizadas em uma sessão de troca de mensagens.

Há, contudo, diversos perigos dessa alternativa, conforme foi apontado por especialistas em ciências da computação do MIT[1], publicado em estudo de julho de 2015. A primeira ressalva é que o *key escrow* vai de encontro às boas práticas que vêm sendo utilizadas em protocolos de comunicação de mensagens, o *forward secrecy*, que consiste na criação de novas chaves criptográficas para cada mensagem trocada, impedindo que um agente malicioso possa ter acesso a todo o conteúdo da conversa caso obtenha uma das chaves. É perceptível que o depósito de todas as chaves trocadas em cada envio-recepção de mensagem para uso eventual dos agentes legais seria inviável, dada a escala exponencial do número de conversas existentes em serviços de mensageria.

O segundo problema é a complexidade da implementação desta "solução". O WhatsApp não é o único serviço de mensagens existente. Para adquirir amplo acesso aos vários canais de comunicação existentes, seria necessário que *backdoors* fossem criados para cada serviço existente. Só no Brasil, podemos citar alguns aplicativos amplamente utilizados como o Telegram, Skype, Facebook Messenger, Viber e Snapchat. A Electronic Frontier Foundation - EFF, publicou uma lista com mais de 30 aplicativos de mensagem que utilizam alguma forma de criptografia[2]. E mais vão sendo criados a cada dia. A dificuldade para se configurar vulnerabilidades em cada sistema reforça a inviabilidade da prática demandada pelas autoridades investigativas.

Em terceiro lugar, a criação de falhas de segurança em aplicativos específicos poderia trazer graves consequências econômicas para as empresas envolvidas. Em razão da crescente complexidade da arquitetura das tecnologias de informação e comunicação e dos riscos atrelados a elas, a demanda por garantias mais efetivas e sofisticadas de proteção às informações pessoais na rede tende a ser cada vez maior. Assim, a abordagem que uma empresa oferece à privacidade se mostra, precisamente, como a vantagem competitiva necessária para obter sucesso no mercado. Por

[1] ABELSON, et al. Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications. Massachusets Institute of Technology. Disponível em: <https://dspace.mit.edu/handle/1721.1/97690>. Acesso em: 15 de maio de 2017.
[2] EFF. Secure messaging Scorecard. Disponível em: <https://www.eff.org/node/82654>. Acesso em: 15 de maio de 2017.

conseguinte, a perda de confiança dos usuários ao saber que as transações criptografadas não seriam mais seguras, levaria à rápida migração para serviços alternativos. Em um cenário ainda mais drástico, porém plenamente possível, os altos custos envolvidos para a implementação e manutenção desses sistemas de backdoors/key escrows, poderiam tornar o negócio de serviços de mensageria inviável de pronto, prejudicando o consumidor de uma forma geral.

Por fim, as autoridades legais devem refletir sobre as consequências de terem em mãos suas "chaves mestras". Como destacado pelos pesquisadores do MIT, os holofotes seriam colocados nos detentores do depósito de chaves, sejam eles o provedor do serviço, as autoridades legais, ou um terceiro confiável. Isto poderia induzir um ataque massivo de atores maliciosos contra estas entidades, aumentando os custos necessários para garantir a segurança na manutenção das chaves.

Um acontecimento recente digno de nota, apesar de não envolver a guarda de chaves, envolve a guarda de outros itens sensíveis. Trata-se do furto de ferramentas de espionagem digital da agência de segurança nacional norte-americana (NSA), cuja tecnologia deu origem ao *ransomware WannaCry*, que atacou sistemas por todo o mundo[3]. Isso demonstra o perigo de se manter informações de interesse a atores maliciosos guardadas num único local, por mais seguro que este possa parecer ser.

Nesse sentido, cumpre destacar trecho de memorial apresentado por experts em cibersegurança e criptografia aplicada do *Stanford Law School Center For Internet And Society,* no caso Apple v. FBI[4], que discutiu, essencialmente, a mesma matéria ora debatida:

---

[3] Conforme descrito em http://www.forbes.com.br/colunas/2017/05/o-que-podemos-aprender-com-o-ataque-massivo-do-ransomware-wannacry/.

[4] Em 2016, o FBI pediu que uma corte federal norte americana determinasse à Apple o desbloqueio de um *Iphone* utilizado por um atirador em massa na cidade de San Bernardino, Califórnia. Representada pelo Departamento de Justiça, a polícia federal de investigação demandava a criação de um novo *software* para contornar o sistema de bloqueio do *iPhone,* onde poderiam estar armazenadas informações relevantes para o caso. A Apple recusou o pedido, centrando o seu argumento no risco de tal tecnologia cair em mãos hostis – *hackers* ou grupos criminosos e terroristas – ou, ainda, ser solicitada por autoridades judiciais de países não democráticos. (Disponivel em https://www.publico.pt/tecnologia/noticia/apple-vs-fbi-nao-sabemos-onde-isto-vai-parar-1727852?page=3#/follw)

> Por razões práticas, o desvio na segurança da Apple determinado por essa Corte certamente será usado em outros Iphones no futuro. Esse spread aumenta os riscos de que o software forense escape do controle da Apple, seja por roubo, descaminho ou ordem de um outro tribunal, incluindo um governo estrangeiro. Caso isso aconteça, o código personalizado poderia ser usado por criminosos e governos para extrair dados sensíveis pessoais ou relacionados a negócios de Iphones apreendidos, perdidos ou furtados (...) Obrigar a Apple a criar um software forense para o governo também é perigoso em razão de quaisquer falhas que o software possa conter. Além disso, a Corte aqui ameaça estabelecer um precedente legal que órgãos estatais aplicadores da lei utilizarão para forçar companhias a desenvolver outros desvios de segurança para propósitos forenses. Não existe nada no All Writs Act ou na decisão do Tribunal que colocaria fora de limites atualizações nos softwares que ativariam os microfones de uma smart TV para propósitos de espionagem ou ligariam a câmera de um laptop para vigilância de vídeo. Esses outros desvios apresentarão seus próprios (potencialmente ainda piores) riscos para a privacidade, cibersegurança e segurança pessoal do público. (...) Assim, os amici, respeitosamente, instam a Corte a reconsiderar a sua decisão. (STANFORD LAW SCHOOL CENTER FOR INTERNET AND SOCIETY, 2016, tradução livre do original)

Assim, conclui-se que a implementação de métodos que criem vulnerabilidades técnicas de forma a permitir o acesso ao conteúdo de mensagens, mesmo quando autorizadas por ordens judiciais, não pode ser feita sem comprometer, de algum modo, a segurança e a privacidade dos demais usuários. Uma vez que a existência de uma “chave mestra” para contornar a segurança do aplicativo implica necessariamente no enfraquecimento do protocolo de criptografia, é possível que essa vulnerabilidade seja usada de forma maliciosa por criminosos cibernéticos, terroristas e até mesmo por estados estrangeiros. Não bastasse, os custos oriundos dessa prática - que não são apenas econômicos, mas também legais e institucionais - são extremamente altos e serão sustentados pelos provedores do serviço e, consequentemente, pelo consumidor.

3. A IMPORTÂNCIA DA CRIPTOGRAFIA PARA A SOCIEDADE DA INFORMAÇÃO

A própria arquitetura da internet depende da habilidade das pessoas confiarem umas nas outras no que diz respeito ao tráfego de comunicações, isto é, para exercer suas liberdades civis digitalmente, os indivíduos precisam poder confiar nos intermediários e destinatários. Nesse cenário, a confiança online significa, principalmente, tornar-se vulnerável para uma pessoa ou organização ao revelar informações pessoais, o que inclui o risco crescente do mau uso dessas informações, vazamento de dados, manipulação e perda da autonomia. Uma vez que a informação é revelada, o indivíduo não detém mais o controle exclusivo sobre o seu uso e disseminação - ele está à mercê daquele que a coletou.

Diante desse cenário, a estratégia recomendada para o desenvolvimento de novas tecnologias é incorporar a privacidade e a proteção de dados como elementos intrínsecos, empregando-se uma abordagem caracterizada por medidas proativas e não reativas, que antecipe e previna eventos invasores de privacidade antes que eles aconteçam. Essa abordagem ficou conhecida como *privacy by design* e vem se expandindo não só como prática de mercado, mas também como imposição legislativa ao redor do globo[5].

Nesse sentido, a criptografia ponta-a-ponta utilizada pelos softwares de comunicação é uma expressão desse princípio, vez que proporciona - de forma harmoniosamente integrada no aplicativo - a privacidade e a segurança necessárias

[5] Diversas legislações internacionais já preveem em seus dispositivos o princípio do privacy by design, dentre elas destaca-se o General Data Protection Regulation, novo Regulamento europeu, aprovado em abril de 2016, que, em seu artigo 25, incorpora expressamente obrigações decorrentes da privacy by design:

Artigo 25: 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.(...) (REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016)

para o exercício do direito à liberdade de opinião e expressão na era digital. Inclusive, a Organização das Nações Unidas emitiu relatório[6] sustentando que tal segurança pode ser essencial para o exercício de outros direitos, incluindo direitos econômicos, privacidade, devido processo legal, liberdade de associação e o direito à vida e integridade física.

4. CONCLUSÃO

De fato, a encriptação de mensagens torna a vigilância mais difícil em alguns casos, mas o cenário real é muito mais diversificado do que se imagina. Sempre existiram, e sempre vão existir, muitas áreas de sombra e escuridão no processo de comunicação, isto é, canais de diálogo resistentes a vigilância. Isso não significa, contudo, que estamos fadados à escuridão e desordem. Como demonstrado acima, exigir da empresa provedora do serviço de mensagens a criação de um *backdoor* na criptografia, implica em criar um risco indesejável para todos os usuários, quando já existem técnicas diversas de interceptação que podem ser empregadas de forma igualmente eficaz e que apresentam menos ônus não só a empresa, mas também ao indivíduo.

Corroborando o exposto até o momento, vale destacar trecho do relatório produzido por grupo de trabalho instituído pela Comissão da Câmara norte americana em Energia e Comércio e pela Comissão do Poder Judiciário (*House Committee on Energy and Commerce and Committee on the Judiciary*) a fim de investigar os desafios apresentados pela criptografia e a sua relação com o cumprimento da lei:

> A criptografia está inexoravelmente ligada aos nossos interesses nacionais. É uma proteção para os nossos segredos pessoais e prosperidade econômica. Ela ajuda a prevenir crimes e proteger a segurança nacional. O uso generalizado de tecnologias de criptografia também complica a missão da aplicação da lei e das agências de inteligência. Como descrito nesse relatório, essas complicações não podem ser ignoradas. Essa é a realidade da sociedade moderna. Nós devemos nos esforçar para encontrar um ponto comum em nossa

[6] KAYE, D. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression**. Human Rights Council, United Nations. [S.l.]. 2015.

> responsabilidade coletiva: prevenir crimes, proteger a segurança nacional e fornecer as melhores condições possíveis para a paz e a prosperidade.
>
> Esse é o motivo pelo qual esse não pode mais ser um debate isolado ou binário. Não existe "nós contra eles" ou "pró-criptografia versus aplicação da lei". Essa conversa envolve todos e tudo que depende de tecnologias interconetadas - incluindo a aplicação da lei e as agências de inteligência. Esse é um desafio complexo que tomará tempo, paciência e cooperação para ser resolvido. As potenciais consequências da inércia - ou de uma reação excessiva - são demasiadamente importantes para permitir que perspectivas históricas ou ideológicas fiquem na frente do progresso. (ENCRYPTION WORKING GROUP YEAR-END REPORT. December 20, 2016. Tradução livre do original)

Conclui-se, portanto, que a criptografia e segurança não estão em pólos opostos. Não se trata, aqui, de colocar a privacidade das comunicações acima do interesse público. Pelo contrário, criptografia forte promove uma forte segurança. É do interesse coletivo que a Internet permaneça como plataforma propiciadora da liberdade de expressão e de opiniões de forma livre e desimpedida.

THIAGO GUIMARÃES MORAES
Pesquisador do LAPIN

ANA CAROLINA HERINGER COSTA CASTELLANO
Pesquisadora do LAPIN

AMANDA ESPIÑERA
Pesquisadora do LAPIN

MARCELO AMARANTE FERREIRA GOMES
Pesquisador do LAPIN