ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/319253588

DEBATENDO CRIPTOGRAFIA EM FACE AO MARCO CIVIL DA INTERNET

Article · January 2017

DOI: 10.11606/9788572051729

CITATIONS
0

READS
6

2 authors:

Nathalia Patrício
University of São Paulo
14 PUBLICATIONS **6** CITATIONS
SEE PROFILE

Edison Spina
University of São Paulo
38 PUBLICATIONS **8** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

QoS Control Heterogeneous Networks View project

CEST - Centro de Estudos Sociedade e Tecnologia View project

All content following this page was uploaded by Nathalia Patrício on 23 August 2017.

The user has requested enhancement of the downloaded file.

DEBATENDO CRIPTOGRAFIA EM FACE AO MARCO CIVIL DA INTERNET

Nathalia Sautchuk Patrício, Edison Spina[22]

Resumo: Este artigo debate a questão do uso da criptografia e suas limitações em face ao Marco Civil da Internet e seu decreto regulamentador. Além disso, explora algumas das controvérsias no debate atual sobre esse tema no Brasil.

Palavras-chave: Segurança da informação, privacidade, Marco Civil da Internet, criptografia.

Abstract: This article aims to debate cryptography use and its limitations in parallel to Marco Civil da Internet and its regulatory decree. In addition, it intends to explore some of the controversies in the current debate about this topic in Brazil.

Keywords: Information security, privacy, Marco Civil da Internet, cryptography.

Introdução

Nos últimos anos, a criptografia tem sido tema de debate em diversos espaços, não mais apenas dentro do círculo de especialistas em segurança da informação. Em muitos desses debates, a criptografia é tratada como a única solução possível para a garantia da privacidade no uso da Internet.

No Brasil, a Lei nº 12.965, conhecida como Marco Civil da Internet, coloca a proteção da privacidade e dos dados pessoais como princípios que disciplinam o uso da Internet no Brasil (BRASIL, 2014, Art. 3º, II, III). Ainda em seus artigos 7º e 8º, diz que o acesso à internet é essencial ao exercício da cidadania e a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet. Vários direitos são assegurados aos usuários tendo em vista os princípios da lei, dentre esses inviolabilidade da intimidade, da vida privada e das comunicações privadas pela Internet e aquelas já armazenadas (salvo por ordem judicial); o não fornecimento a terceiros dos dados pessoais (salvo mediante consentimento livre, expresso e informado); informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção dos dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta, que não sejam vedadas pela legislação e que estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de Internet mediante consentimento expresso; e exclusão definitiva dos dados pessoais que tiverem sido fornecidos a determinada aplicação de Internet, ao término da relação entre as partes.

Até o ano passado, ainda estava em aberto como os direitos expostos no Marco Civil da Internet poderiam ser garantidos na prática. O decreto Nº 8.771 elucidou alguns pontos no que concerne aos padrões de segurança e ao sigilo dos registros, dados pessoais e comunicações privadas. Segundo esse decreto (BRASIL, 2016, Art. 13), os provedores de conexão e de aplicações devem estabelecer controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e privilégios de acesso exclusivo para determinados usuários; devem prever mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros; devem criar

[22] Escola Politécnica da Universidade de São Paulo (EPUSP)

inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado; e devem usar soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

Mesmo com a regulamentação em vigor, ainda permanecem dúvidas se as medidas previstas no decreto serão suficientes para assegurar a privacidade dos usuários. Um dos debates importantes a serem feitos é sobre o real propósito do uso da criptografia, bem como suas limitações, na garantia da privacidade e na proteção dos dados pessoais dos usuários da Internet assegurados através do Marco Civil da Internet e seu decreto regulamentador.

Neste artigo, serão apresentados alguns conceitos de segurança da informação e de criptografia. Depois serão explorados alguns aspectos do Marco Civil da Internet e do seu decreto regulamentador, focando-se no que concerne à segurança da informação e criptografia. É apresentado o debate sobre a questão do uso da criptografia e as controvérsias atuais no cenário brasileiro. Para finalizar são apresentadas algumas considerações finais do trabalho.

Segurança da informação e criptografia

A segurança da informação é um processo em uma organização, que deve considerar a informação tanto no ambiente convencional quanto no ambiente de tecnologia. Uma vez que a utilização da informação acontece pelas pessoas, a segurança também deve ser assegurada por elas. Segundo Fontes (2012) uma definição mais formal para segurança da informação seria o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada.

Diz-se que 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 (STALLINGS E BROWN, 2011). 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 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 (STALLINGS, 2015), sendo que esta última pode ser definida como a garantia de que os indivíduos controlam ou influenciam quais informações sobre eles podem ser coletadas e armazenadas e por quem e para quem tais informações podem ser reveladas (STALLINGS E BROWN, 2011). Sendo assim, a privacidade, além de abranger a confidencialidade de dados, também envolve as políticas de uso por usuários autorizados. Já 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 (STALLINGS, 2015).

Segundo Tanembaum e Wetherall (2011), com exceção da segurança na camada física, quase toda a segurança da informação se baseia em princípios criptográficos. A palavra criptografia vem de palavras gregas que significam "escrita secreta". De acordo com Stallings (2015), os muitos esquemas utilizados para a encriptação constituem a área de estudo conhecida como criptografia.

De acordo com Tanembaum e Wetherall (2011), as mensagens a serem criptografadas, conhecidas como texto simples, são transformadas por meio de uma função parametrizada por uma chave. Em seguida, a saída do processo de criptografia, conhecido como texto cifrado, é transmitida. Stallings (2015) diz que o processo de converter um texto claro em um texto cifrado é conhecido como cifração ou encriptação, enquanto que restaurar o texto claro a partir do texto cifrado é decifração ou decriptação.

Stallings (2015) afirma que não existe algoritmo de encriptação que seja incondicionalmente seguro. O que se pode obter é um esquema de encriptação considerado computacionalmente seguro, em que o algoritmo atende a pelo menos um dos critérios: (1) o custo para quebrar uma cifra ultrapassa o valor da informação encriptada e (2) o tempo exigido para quebrar a cifra supera o tempo útil da informação.

Apesar do que se possa pensar inicialmente, Tanembaum e Wetherall (2011) enfatizam o caráter não sigiloso do algoritmo de encriptação a ser utilizado. A estratégia, conhecida como segurança pela obscuridade, em que se tenta manter o algoritmo secreto, não é aconselhada. Ao tornar o algoritmo público, inúmeros criptólogos podem tentar decodificar o sistema e caso muitos tenham tentado isso durante cinco anos após a sua publicação e nenhum tenha conseguido, há uma grande probabilidade de que o algoritmo seja sólido (TANEMBAUM E WETHERALL, 2011). Na verdade, o sigilo deve estar na chave, e seu tamanho é uma questão muito importante no projeto de um algoritmo de encriptação.

Segundo Stallings (2015) os algoritmos criptográficos são caracterizados em relação a três dimensões. Uma das mais conhecidas é quanto ao número de chaves usadas no processo: se tanto o emissor quanto o receptor utilizarem a mesma chave, o sistema é considerado de encriptação simétrica; já se emissor e receptor usarem chaves diferentes, o sistema é considerado de encriptação assimétrica ou de chave pública. Outra dimensão diz respeito ao tipo de operações usadas para transformar o texto claro em texto cifrado. Todos os algoritmos de encriptação são baseados em dois princípios gerais: substituição, em que cada elemento no texto claro é mapeado em outro elemento, e transposição em que os elementos no texto claro são rearranjados. Por último, há o modo em que o texto claro é processado. Quando há um processamento de uma entrada de um bloco de elementos de cada vez, produzindo um de saída para cada de entrada, há uma cifra de bloco. Já se os elementos de entrada são processados continuamente, proporcionando a saída de um elemento de cada vez, a cifra é de fluxo.

Com o advento de aplicativos de comunicação via celular, o uso de algoritmos criptográficos migrou para essa plataforma a fim de garantir uma comunicação sigilosa ponta a ponta. Nesse cenário, há um grande desafio que é a distribuição segura das chaves através da Internet. Segundo Stallings (2015), a força de qualquer sistema criptográfico está na técnica de distribuição de chave, um termo que se refere aos meios de entregar uma chave a duas partes que querem trocar dados, sem permitir que outros vejam a chave. Isso porque para que a encriptação simétrica funcione, as duas partes precisam compartilhar a mesma chave, que precisa ser protegida contra o acesso por outras partes sem permissão.

A distribuição de chave pode ser feita de várias maneiras, sendo que o uso de um centro de distribuição de chaves (CDC) tem sido bastante adotado (STALLINGS, 2015). Ele é responsável por distribuir chaves a pares de usuários conforme a necessidade. Cada usuário precisa compartilhar uma chave exclusiva com o CDC, para fins de distribuição delas. De acordo com Stallings (2015), a utilização de um CDC é baseado no uso de uma hierarquia de chaves com, no mínimo, dois níveis de chaves. A comunicação entre as pontas é encriptada usando uma chave temporária, normalmente referenciada como uma chave de sessão, que normalmente, é usada pela duração de uma conexão lógica e depois descartada. Cada chave de sessão é obtida a partir do CDC, transmitidas em formato encriptado, usando uma chave mestra exclusiva que é compartilhada pelo centro e o usuário final (STALLINGS, 2015). Pode-se adicionar mais um nível na hierarquia de chaves, em que a encriptação de chave pública é usada apenas para atualizar a chave mestra entre um usuário e o CDC. O acréscimo dessa camada oferece um meio seguro e eficiente de distribuir chaves mestras.

Marco civil da Internet

Segundo Solagna (2015) a proposta do Marco Civil da Internet nasceu como uma reação à tendência criminalizante no tratamento de diversos comportamentos na Internet e na Web que se apresentava no projeto de lei 89/2003. Esse projeto de lei, que era um agregado de outras iniciativas legislativas com o objetivo de modificar o código penal para tipificar "crimes cibernéticos", gerou um projeto substitutivo de autoria do deputado Eduardo Azeredo que foi reapresentado em 2006.

Desde o início, a proposta do Marco Civil da Internet se baseou em diversos fundamentos, tais como a liberdade de expressão, os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais, a pluralidade e a diversidade, a abertura e a colaboração, a livre iniciativa, a livre concorrência e a defesa do consumidor e a finalidade social da rede (BRASIL, 2014).

Vários princípios que disciplinam o uso da Internet também foram reconhecidos na lei, dentre os quais destacam-se a proteção da privacidade, proteção dos dados pessoais, e a preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas (BRASIL, 2014). Esses princípios têm relação direta com a área de segurança da informação, uma vez que as práticas dessa área podem ajudar a promovê-los.

A questão tecnológica das salvaguardas para a segurança da informação aparece claramente no decreto regulamentador. O artigo 13 fala explicitamente que os provedores de conexão e de aplicações devem observar algumas diretrizes sobre padrões de segurança, como controle de acesso aos dados de usuários com uso de mecanismos de autenticação, inventário dos acessos aos dados e a garantia da inviolabilidade dos dados através de uso de soluções como encriptação (BRASIL, 2016, Art. 13).

A controvérsia no uso de criptografia

Na última década, observa-se uma maior facilidade com que os governos podem espionar seus cidadãos e também de como os cidadãos podem impedir tais atos de espionagem através do uso da criptografia (TANEMBAUM E WETHERALL, 2011). Por exemplo, qualquer pessoa que instale o PGP e que utilize uma chave bem protegida pode ter certeza que ninguém poderá ler as mensagens de seu correio eletrônico, com ou sem mandado de busca. Os governos não apreciam essa possibilidade de uma privacidade real, através da qual é muito mais difícil seus agentes espionarem criminosos de todos os tipos, mas também é muito mais difícil fazer o mesmo com jornalistas e adversários políticos (TANEMBAUM E WETHERALL, 2011). Como resultado, alguns governos já tentaram restringir ou proibir o uso de criptografia em algum momento de sua história.

Segundo Tanembaum e Wetherall (2011), antes de 1999, toda criptografia na França era proibida, a menos que o governo recebesse as chaves. Já o governo dos Estados Unidos, em abril de 1993, anunciou sua intenção de criar um criptoprocessador em hardware, que seria o padrão para todas as comunicações em rede de forma a garantir a privacidade dos cidadãos. Porém, esse processador forneceria ao governo a possibilidade de decodificar todo tráfego por meio de um esquema chamado custódia de chaves, que permitia o acesso do governo a todas as chaves, através da alegação de que a espionagem só aconteceria quando tivesse um mandado de busca válido. O resultado foi uma enorme agitação, com os defensores da privacidade denunciando todo o plano e os promotores de justiça elogiando o esquema. Por fim, o governo voltou atrás e descartou a ideia (TANEMBAUM E WETHERALL, 2011).

Atualmente a criptografia está no centro de uma polêmica no Brasil. Em um caso recente, o aplicativo WhatsApp teve seu funcionamento suspenso no país devido ao descumprimento de ordem judicial de fornecimento de dados à Justiça. A empresa diz não poder fornecer os dados requeridos devido a utilização da criptografia ponta a ponta, que foi brevemente explicada no item 2 deste artigo. Nesse caso, o WhatsApp funciona como um CDC.

Segundo Alves (2016), a juíza exigiu "a desabilitação da chave de criptografia", alegando, inclusive, não ser possível a prestação de serviços de comunicação digital no mercado brasileiro que impeçam a efetividade da Justiça criminal. Esse caso trouxe à tona um debate sobre a legalidade do uso da criptografia no Brasil. Por um lado, o próprio decreto regulamentador do Marco Civil da Internet coloca a criptografia como uma das técnicas a serem utilizadas para garantir a inviolabilidade dos dados, por outro, com base na mesma lei, uma juíza questiona seu uso, citando-na como impeditivo para o cumprimento das medidas judiciais necessárias.

Nesse cenário, o STF convocou uma audiência pública para tratar a questão da criptografia do WhatsApp, colocando as seguintes questões a serem respondidas por especialistas:

1. Em que consiste a criptografia ponta a ponta (end to end) utilizada por aplicativos de troca de mensagens como o WhatsApp?
2. Seria possível a interceptação de conversas e mensagens realizadas por meio do aplicativo WhatsApp ainda que esteja ativada a criptografia ponta a ponta (end to end)?
3. Seria possível desabilitar a criptografia ponta a ponta (end to end) de um ou mais usuários específicos para que, dessa forma, se possa operar interceptação juridicamente legítima?
4. Tendo em vista que a utilização do aplicativo WhatsApp não se limita a apenas uma plataforma (aparelhos celulares/smartphones), mas permite acesso e utilização também em outros meios, como, por exemplo, computadores (no caso do WhatsApp mediante o WhatsApp Web/Desktop), ainda que a criptografia ponta a ponta (end to end) esteja habilitada, seria possível "espelhar" as conversas travas no aplicativo para outro celular/smartphone ou computador, permitindo que se implementasse ordem judicial de interceptação em face de um usuário específico?

   (SUPREMO TRIBUNAL FEDERAL, 2016)

A controvérsia no uso da criptografia ainda está longe de estar finalizada. Por um lado, os aplicadores de lei desejam formas de ter acesso a informações de suspeitos de crimes para constituir provas de suas ações. Por outro lado, os técnicos e os ativistas em direitos humanos chamam atenção para o perigo na criação de formas de "burlar" os mecanismos de criptografia de sistemas, criando algo conhecido como backdoors.

Para aquecer ainda mais esse debate, recentemente, Tobias Boelter, um pesquisador da área de segurança da informação da Universidade de Berkeley, divulgou a existência de uma vulnerabilidade, através da qual, terceiros ou mesmo a empresa WhatsApp poderiam ter acesso às mensagens trocadas entre dois usuários, no caso de retransmissão de mensagens quando o destinatário está offline (TOBIAS BOELTER'S BLOG, 2016). O jornal The Guardian noticiou que se tratava da existência de uma backdoor no aplicativo (The Guardian, 2017). Com isso, abre-se margem ao questionamento do argumento usado pela empresa para não fornecer dados a Justiça brasileira, já que o algoritmo criptográfico descrita pela seu Technical White Paper (WHATSAPP, 2016) pode não estar corretamente implementado, contendo brechas na segurança que podem ser exploradas. Várias entidades e pesquisadores da área de criptografia se posicionaram contra a versão de que essa vulnerabilidade seria uma backdoor, inserida de forma proposital pela empresa WhatsApp, esclarecendo que se tratava de um "*trade-off*" para que o aplicativo tivesse uma boa usabilidade (ELECTRONIC FRONTIER FOUNDATION, 2017; OPEN WHISPER SYSTEMS, 2017, TECHNOSOCIOLOGY, 2017). Além disso, foi enfatizado de que a "interceptação" das mensagens só pode ser feita em um caso muito específico (de retransmissão pelo fato do destinatário estar offline) e que a falha não é fácil de ser reproduzido por usuários que não sejam especialistas em criptografia.

Considerações finais

O Marco Civil da Internet é uma lei que estabeleceu vários princípios para o uso da Internet no Brasil, dentre eles a privacidade dos usuários. Apesar de não citar nominalmente a questão da segurança da informação pode-se estabelecer paralelos entre a lei e essa área.

Como Tanembaum e Wetherall (2011) deixam claro em seu livro, quase toda a segurança da informação se baseia em princípios criptográficos. Por isso, a criptografia tem sido vista como uma das formas para assegurar a privacidade dos usuários na Internet, inclusive sendo citada em seu decreto regulamentador.

Apesar disso, ainda há muito debate em relação ao seu uso no Brasil, especificamente no caso do WhatApp apresentado neste artigo. Muito se deve ao desconhecimento de como funcionam os algoritmos criptográficos, o que se tentou esclarecer brevemente. Mas há também uma vertente mais antiga desse debate, que acaba se estendendo para o ambiente virtual, que é a da aparente dicotomia entre segurança e privacidade, pois muitos juristas argumentam de que não é possível ter segurança se houver privacidade total das pessoas. Porém, muitos ativistas colocam que a privacidade também é um modo de garantia de segurança dos indivíduos e que esse argumento pode ser usado para que os governos instalem programas de vigilância em massa de seus cidadãos com a cooperação de grandes empresas, hoje detentoras de grande quantidade de dados. A grande questão que fica é se é possível atingir um ponto de equilíbrio entre a segurança e a privacidade. Enquanto isso, esse debate promete continuar no Brasil.

Referências bibliográficas

ALVES, F. M. **Representação criminal e bloqueio de aplicativo**. 2016. Disponível em: <http://omci.org.br/jurisprudencia/115/representacao-criminal-e-bloqueio-de-aplicativo/ >. Acessado em: 30 out. 2016.

BRASIL. **Lei Nº 12.965, de 23 de abril de 2014**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acessado em: 30 out. 2016.

BRASIL. **Decreto Nº 8.771, de 11 de maio de 2016**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm >. Acessado em: 30 out. 2016.

ELECTRONIC FRONTIER FOUNDATION. **Google Launches Key Transparency While a Trade-Off in WhatsApp Is Called a Backdoor**. 14 jan 2017. Disponível em: < https://www.eff.org/deeplinks/2017/01/google-launches-key-transparency-while-tradeoff-whatsapp-called-backdoor >. Acessado em 29 jan. 2017.

FONTES, E. **Políticas e Normas para a Segurança da Informação**. Rio de Janeiro: Brasport, 2012.

HOEPERS, C.; FAULHABER, H.; STEDING-JESSEN, K. (Orgs.). **Combate ao spam na Internet no Brasil: Histórico e reflexões sobre o combate ao spam e a gerência da porta 25 coordenados pelo Comitê Gestor da Internet no Brasil**. São Paulo, 2015. Disponível em: < http://www.cgi.br/publicacao/combate-ao-spam-na-internet-no-brasil-historico-e-reflexoes-sobre-o-combate-ao-spam-e-a-gerencia-da-porta-25-coordenados-pelo-comite-gestor-da-internet-no-brasil/ >.

OPEN WHISPER SYSTEMS. **There is no WhatsApp 'backdoor'**. 13 jan. 2017. Disponível em: < https://whispersystems.org/blog/there-is-no-whatsapp-backdoor/ >. Acessado em 29 jan. 2017.

SOLAGNA, F. **A formulação da agenda e o ativismo em torno do Marco Civil da Internet**. 2015.

Supremo Tribunal Federal. **Ministro Fachin convoca audiência pública para debater bloqueios judiciais do WhatsApp.** Disponível em:

<http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=328600>. Acessado em: 17 dez. 2016.

STALLINGS, W. **Criptografia e Segurança de Redes: Princípios e Práticas** – 6ª edição. São Paulo: Pearson. 2015. ISBN 978-8543005898.

STALLINGS, W.; BROWN, L. **Computer Security Principles And Practice** - 2nd edition. Prentice-Hall, ISBN: 0-13-277506-9. 2011.

TANENBAUM, A. S.; WETHERALL, D. **Redes de Computadores** - 5ª Edição. São Paulo: Pearson. 2011. ISBN 857605924X.

TECHNOSOCIOLOGY. **In Response to Guardian's Irresponsible Reporting on WhatsApp: A Plea for Responsible and Contextualized Reporting on User Security**. Disponível em:< http://technosociology.org/?page_id=1687 >. Acessado em 29 jan. 2017.

TOBIAS BOELTER'S BLOG. **WhatsApp Retransmission Vulnerability**. 16 abril de 2016 Disponível em: < https://tobi.rocks/2016/04/whats-app-retransmission-vulnerability/ >. Acessado em: 29 jan. 2017.

THE GUARDIAN. **WhatsApp vulnerability allows snooping on encrypted messages**. 13 jan. 2017. Disponível em: < https://cdn.ampproject.org/c/s/amp.theguardian.com/technology/2017/jan/13/whatsapp-backdoor-allows-snooping-on-encrypted-messages >. Acessado em: 29 jan. 2017.

WHATSAPP. **WhatsApp Encryption Overview – Technical White Paper**. 17 nov. 2016. Disponível em: < https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf >. Acessado em: 27 jan. 2017.

View publication stats