OS DILEMAS DA CRIPTOGRAFIA DE MENSAGENS NA INTERNET

The Dilemmas of Internet Encryption

Glaydson de Farias Lima[1]

RESUMO: A recente popularização dos modernos dispositivos informáticos, em especial dos *smartphones,* permitiu acesso de milhões de brasileiros às poderosas ferramentas capazes de realizar instruções complexas. Nesse artigo é analisada a criptografia nas mensagens trocadas para comunicação e como o uso de tal tecnologia inviabiliza ordens judiciais de quebra de sigilo. Oferece-se um estudo inicial sobre a origem do uso da criptografia de dados, suas utilidades e mecanismos alternativos para permitir que informações trocadas por criminosos sejam identificadas pelas autoridades, apontando, contudo, as consequências que tais medidas podem trazer à coletividade. Também são debatidas as vertentes que tratam da competência jurisdicional no direito internacional que se aplicam ao caso desses aplicativos, identificando as vantagens e desvantagens de cada posição.

Palavras-chaves: Internet; criptografia; *Whatsapp*; mensagens; digital.

ABSTRACT: *The recent popularization of modern computing devices, especially smartphones, has allowed millions of Brazilians access to powerful tools capable of performing complex instructions. This article analyses the cryptography in the messages exchanged by modern applications of communication and how the use of such technology obstructs court orders of breach of confidentiality. An initial study is offered about cryptography of data, its utilities and alternative mechanisms to allow exchanged information by criminals to be identified by the designated authorities, however, the consequences that the aforementioned measures might bring to the collectivity. It also discusses the aspects dealing with jurisdiction in international law that apply to the case of these applications, identifying the advantages and disadvantages of each position.*

Keywords: *Internet, encryption, Whatsapp, messages, digital.*

[1] Bacharel em Direito e Informática pela Universidade de Fortaleza - UNIFOR. Pós-graduado no MBA em Gestão de Negócios oferecido pelo IBMEC/BOVESPA. É advogado participante da Comissão de Direito da Tecnologia da Informação da OAB/CE. Membro da Associação de Peritos em Computação Forense – APECOF. Autor do livro "Manual de Direito Digital: Fundamentos, legislação e jurisprudência" (Editora Appris/2016). E-mail glaydson@gmail.com.

INTRODUÇÃO

A resistência das empresas desenvolvedoras dos modernos aplicativos de comunicação em acatar ordens judiciais para o fornecimento de dados tem como principal fundamento técnico a utilização da criptografia. As companhias alegam que nem mesmo elas teriam acesso às informações, pois, enquanto os dados estão em seus servidores, ficam protegidos, sendo possível somente aos pares da comunicação a sua visualização.

Criado o impasse com a ordem judicial para quebra de sigilo de dados e a alegada impossibilidade de executá-la, vários juízes têm decidido pelas sanções previstas no artigo 12 do Marco Civil da Internet (advertência, multa, bloqueio temporário e proibição permanente). Tais sanções são derivadas do não respeito ao artigo 11 da referida lei que estipula:

> *Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.*[2]

Entretanto, esses modernos aplicativos de troca de mensagens são desenvolvidos em escala mundial, sujeitos à legislação brasileira, bem como de todos os países onde seja possível seu uso, ocasionando uma série de dilemas para seus desenvolvedores e para aqueles que necessitam fazer valer as ordens legais. Este artigo trata desses dilemas, mas, inicialmente, é necessário esclarecer o que é criptografia, quais seus usos e limites.

CRIPTOGRAFIA

Há milhares de anos a humanidade usa a criptografia como meio para codificar mensagens e não permitir que terceiros tenham acesso ao seu conteúdo. Como destaca Marcacini, a utilização da criptografia é bem mais antiga do que se imagina:

---

[2] 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. Acesso em: 11 dez 2016.

> *Considera-se que a criptografia seja tão antiga quanto a própria escrita. Há indícios de que, na Antiguidade, foi conhecida no Egito, Mesopotâmia, Índia e China, mas não se sabe bem qual foi sua origem, e pouco se sabe acerca de seu uso nos primórdios da História.*[3]

Segredos de guerra ou industriais já foram protegidos por esse sistema que vem se desenvolvendo para manter as informações disponíveis apenas ao remetente e ao destinatário das mensagens mesmo que elas sejam interceptadas por terceiro (um soldado inimigo ou um concorrente industrial, por exemplo).[4]

Se um soldado levava uma mensagem criptografada por dezenas de localidades que poderiam conter tropas inimigas, também ocorre algo semelhante na Internet, pois uma informação enviada por um usuário passa por uma boa quantidade de dispositivos eletrônicos até encontrar o destinatário. O primeiro risco pode estar na rede *Wi-Fi* disponibilizada em um café, até as dezenas de servidores por onde uma mensagem trafega.

Desta forma, quer sejam mensagem transportadas no início da história escrita ou nos modernos equipamentos que temos hoje, é necessário que os dados sejam codificados para que se evite interceptação indevida.

Marcacini relata uma das primeiras formas de criptografia que se tem conhecimento:

> *Na Roma antiga, Júlio César utilizava um método para cifrar sua correspondência, pelo qual cada letra do texto era substituído pela terceira subsequente no alfabeto. Ou seja, para enviar uma mensagem com os dizeres "ENCONTRO CONFIRMADO PARA DOMINGO", mediante o cifrado de Júlio César o texto seria escrito assim: "HQFRQWUR FRQILUPDGR SDUD GRPLQJR".*[5]

Evidente que este modelo de criptografia rudimentar seria facilmente identificável pelos sistemas atuais. Contudo, podemos propor um sistema ainda mais simples onde as mensagens seriam codificadas com a substituição das letras pelas seguintes do alfabeto. Dessa forma, se João deseja enviar a mensagem "Venha para minha casa amanhã" para Maria, ele o transformaria em "*Wfoib qbsb njoib dbtb bnboib*". Caberia ao destinatário, sabendo da forma de

---

[3] MARCACINI, Augusto. *Direito e Informática: uma abordagem jurídica sobre a Criptografia*. Lulu. Com, 2010, p. 19.
[4] Idem.
[5] Id., p. 20.

codificação utilizada, reconverter para a mensagem original, modificando cada letra pela sua exata antecessora.

Por sua vez, o interceptador da mensagem tentaria procurar padrões que permitissem quebrar a criptografia para ter acesso ao seu conteúdo, pois, se a codificação é realizada da mesma forma para todos os usuários, bastaria verificar algumas características da língua[6], identificar sequências e obter as regras para conseguir a operação inversa para remontar a mensagem original (descriptografia).

Para evitar esse tipo de ataque houve a criação de sistemas mais complexos e, dentre eles, há o que se utiliza de criptografia ponta a ponta, que consiste em modelos específicos para cada par de remetente e destinatário, permanecendo os dados protegidos enquanto ficam nos servidores da empresa desenvolvedora. Ou seja, não há uma fórmula única que transcreva todas as mensagens em determinado ambiente e sim uma regra que muda para cada par de comunicação realizada.

É esse o sistema utilizado por aplicativos como o *Whatsapp* e o *Telegram,* em que nem mesmo os desenvolvedores têm acesso ao conteúdo.

Importante destacar que a criptografia dos dados enquanto estão nos servidores das empresas não é requisito indispensável para criação desses aplicativos. Poderia ser utilizado o modelo de *e-mail* onde a criptografia existe na comunicação, preservando o sigilo dos dados nestes momentos mais importantes, mas não existindo quando os dados estão guardados nos servidores.[7] A criptografia da forma que é aplicada nos aplicativos em debate é uma escolha dos desenvolvedores. Nesse ponto, iniciam os dilemas de seu uso.

COMPETÊNCIA JURISDICIONAL

A internet é um sistema que liga várias pequenas redes de dispositivos informáticos em uma gigante e complexa plataforma que une, a princípio, todos os pontos no planeta.

---

[6] Por exemplo, em línguas algumas letras aparecem mais ou certas combinações são impossíveis.

[7] É possível criar mecanismo que deixam as mensagens criptografadas nos *e-mails* utilizando de alguns *softwares adicionais, contudo não é a forma padrão de uso*.

José de Oliveira Ascensão alerta sobre as consequências da popularização da internet nas questões jurídicas:

> *(...) a sociedade da informação acarreta consigo uma vertente inevitável de internacionalização. Particularmente, a interconexão de redes tornará aberta a penetração em estados estrangeiros. Mas isso traz grandes problemas jurídicos, dada a diversidades das leis.*[8]

Neste mecanismo global que conecta pessoas de diferentes partes do mundo há questões importantes para desvendar a competência jurisdicional aplicável para solução de conflitos. Wilson Furtado Roberto dividiu em duas correntes: a implantação do modelo denominado *international cyberlaw* e a utilização das normas e princípios do direito internacional privado.[9]

Na proposição da *international cyberlaw,* dada sua característica de rede global, não haveria a possibilidade da utilização das leis dos Estados conforme explica Wilson:

> *A analogia com o Direito Marítimo Internacional (Admiralty Law), própria dos países anglo-saxões, é clara, da forma que se cria uma normativa material para um espaço, as águas internacionais, sobre as quais nenhum Estado reclama soberania. Da mesma forma, o ciberespaço estaria à margem da soberania dos Estados, pois, para o exercício da soberania, é essencial o controle sobre as coisas e as pessoas que é de competência do Estado soberano. Como seria difícil o exercício da soberania pelos Estados, o ciberespaço seria um espaço próprio para elaboração de uma normativa material ad hoc, que não coincidiria com a lei estadual de nenhum país em concreto.*[10]

A lei global seria baseada pelos costumes da rede e com forte força de características implantadas por desenvolvedores, o que levaria a problemas óbvios para os Estados soberanos como afirma o autor:

> *A internet cyberlaw causa também um problema de soberania. Aceitar sua existência supõe aceitar simples e facilmente que os usuários da internet, ou melhor, as empresas dominantes do setor, adquiram poder soberano no ciberespaço, de modo que são os que podem legislar e produzir normas para regular o mundo virtual da internet.*[11]

---

[8] ASCENSÂO, José de Oliveira. E agora? Pesquisa de um futuro próximo. *In: Direito da Sociedade da Informação.* Coimbra: Coimbra, 1999, p. 03.

[9] ROBERTO, Wilson Furtado. *Dano transnacional e internet: Direito aplicável e competência internacional*. Curitiba: Juruá Editora, 2010.

[10] Ibidem. p. 32.

[11] Ibidem. p. 37.

Por sua vez, a aplicação de normas de direito internacional privado permite que sejam determinadas quais normas devem ser aplicadas em casos onde o autor de um ilícito esteja localizado em um país, a vítima em outro e os dados numa terceira nação. Consolidou a jurisprudência internacional que o Estado competente é aquele onde ocorreu o efeito do dano.

No caso de ilícitos que se utilizam dos aplicativos mencionados onde tanto autores de ilícitos como as vítimas estejam localizados no Brasil, torna-se uma questão clara que a justiça brasileira tem a competência para julgar, especialmente, no caso onde as empresas desenvolvedoras também possuem escritório no país. Porém, a questão é como definir a solução racional, analisando todos os aspectos técnicos e resultados práticos, para algo que é aplicável em todo o mundo.

DILEMAS DOS DESENVOLVEDORES

Aplicativos de comunicação de massa como *Whatsapp* permitem que mensagens sejam enviadas de um usuário ao outro, mesmo que o destinatário não esteja conectado. Para isso, necessita-se que um banco de dados guarde as informações até que, pelo menos, sejam recebidas.

Dada a popularidade dessas aplicações, o volume de dados é gigante, com o consequente alto custo para armazená-lo. As empresas, por si só, ponderam que tipo de informação deve ser guardada e por quanto tempo na sua visão comercial da operação é razoável.

A princípio, os dados do *Whatsapp* são apagados assim que lidos pelo destinatário, já no caso do *Telegram* ficam guardados, podendo ser acessados mesmo com aquisição de novos aparelhos.

Entretanto, empresas controladoras que tenham sede no Brasil devem se sujeitar à legislação nacional (cf. CPC, art. 21, parágrafo único e Marco Civil da Internet, art. 11, § 2º). Dessa forma, como são disponibilizados em escala mundial, devem respeitar a legislação brasileira, norte-americana, francesa, angolana, chinesa, dinamarquesa.

A possibilidade de adaptar seus aplicativos em escala mundial com regras específicas para cada Estado poderia impedir a comunicação entre pessoas em

diferentes territórios pois, pode uma lei de um país exigir a criptografia de dados, enquanto outro proibir tal função.

Começam aí os desafios para empresas que se dispõem a fornecer serviços de mensagens. O primeiro ponto é encontrar um núcleo comum e tentar arcar com as consequências da não obediência a determinados termos como no caso da guarda solicitada pelo MCI. Outra questão é que a criptografia permite a segurança das informações de todos os usuários, não só da invasão indiscriminada de Estados como do próprio acesso por *crackers.*

Nessa última situação, se os dados não fossem criptografados e as mensagens permanecessem nos servidores dos aplicativos por longo tempo, invasores poderiam ter acesso a um vasto histórico de conversação dos usuários permitindo que, por exemplo, pudessem ser extorquidos para que as mensagens não fossem disponibilizadas em público, gerando ainda um risco jurídico das empresas de serem acionadas por seus clientes. Também, como já abordado, a falta de criptografia permitiria que mensagens pudessem ser interceptadas por terceiros, mesmo em redes públicas com acesso *Wi-Fi.*

Não há, portanto, uma vontade dirigida de desrespeitar a legislação brasileira, como aparentemente pode parecer quando da alegação de uso de criptografia para não fornecimento às solicitações judiciais. Há uma razão para preservação da segurança das informações dos usuários que, na maioria das vezes, as utilizam para atividades lícitas. Caso a funcionalidade não existisse, os dados estariam em risco de serem interceptados por estranhos.

Evidente que a utilização de criptografia permite que uma série de atividades ilícitas seja realizada na *Internet* com a dificuldade de obtenção dessas informações por parte das autoridades.

Uma saída sugerida para preservação do sigilo da maioria dos usuários e controle da sociedade sobre atos ilícitos seria a interrupção da criptografia das comunicações entre pares, por ordem judicial, a partir de um determinado momento. Conforme ocorre na telefonia, o juiz só teria acesso ao conteúdo trocado em determinado lapso de tempo e a partir de sua solicitação.

A ideia, tecnicamente possível, permitiria a proteção de imensa maioria dos usuários que se utilizam para fins lícitos, mantendo o sigilo de seus dados e só atingiria uma minoria de criminosos.

Outra sugestão apontada seria a instalação de um *backdoor* nos aplicativos para que a autoridade judicial tenha acesso às mensagens do remetente ou destinatário. Afinal, antes do envio e após o recebimento, as mensagens ficam abertas para leitura pelos pares da comunicação. Se o desenvolvedor tem acesso a todos as funcionalidades, poderia criar tal acesso com a leitura do que é apresentado na tela de seus usuários. Entretanto, tal procedimento, apesar de possível, traz um enorme risco a toda rede de informações.

Ressalta-se que *backdoor* é um conceito informático, cuja aplicação abre um acesso não autorizado de terceiro e está fortemente ligado às atividades ilícitas.[12] Dessa forma, se o próprio desenvolvedor oferece esse tipo de caminho, mesmo sob ordem judicial, abre-se uma brecha para um nível de acesso possível de ser utilizado por invasores. Novamente, para conseguir identificação de informações sobre atividades criminosas, cria-se um risco em potencial para todos os usuários do sistema.

Ainda existe o dilema de identificar qual lei seria justa e qual seria o precedente aberto. Explico: na maioria dos casos com pedido de bloqueio do *Whatsapp* no Brasil havia a investigação de casos graves de organização criminosa e rede de distribuição de material contendo pornografia infantil. A princípio, não há que se discutir que tais ações são de interesse da sociedade brasileira e os esforços realizados pelas autoridades com fim de identificar e punir tais criminosos são legítimos.

Mas imaginemos que o grupo controlador do *Whatsapp* fornecesse tais dados sobre possíveis membros de uma organização criminosa para a justiça brasileira. Posteriormente, um governo totalitário requisitaria as informações de uma organização que luta pela democracia, afinal, na visão desse Estado, ela seria criminosa. Depois, seguindo os precedentes, um terceiro país dominado por uma legislação fundamentalista religiosa faria a requisição de informações de troca de mensagens de casais homossexuais ou de uma mulher que foi acusada de não usar um véu em determinada situação que os fariam ser executados. Quem está certo? Como ficaria a imagem das empresas em relação à entrega

[12] LIMA, Glaydson de Farias. *Manual de Direito Digital: Fundamentos, Legislação e Jurisprudência*. Curitiba: Appris, 2016, p. 87.

de pessoas que, segundo parte de uma visão ocidental, lutariam por razões legítimas? Que leis são justas?

Portanto, existe uma série de dilemas que precisam ser discutidos pela sociedade. Além disso, demonstra que o interesse das empresas em fornecer mecanismos de proteção de dados de seus usuários não se trata de uma atitude direcionada a desafiar qualquer ordem jurídica. É uma questão bem mais complexa.

DILEMAS DAS AUTORIDADES

Devido à popularidade dessas aplicações modernas, elas também são utilizadas para atividades ilícitas. Identificados pelas autoridades como possíveis meios de prova para punição de criminosos, passam a ser alvo de investigações criminais.

Respeitando a ordem estabelecida pelo Marco Civil da Internet, o juiz solicita às empresas controladoras informações com envio advertência (art. 12, I). Tal requisição é negada. Posteriormente, é aplicada multa de até 10% sobre o faturamento (art. 12, II) sem que, novamente, as informações sejam fornecidas. Pela escala legal a próxima sanção é a suspensão temporária (art. 12, III) que aconteceu algumas vezes com o bloqueio do *Whatsapp* durante algumas horas.

No momento que um determinado aplicativo popular é bloqueado em todo território nacional ele passa a interferir na vida social e comercial de milhões de pessoas. Inicialmente, parece ferir o princípio da proporcionalidade que uma ação que envolva uma pequena parcela da população crie impedimento para um grupo imensamente maior. Entretanto, qual seria outra saída dada aos juízes?

O bloqueio temporário das atividades poderia gerar a migração de um determinado aplicativo para um concorrente e poderia ter até mais força que a própria multa sob o faturamento, já que a expectativa de receita futura é uma moeda mais valiosa para as empresas do que a auferida no presente.

Porém, depois das experiências recentes, não se conseguiu visualizar a migração para serviços de terceiros. Nos momentos do bloqueio do *Whatsapp* foi possível verificar uma migração temporária para concorrentes. Desfeita a proibição, os usuários retornaram ao aplicativo penalizado.

Resta, por fim, a última sanção prevista no art 12 do Marco Civil da Internet: a proibição do exercício das atividades que poderia ser feito com o bloqueio total nas bases realizadas quando da interrupção temporária, como utilizado por países totalitários.

Uma possível sanção final realizada no *Whatsapp* resultaria numa migração definitiva, possivelmente para o *Telegram*. Acontece que esse último aplicativo, diferente do primeiro, não tem sede no Brasil e possui sistema de criptografia bem mais apurado do que o popular concorrente. Ou seja, tal decisão não teria nenhuma consequência prática para a sociedade e levaria ao bloqueio definitivo de mais um aplicativo com criptografia até ser substituído por um terceiro, por um quarto.

Evidente que as autoridades brasileiras enfrentam esses aplicativos com objetivo de proteger a sociedade de criminosos. Entretanto, mesmo se utilizando da legislação específica, não conseguem obter os resultados que almejam.

Tribunais têm decidido que o bloqueio temporário de aplicativos não se constitui uma alternativa proporcional, uma vez que penaliza milhões de pessoas inocentes.[13] A possível saída seria a aplicação de penas pecuniárias maiores que, todavia, não tem conseguido surtir efeito, pois os grandes conglomerados que dominam a internet como *Facebook, Google, Apple* e *Microsoft* possuem reservas financeiras maiores que países tradicionais.[14]

Qual seria então a solução jurídica para cumprimento dessas ordens já esclarecidas as questões técnicas anteriormente citadas? São esses dilemas jurídicos que preocupam as autoridades legais brasileiras.

CONCLUSÃO

Dentro desse emaranhado tecnológico e jurídico é preciso se utilizar da legislação e dos princípios constitucionais dos Estados democráticos de direito para tentar buscar uma solução para estes modernos dilemas. Aplicativos de mensagens foram desenvolvidos com criptografia para proteger a imensa

[13] Neste sentido: Mandado de Segurança nº 201600110899 TJ-SE.

[14] TI INSIDE. *Apesar de ter a maior reserva de caixa, Apple é a empresa de tecnologia mais endividada.* Disponível em: <http://convergecom.com.br/tiinside/07/05/2015/apesar-de-ter-a-maior-reserva-de-caixa-apple-e-a-empresa-de-tecnologia-mais-endividada/>. Acesso em: 11 dez. 2016.

maioria dos usuários que se utilizam para atividades lícitas. Se há excesso por parte de um grupo que se utiliza dos meios para coordenar atividades criminosas é uma consequência natural de qualquer invenção realizada pelo ser humano.

A *international cyberlaw* e as normas de direito internacional privado não trazem soluções definitivas para as questões abordadas. A primeira solução falha em propor uma ideia demasiadamente abstrata em regulação e a segunda por poder gerar uma série de normas conflitantes que podem inviabilizar a existência destes comunicadores eletrônicos.

Portanto, é necessária a cooperação internacional para buscar um termo que permita que os avanços tecnológicos não se transformem em ambiente amplamente propício para atos que atingem a sociedade e também que se protejam as informações da imensa maioria dos usuários que precisam ter suas comunicações preservadas.

A saída passa, necessariamente, por algum tipo de acordo internacional que estabeleça regras mínimas de regulação que permitam que as autoridades possam ter ferramentas para combater determinadas ações ilícitas na internet garantindo, entretanto, que diversos direitos fundamentais modernos como a garantia de privacidade das comunicações sejam preservados.

É um longo e difícil processo onde devemos estabelecer os mecanismos e garantias para o desenvolvimento sustentado de um das maiores e revolucionárias invenções da história da humanidade: a internet.

REFERÊNCIAS

ASCENSÃO, José de Oliveira. *E agora? Pesquisa de um futuro próximo*. *In: Direito da Sociedade da Informação.* Coimbra: Coimbra, 1999.

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. Acesso em: 11 dez 2016.

LIMA, Glaydson de Farias. *Manual de Direito Digital: Fundamentos, Legislação e Jurisprudência.* Curitiba: Appris, 2016.

MARCACINI, Augusto. *Direito e Informática: uma abordagem jurídica sobre a Criptografia*. Lulu. Com, 2010.

ROBERTO, Wilson Furtado. *Dano transnacional e internet: Direito aplicável e competência internacional.* Curitiba: Juruá Editora, 2010.

TI INSIDE. *Apesar de ter a maior reserva de caixa, Apple é a empresa de tecnologia mais endividada.* Disponível em: <http://convergecom.com.br/tiinside/07/05/2015/apesar-de-ter-a-maior-reserva-de-caixa-apple-e-a-empresa-de-tecnologia-mais-endividada/>. Acesso em: 11 dez. 2016.