VI ENCONTRO INTERNACIONAL DO CONPEDI - COSTA RICA

NOVAS PERSPECTIVAS DO DIREITO: DIÁLOGOS OU DISJUNÇÕES ENTRE O DIREITO PÚBLICO E O DIREITO PRIVADO

LUIZ GUSTAVO GONÇALVES RIBEIRO

MARIA CRISTINA VIDOTTE BLANCO TARREGA

N935
Novas perspectivas do direito: diálogos ou disjunções entre o direito público e o direito privado [Recurso eletrônico on-line] organização CONPEDI/UNA/UCR/IIDH/IDD/UFPB/UFG/Unilasalle/UNHwN;

Coordenadores: Luiz Gustavo Gonçalves Ribeiro, Maria Cristina Vidotte Blanco Tarrega -

Florianópolis: CONPEDI, 2017.

Inclui bibliografia
ISBN: 978-85-5505-393-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direitos Humanos, Constitucionalismo e Democracia no mundo contemporâneo.
1.Direito – Estudo e ensino (Pós-graduação) – Encontros Internacionais. 2. Perspectiva. 3. Diálogo. 4.

Disjunção. I. Encontro Internacional do CONPEDI (6. : 2017 : San José, CRC).

CDU: 34

Universidad Nacional de Costa Rica
Heredia – Costa Rica
www.una.ac.cr

Conselho Nacional de Pesquisa e Pós-Graduação em Direito Florianópolis – Santa Catarina – Brasil

Universidad de Costa Rica San José – Costa Rica https://www.ucr.ac.cr

VI ENCONTRO INTERNACIONAL DO CONPEDI - COSTA RICA

NOVAS PERSPECTIVAS DO DIREITO: DIÁLOGOS OU DISJUNÇÕES ENTRE O DIREITO PÚBLICO E O DIREITO PRIVADO

Apresentação

A obra expõe, de forma bastante evidente, o quão ecléticas e ricas foram as apresentações e os debates ocorridos no âmbito do Grupo de trabalho intitulado “Novas perspectivas do direito: diálogos ou disjunções entre o direito público e o direito privado”, por ocasião do VI Encontro Internacional do CONPEDI, na Costa Rica.

Os artigos externam a preocupação dos seus autores de real e efetivamente trazerem à baila as novas discussões empreendidas nos mais diversos ramos do Direito. Se por um lado enaltecem a novidade, os textos não descuidam, por outro, da doutrina tradicional e da perspectiva constitucional tradutora do empoderamento da dignidade da pessoa humana.

A riquíssima experiência de apresentação dos textos de tamanha qualidade somente foi possível pela envergadura dos autores, os quais se comprometeram com a discussão, séria e necessária, de diversos e atuais temas, que entoam a regência da vida moderna pelo direito nas mais diversas áreas.

Por óbvio, os trabalhos não estão a salvo de críticas, mas procuram estabelecer, em intensidades diferentes, a comunicabilidade e a interseção vigentes entre o que outrora se distinguia de forma acentuada como público e privado, nacional e internacional. Novos horizontes se avistam e inovadoras perspectivas estabelecem as relações humanas e estatais.

Aos leitores, desejamos aprazível e inspiradora reflexão!

San Jose, Costa Rica, maio de 2017.

Prof. Dr. Luiz Gustavo Gonçalves Ribeiro - ESDHC

Profa. Dra. Maria Cristina Vidotte Blanco Carrega - UFG

A (IN) SEGURANÇA JURÍDICA DAS COMUNICAÇÕES DIGITAIS NO BRASIL: O CASO WHATSAPP

A LEGAL (IN) SECURITY OF DIGITAL COMMUNICATIONS IN BRAZIL: THE WHATSAPP CASE

Rodrigo Cardoso Silva [1]
Valter Moura do Carmo

Resumo

Em que medidas o judiciário brasileiro poderá bloquear o aplicativo WhatsApp sem transgredir a Constituição da República e o Marco Civil da Internet? A partir desta reflexão, o presente artigo irá analisar a Argüição de Descumprimento de Preceito Fundamental 403, a Ação Direta de Inconstitucionalidade 5.527 e a relação da troca de mensagens instantâneas com o universo da criptografia para traçar um panorama jurídico do futuro das comunicações digitais no Brasil.

Palavras-chave: Adpf 403, Adi 5.527, Bloqueio judicial do whatsapp, Marco civil da internet (lei 12.965/2014), Criptografia de dados e informações

Abstract/Resumen/Résumé

What measures can the brazilian judiciary block WhatsApp without violating the Constitution of the Republic and Civil Internet Framework? About this reflection the present text will analyze the Argument of Non-compliance with Fundamental Precept 403, the Direct Action of Unconstitutionality 5.527 and the relation of the exchange of instantaneous messages with the universe of the cryptography to draw a legal scenario of the future of digital communications in Brazil.

Keywords/Palabras-claves/Mots-clés: Adpf 403, Adi 5.527, Judiciary block whatsapp, Civil internet framework (law 12.965/14), Data encryption and information

[1] Pesquisador em Direito Digital, eGOV e Governança da Internet. Mestre em Direito Internacional. Doutorando em Tecnologias da Inteligência pela PUC-SP. Membro do ILA e da Internet Society. Comentarista do OMCI.

1. INTRODUÇÃO

No ano de 2015 até 2016 já foram realizados quatro bloqueios judiciais do aplicativo WhatsApp[1] na tentativa de conseguir informações privadas durante as investigações criminais, especificamente, nas comarcas de Teresina (PI), São Bernardo do Campo (SP), Lagarto (SE) e Duque de Caxias (RJ)[2]. No entanto, o bloqueio somente impediu a troca de mensagens instantâneas entre milhões de brasileiros pela Internet, ocasionando um imbróglio jurídico.

Após o terceiro e o quarto bloqueios, o assunto chegou ao Supremo Tribunal Federal (STF) do país sob dois instrumentos jurídicos, a Argüição de Descumprimento de Preceito Fundamental (ADPF) 403 e, posteriormente, a Ação Direta de Inconstitucionalidade (ADI) 5.527. Em breve síntese, a ADPF 403 discutiu a violação do preceito fundamental da liberdade de comunicação disciplinado no artigo 5º, inciso IX, Carta da República, que diz respeito ao direito à comunicação, quando o bloqueio de aplicativos de mensagens, neste caso, o *WhatsApp*, é determinado pela justiça criminal. Já a ADI 5.527 questionou a constitucionalidade de artigos do Marco Civil da Internet que foram utilizados para fundamentar os bloqueios do mesmo aplicativo.

Não obstante, porém, bastante importante ao contexto e que causa impacto diretamente nessa discussão jurídica é o protocolo de segurança da informação do WhatsApp. O *software* de criptografia adotado nas transferências de comunicação entre os usuários se transformou no tema latente e, quiçá, como sendo um dos responsáveis pelo litígio em questão.

Então, pode-se observar que são três assuntos que transitam de forma transdisciplinar na busca de uma solução ao problema. Com efeito, a proposta aqui é percorrer esses pontos divergentes para se chegar a um senso comum, sem transgredir o assunto no âmbito jurídico e, especialmente, dentro do ecossistema da Internet.

O problema mencionado acima diz respeito a dois questionamentos: a) saber em que medidas o judiciário brasileiro poderá bloquear o WhatsApp ou outro modelo de comunicação

[1] É uma ferramenta de comunicação digital que utiliza a Internet móvel (diferente da Internet fixa) para trocar mensagens instantâneas ponta a ponta. Tornou-se indispensável para fins, inclusive laborais, do mundo contemporâneo, tanto na esfera privada ou pública. Ele é utilizado por médicos, juízes, advogados, agentes públicos e cidadãos em geral. É a telefonia do futuro mediante a comunicação pela voz, escrita e a imagem. Uma evolução sem fim aparente para a sociedade global. (Nota dos autores).

[2] No decorrer da pesquisa, os autores irão expor um relato sintetizado sobre esses bloqueios ocorridos entre o ano de 2015 e 2016.

digital semelhante; b) até que ponto o judiciário poderá interferir no protocolo criptográfico de proteção de dados e informações utilizado entre os usuários do aplicativo.

A partir desse ponto, percebe-se que os objetivos traçados nesta pesquisa científica estão direcionados para esclarecer e propor soluções aos aspectos normativos postos em discussão, e que não devem interferir, direta ou indiretamente, na tecnologia de comunicação digital pela Internet de maneira que possa construir um óbice para o futuro do Brasil[3].

Igualmente, aduziu o eminente professor e ministro da Suprema Corte Argentina, Ricardo Luís Lorenzeti:

> "O surgimento da era digital tem suscitado a necessidade de repensar importantes aspectos relativos à organização social, à democracia, à tecnologia, à privacidade, à liberdade e observa-se que muitos enfoques não apresentam a sofisticação teórica que semelhantes problemas requerem; esterilizam-se obnubilados pela retórica, pela ideologia e pela ingenuidade (Apud LEONARDI, 2011, p. 12)."

Vale ressaltar que, a Carta de Direitos Civis da Internet do Brasil é bastante objetiva e clara em manter a Internet livre e aberta com base em seus princípios, sem se esquecer do seu reconhecimento pelas Nações Unidas como um direito humano fundamental e outros princípios norteadores para o convívio social.

Além disso, o ciberespaço é o ecossistema da Internet que, identicamente, reproduz a sociedade corpórea (material) no ambiente incorpóreo (virtual), perfazendo-se, assim, dos mesmos direitos. Deste modo, o importante é adaptar esses dois mundos sem tentar transgredir a autonomia evolutiva da rede mundial de computadores construída desde a sua origem.

No mesmo sentido, são as palavras de Pierre Lévy ao afirmar que a sociedade involuntariamente tende a refletir sobre o seu futuro a partir de um conhecimento científico local e global[4]:

> "A cibercultura sempre evoca uma reflexão sobre o futuro (LEVY, 1999, p. 22)".

[3] É importante lembrar que a Internet é uma rede colaborativa onde os participantes concordam em seguir protocolos e padrões abertos pela *Internet Engeneering Task Force (IETF).* (Nota dos autores).

[4] A aceleração do paradigma informacional, ou seja, um fenômeno de junção do eletrônico com o digital faz com que o ser humano tenha que ser resiliente para desenvolver as capacidades necessárias para o uso das inovações tecnológicas na sociedade do conhecimento e da informação digital (Nota dos autores).

Por fim, o objetivo desta investigação científica é apresentar propostas de soluções eficientes para o tema em questão que é, sem dúvida, tarefa desafiadora, da qual o intérprete do Direito não pode se esquivar, sob pena de se perpetuarem situações dúbias e, possivelmente, injustas.

2. METODOLOGIA

O método adotado para esta pesquisa científica é o documental, o sistêmico e o qualitativo em vista da abordagem jurídica e tecnológica em torno do problema que, neste caso, é um fenômeno empírico no ecossistema da Internet.

3. ANÁLISE DOS DESCUMPRIMENTOS DE ORDENS JUDICIAIS PARA ENTREGA DE DADOS DIGITAIS

3.1. Primeiro caso: Teresina (PI)

Em 11/02/2015, o juiz da Central de Inquéritos da comarca de Teresina, estado do Piauí, determinou em decisão de primeira instância o bloqueio da aplicação WhatsApp em todo o Brasil por descumprimento de ordens judiciais para a entrega de dados de usuários suspeitos por cometimento de crimes.

Este foi o primeiro caso de bloqueio do WhatsApp no país, sendo realizado inclusive em segredo de justiça, tanto a decisão do bloqueio quanto a sua suspensão no Tribunal de Justiça (TJ)[5]. Assim, é notório dizer que muitas informações sobre o caso foram noticiadas por meios de comunicação do próprio tribunal ou jornalístico.

Segundo consta, o bloqueio judicial ocorreu em face de empresas provedoras de acesso à Internet que ingressaram com mandado de segurança[6] contra a ordem judicial que foi posteriormente suspensa em 25/02/2015. A decisão de bloqueio das atividades do WhatsApp no Brasil se deu em razão de reiterados descumprimentos de ordens judiciais emanadas desse juízo de primeiro grau.

[5] Ações Penais Públicas n. 0013872-87.2014.8.18.0140 e 007620-68.2014.8.18.0140.

[6] Em resposta, as empresas impetraram mandados de segurança para suspender a decisão monocrática. Os impetrantes do remédio constitucional, apenas três provedores de acesso à Internet alegaram que a determinação não poderia ser cumprida. Fundamentaram que: a) esbarra em limitações técnicas; b) viola os artigos 3º, inciso VI e 18, ambos da Lei 12.965/14; c) contraria a própria finalidade de coletar dados; d) constitui ato destituído de razoabilidade, pois impõe o bloqueio do acesso de uma infinidade de usuários às funcionalidades do aludido aplicativo, apenas para atender a pretensões de um procedimento investigatório cujo fim pode ser alcançado por meio de inúmeras outras medidas.

Igualmente, o magistrado alegou que por a empresa não ter escritório no país, ela se manteve inerte às solicitações da justiça brasileira. Nesse sentido, a ordem judicial teve o objetivo causar um *enforcement* para que o WhatsApp auxiliasse com as investigações policiais.

Já a decisão que concedeu o pedido de liminar de suspensão[7] pelo desembargador foi realizada em 26/02/2016. Aludiu que, independentemente do teor da ordem descumprida, em hipótese alguma se justifica a interrupção do acesso a todo um serviço, já que se afeta a comunicação entre um sem número de pessoas. Ademais, faltaria proporcionalidade à medida, pois se trata de suposta tentativa de paralisação de uma gigantesca e pesada estrutura tecnológica em prol de uma investigação criminal que, muito provavelmente, possui número limitadíssimo de suspeitos. Ratificou, ainda, que existem outros meios de investigação, não se mostrando plausível que toda uma investigação passe a depender de informações de natureza telemática. A decisão foi confirmada em julgamento de mérito no dia 06 de junho de 2016.

3.2. Segundo caso: São Bernardo do Campo (SP)

Em 06 de dezembro de 2015, a juíza da 1ª Vara Criminal de São Bernardo do Campo, São Paulo (SP), determinou o bloqueio do WhatsApp em todo o Brasil como punição pelo descumprimento de ordens judiciais de acesso a dados de usuário denunciado. Foi a segunda decisão de bloqueio do aplicativo e a primeira a ser aplicada, perdurando-se por aproximadamente 12 horas[8].

Consta que no relatório da decisão de suspensão do bloqueio, a ordem esta fundamentada para a investigação de tráfico de drogas[9], sendo oficiada ao Facebook Brasil – detentora do produto *WhatsApp* com escritório no país.

Em nota, o Tribunal de Justiça de São Paulo (TJSP) afirmou que a empresa WhatsApp não atendeu a uma determinação judicial de 23 de julho de 2015, sendo que em 07 de agosto de 2015, a empresa foi novamente notificada, fixando-se multa em caso de não cumprimento. O processo inicial foi posto em segredo de justiça, mas o TJSP publicou uma nota afirmando que o Ministério Público requereu o bloqueio dos serviços pelo prazo de 48 horas com base na lei do Marco Civil da internet.

[7] Mandado de Segurança n. 2015.0001.001592-4.
[8] Procedimento de Interceptação Telefônica n. 0017520-08.2015.8.26.0564.
[9] Solicitava-se a interceptação digital de mensagens do WhatsApp vinculada a três contas (uma linha brasileira e duas linhas paraguaias).

Em contrapartida, a WhatsApp Inc. ingressou com mandado de segurança contra a decisão e alegou que: a) o pretexto de investigar três linhas telefônicas afasta milhões de usuários, incluindo redes de serviços de utilidade pública; b) não intimou a impetrante a cumprir a ordem judicial, o que era possível através da cooperação jurídica internacional; c) violou a Lei 12.965/14 e o Decreto no 3.810/2001. Por fim, o desembargador do TJSP deferiu liminar impetrada pela suspensão do bloqueio.[10]

3.3. Terceiro caso: Largato (SE)

No dia 26/04/2016, a decisão de bloqueio foi emanada pelo juiz da Vara Criminal de Lagarto em primeira instância, no estado de Sergipe, após o pedido da Polícia Federal, em processo de medida cautelar de interceptação telemática dirigida à empresa Facebook Brasil pelo prazo de 72 horas. No entanto, a duração da suspensão dos serviços do aplicativo durou apenas no dia 02/05/2016.

Após a decisão de bloqueio, a empresa WhatsApp Inc. impetrou mandado de segurança com pedido de liminar, mas que foi denegado pelo desembargador plantonista do Tribunal de Justiça de Sergipe, sendo que, posteriormente, a liminar foi revista e concedida no dia 03/05/2016[11].

Segundo consta, a investigação estava atrás de trinta e seis usuários supostamente envolvidos em uma organização criminosa que, com base nas investigações da autoridade policial, patrocinava de tráfico interestadual de drogas. A Autoridade Policial responsável pela investigação denominou o *WhatsApp* como plataforma do crime, pois a dificuldade em ter acesso aos dados interrompeu o desfecho das diligências policiais.

O caso em si é emblemático, não em vista da decisão ter sido baseada no artigo 12, inciso III, da Lei 12.965/2014, pois, segundo o magistrado, uma vez que a empresa Facebook Brasil estaria em mora com relação à ordem de interceptação de mensagens em tempo real no aplicativo *WhatsApp*, mas porque além do arbitramento de multa, o juiz decretou a prisão do vice-presidente da empresa Facebook no país[12] e, também, o reconhecimento do juiz na sentença que a medida afetaria milhões de usuários do aplicativo[13]. Novamente, é percebida outra medida de *enforcenment* judicial contra a empresa Facebook Brasil.

[10] Mandado de Segurança n. 2271462-77.2015.8.26.0000.
[11] Número do processo 201600110899.
[12] Número do processo 201655090027.
[13] Na sentença, o juiz disse que o *Facebook* e o *WhatsApp* não são serviços essenciais pela legislação brasileira e que há outras formas de comunicação. E, também, acolheu o parecer da Polícia Federal acerca da

Em contrapartida, a empresa WhatsApp impetrou um mandado de segurança[14] contra a ordem de bloqueio e argumentou que a determinação judicial sobre a quebra de sigilo foi direcionada à empresa Facebook Brasil, sem ter recebido notificação de conhecimento do processo.

Por fim, é importante consubstanciar a posição do desembargador no pedido de reconsideração da denegação anterior, pois ele concedeu a liminar de suspensão de bloqueio em razão do caos social e insatisfação da sociedade civil gerado pela interrupção dos serviços de comunicação do *WhatsApp*.

3.4. Quarto caso: Duque de Caxias (RJ)

Em 19 julho de 2016, a juíza da 2ª Vara Criminal da cidade de Duque de Caxias, estado do Rio de Janeiro, determinou o bloqueio do *WhatsApp* em todo o Brasil, como punição pelo descumprimento de ordens de interceptação policial[15].

Consta que a empresa Facebook Brasil recebeu ordem de quebra de sigilo e interceptação telemática de mensagens e o desligamento da chave criptográfica do aplicativo *WhatsApp* em relação a terminais-alvo[16] nos autos do inquérito policial que investigava uma organização criminosa que, segundo os autos, dedicava-se ao cometimento de vários crimes.

Em contrapartida, o WhatsApp argumentou que não detém informações das troca de mensagens e não tinha meios técnicos para realizar a interceptação telefônica judicial. Também tentou se reunir com a magistrada, promotor de justiça do caso e especialista em criptografia para esclarecer os obstáculos técnicos, mas não logrou êxito.

No dia 18/07/2016, a empresa Facebook Brasil recebeu outro ofício com suposto pedido de monitoramento dos suspeitos vinculados a 23 terminais-alvo e para desabilitar a chave de criptografia do *WhatsApp* pelo prazo de quinze dias, sob pena de multa e suspensão dos serviços.

---

possibilidade de interceptar a comunicação pelo protocolo de criptografia de ponta-a-ponta do *WhatsApp*. Ratificou, ainda, que não há necessidade de seguir procedimento de acordo de cooperação internacional para obter os dados requisitados, pois o crime investigado ocorreu no Brasil, sendo, neste caso, os afetados nacionais.

[14] Argumentou que houve a: a) desproporcionalidade do bloqueio; b) a impossibilidade jurídica de se ordenar a suspensão de aplicativo nas circunstâncias do caso; c) a inexistência de obrigação de retenção do conteúdo e; d) impossibilidade técnica de interceptação das mensagens privadas pelo WhatsApp.

[15] Inquérito Policial 062-00164/2016.

[16] Conforme a disciplina do artigo 5º, II, Lei 12.965/14, terminal é qualquer computador ou dispositivo que se conecte a Internet.

A suspensão aqui veio embasada pelo por um partido político e peticionada no STF[17]. Fato este que culminou na medida cautelar ADPF 403 e que, ulteriormente, ganhou mais força em razão da ação impetrada pela WhatsApp Inc. com pedido de liminar no Tribunal de Justiça do Rio de Janeiro[18].

4. ARGUIÇÃO POR DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL 403

No dia 03/05/2016, o STF recebeu a ação proposta por um partido político que é contrário às decisões de bloqueio do aplicativo *WhatsApp* no país. O principal argumento do partido político é o de que a decisão de bloqueio violou o preceito fundamental da liberdade de comunicação, disciplinado no artigo 5º, inciso IX, da Constituição Federal e, também, o princípio da proporcionalidade, em razão de milhares de brasileiros terem o serviço do aplicativo bloqueado.

O partido considerou ainda a argumentação da decisão como controversa pelo fato das decisões anteriores semelhantes terem sido objeto de denegação pelos respectivos Tribunais de Justiça. Com efeito, a legenda partidária ajuizou a ADPF 403 no STF pedindo não somente a suspensão do bloqueio, mas o impedimento de qualquer decisão judicial que ensejem bloqueios futuros.

Não obstante, cinco instituições também ingressaram na ação acima como *amici curiae*[19]. A posição delas é favorável ao argumento da petição inicial, porém, existem diferenças quanto à fundamentação e à extensão de seus pedidos[20].

[17] Petição 39344/2016-STF.

[18] Mandado de Segurança n. S 0036719-20.2016.8.19.0000.

[19] Significa que as instituições não são partes do processo, mas irão fornecer informações necessárias com a finalidade de subsidiar as decisões do tribunal para se obter uma melhor base de conhecimento para o assunto relevante e latente no país.

[20] A Federação das Associações das Empresas de Tecnologia da Informação (ASSESPRO) caracterizou o ato judicial de bloqueio como inconstitucional também por impedimento ao livre acesso de todos à informação (artigo 5º, inciso XIV) e proibição à continuidade do próprio objeto social da WhatsApp (artigo 170 da Carta da República, parágrafo único, inciso IV) e argumentou de maneira ainda mais ampla do que o feito pelo PPS. No mesmo sentido, a Associação Brasileira de Defesa do Consumidor (PROTESTE) pediu o impedimento a qualquer outra decisão judicial que venha causar lesão aos preceitos fundamentais violados de liberdade de expressão, de comunicação e de intimidade e comunicação privada. O Instituto Beta para Democracia e Internet (IBIDEM) e o Laboratório de Pesquisa Direito Privado e Internet da Faculdade de Direito da Universidade de Brasília (LAPIN) afirmaram que as decisões anteriores de bloqueios, o principal fundamento utilizado para justificá-los foi o artigo 461, §1.º, do CPC/73. E, somente no terceiro caso, da cidade de Lagarto, a decisão expressamente utilizou o artigo 12, inciso III do Marco Civil. Já a Frente Parlamentar pela Internet Livre e Sem Limite vai além da questão dos bloqueios e pede a declaração de interpretação conforme a Constituição ao artigo 10, caput, parágrafo 2º, da Lei 12.965/14 para que seja inconstitucional a interpretação de que haveria um dever irrestrito de guarda de registros de acesso, de conexão e de conteúdos de comunicações. Eles defendem que tal dever importaria em violação aos direitos fundamentais à intimidade, à vida privada, ao sigilo das comunicações, e ao princípio da proporcionalidade. O Instituto de Tecnologia e Sociedade (ITS) teve a mesma posição quanto ao artigo 12. A instituição pede a declaração de inconstitucionalidade de qualquer interpretação

5. AÇÃO DIRETA DE INCOSTITUCIONALIDADE 5.527

Em 13/05/2016, a ADI 5.527 foi impetrada por outro partido político que requereu a suspensão imediata do bloqueio e, ao final, a declaração de inconstitucionalidade do artigo 12, incisos III e IV da Lei 12.965/14 que foram utilizados para fundamentar os bloqueios do aplicativo *WhatsApp*.

A legenda partidária argumentou também que três artigos a respeito da liberdade de comunicação, são eles: os artigos 5º, inciso IX e 170, caput, ambos da Constituição Federal do Brasil e o artigo 13 da Convenção Americana de Direitos Humanos.

Diante da relevância jurídica do tema, surgiram partes *amici curiae* que ingressaram na ação com posições críticas aos bloqueios, mas com posicionamentos até que relevantes para o assunto em tela[21].

6. A POSIÇÃO DO SUPREMO TRIBUNAL FEDERAL

Com base nos artigos 21, inciso XVII, e 154, inciso III, do Regimento Interno do STF, os relatores da ADPF 403 e ADI 5.527 decidiram convocar uma audiência pública[22] simultânea para os dois casos com o objetivo de tornar mais ampla à participação de especialistas, órgãos públicos, atores não governamentais e a sociedade civil.

Para o STF, os julgados nesses dois últimos anos demonstraram uma notória controvérsia entre o poder público brasileiro e a pessoa jurídica WhatsApp (direito privado) que, na evidência das decisões de bloqueio do aplicativo e a ulterior suspensão dele, estão além do direito à liberdade de comunicação.

---

feita das sanções previstas pelo respectivo artigo que possibilite ser fundamento para o bloqueio de serviços de internet, mas que estas sejam aplicadas somente como forma de compelir que os aplicativos e sites respeitem o direito à privacidade dos usuários. Corroborou e pediu a vedação de novas decisões judiciais que determinem o bloqueio geral e indeterminado de serviços de comunicação em sites ou aplicativos de Internet.

[21] Recebeu manifestações da Câmara dos Deputados, do Senado Federal e da Advocacia-Geral da União que, em linhas gerais, não vêem inconstitucionalidade do artigo do Marco Civil da Internet (MCI). O Comitê Gestor da Internet no Brasil (CGI.br) afirmou em nota que as sanções do artigo 12 do MCI não são inconstitucionais, sendo que o obstáculo está na interpretação do MCI, ou seja, no âmbito da aplicação da lei que pode sobrepor interesses econômicos de provedores a direitos fundamentais dos usuários. O Instituto Beta para Democracia e Internet (IBIDEM), em parceria com os pesquisadores do Laboratório de Pesquisa, Direito Privado e Internet da Faculdade de Direito da Universidade de Brasília (LAPIN) pede que essa ADI 5.527 não seja reconhecida em juízo, pois o MCI não é para ser interpretado como fundamento de bloqueios de aplicativos de comunicação. O ITS Rio adotou posição idêntica à da AGU. Por fim, a Frente Parlamentar pela Internet Livre e Sem Limites seguiu com o mesmo raciocínio do ITS Rio.

[22] Até o dia 01/02/2017 o STF recebeu inscrições via *e-mail* (adpf403@stf.jus.br e marcocivilinternet@stf.jus.br) de interessados a participar da audiência pública sobre os dois casos.

Desta forma, a investigação preconiza que a interpretação do MCI também é relevante em razão do seu objetivo real. Ou seja, o MCI é um instrumento de defesa da existência da Internet no país para que ela permaneça livre a aberta, e não uma ferramenta de punição. A hermenêutica, neste caso, deverá ser reavaliada.

Por fim, o posicionamento do STF foi cauteloso em chamar uma audiência pública que irá buscar respostas para o problema, que segundo ele, apenas abordará à complexa relação de troca de mensagens criptografadas no *WhatsApp*, com o propósito de encontrar possibilidades técnicas de se interceptar conversas, decretar a suspensão temporária das atividades do aplicativo e vincular a colaboração da empresa WhatsApp com as decisões judiciais fundadas no art. 5º, XII da Carta Magna.

7. COMO FUNCIONA A CHAVE CRIPTOGRÁFICA DO WHATSAPP?

O chamamento para uma audiência pública fez ressaltar a importância do entendimento sobre o conceito, tipos e a forma de operação das trocas de mensagens com a chave de segurança criptográfica do aplicativo de comunicação digital *WhatsApp*.

Conforme as palavras de Stallings (2015), a criptografia é a ciência que transforma a informação original de qualquer linguagem escrita para outra informação ilegível, tornando-a conhecida apenas pelo destinatário possuidor da chave secreta. A evolução da escrita secreta utilizada por muito tempo pela humanidade como forma de assegurar as informações constitui atualmente em diversos modelos de encriptação.

Para entender o processo de parametrização de uma chave, as mensagens a serem criptografadas, ou seja, converter um texto normal em um texto cifrado é denominado de encriptação. De outra parte, a restauração do mesmo texto para leitura é chamado de decifração ou decriptação (TANEMBAUM et. al., 2011).

Com efeito, é importante esclarecer os tipos tecnológicos de criptografia existentes até hoje. Para Stallings (2015), uma das formas de classificar sistemas criptográficos se refere ao número de chaves utilizadas no processo. Por exemplo, se tanto o emissor quanto o receptor utilizarem a mesma chave, o sistema é classificado como encriptação simétrica. Todavia, se emissor e receptor usarem chaves diferentes, o sistema é classificado como encriptação assimétrica ou de chave pública.

No aplicativo *WhatsApp* se utiliza o protocolo de chave de segurança denominado *Signal Protocol*, que fornece criptografia ponto a ponto para mensagens instantâneas. É mister destacar que o núcleo do protocolo foi recentemente adotado por outros aplicativos bastante

populares e semelhantes, dentre os quais podemos destacar o próprio *WhatsApp*, *Facebook Messenger* e *Google Allo*, entre outros.

Para a melhor compreensão do cenário tecnológico que envolve o problema desta pesquisa científica, ela irá buscar responder os quatro questionamentos técnicos solicitados pelo STF[23] para a audiência pública proposta[24].

O primeiro quesito diz respeito à criptografia de ponta a ponta. Na ótica computacional, é preciso antes entender o conceito sobre interconexão *peer-to-peer* ou ponta a ponta. Com efeito, pode-se afirmar que é uma arquitetura de redes de computadores de elevada disponibilidade em que cada um dos pontos ou nós da rede funcionam tanto como cliente quanto como servidor, permitindo, assim, o compartilhamento de serviços e dados sem a necessidade de um servidor central. Isto é, o servidor não é o responsável pela execução de todas as funções da rede, pois todos os nós estão interconectados possibilitando que o acesso a qualquer nó tenha origem em qualquer outro nó.

Desta maneira, corrobora Stallings (2015) quando diz que 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. Isto ocorre porque para que a encriptação simétrica funcionem corretamente, as duas partes precisam compartilhar a mesma chave, que deve ser protegida contra o acesso de outras partes sem permissão. Hoje, as chaves mencionadas são fornecidas por um Centro de Distribuição de Chaves (CDC).

O CDC é responsável por distribuir chaves em pares de usuários conforme a necessidade de cada um para que cada usuário compartilhe uma chave exclusiva com o CDC. Neste sentido, 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. Novamente, na acepção de Stallings:

> "Cada chave de sessão é obtida a partir do CDC, transmitidas em formato encriptado, usando uma chave mestra exclusiva que é

[23] Os quesitos são: 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?

[24] Até a submissão deste artigo, o STF não determinou a data da audiência pública.

> compartilhada pelo centro e o usuário final (STALLINGS, 2015, p. 125)".

Assim, pode 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, sendo que o acréscimo dessa camada um meio seguro e eficiente de distribuir chaves mestras.

Com base nessa explanação, a pesquisa aduz que o aplicativo *WhatsApp* funciona da maneira supracitada, ou seja, o aplicativo opera como um CDC. Esta afirmação também pode ser encontrada no portal da empresa WhatsApp:

> "É colocado que existem seis chaves, porém há dois tipos diferentes utilizados no processo em si: par de chaves público-privada e chaves de sessão. As chaves de sessão são chaves simétricas geradas entre as partes e utilizadas unicamente em cada sessão de mensagem. Essa chave é descartada após o encaminhamento da mensagem. Já a chave privada do par de chaves público-privada é utilizada para a autenticação do usuário na plataforma (WHATSAPP, 2016)".

Mas afinal, como elas são geradas e armazenadas?[25] Segundo informações da empresa do aplicativo, os pares de chaves são gerados no momento da instalação do aplicativo em determinado dispositivo de telefonia celular. Diferentemente do que comumente é exposto, parte dessas informações com chaves públicas são transmitidas para o servidor. Deste modo, as *PreKeys* – como são denominadas, são utilizadas basicamente para identificação e registro de cada usuário no sistema[26].

As figuras abaixo demonstram uma visualização semiótica do processo em quatro estágios: chaves, registro, sessão e troca de mensagens.

[25] Este questionamento é uma linha de raciocínio para tentar elucidar alguns pontos que envolvem o Marco Civil da Internet.

[26] Além disso, também ocorrem outras três sessões para a troca de mensagens quando é usado o *Signal Protocol* pelos usuários do aplicativo. São elas: a) *PreKeyBundles* - quando uma mensagem é enviada a algum contato ou é adicionado algum contato no dispositivo de um usuário (alguém que já possui o aplicativo instalado ou uma sessão com aquele usuário é estabelecida) diante da obtenção da chave daquele usuário a partir do servidor. Percebe-se que o contato com quem a comunicação pretende ser estabelecida tem o aplicativo Whatsapp instalado em seu dispositivo, uma vez que é possível visualizar o status do aplicativo daquele contato. E mesmo que não tenha ocorrido a troca de mensagens, o usuário que deseja iniciar a comunicação já tem a chave obtida do servidor e tem conhecimento que o contato pode receber mensagens pelo aplicativo; b) *PreKeySignalMessages* - um cliente do WhatsApp pode receber uma mensagem de um usuário que ainda não está em sua lista de contatos. A partir dessa mensagem ele passará a obter a chave do emissor, estabelecendo-se, assim, outra forma de sessão; c) *KeyExchangeMessages* - dois usuários do aplicativo podem trocar contatos de um terceiro, isto é, o que é trocado de fato são as chaves desse terceiro, tornando-se possível que qualquer um desses dois usuários estabeleçam uma sessão com aquele que recebeu as suas chaves criptográficas.

Figura 1: Chaves Usadas no Processo

Figura 2: Processo de Registro do Usuário

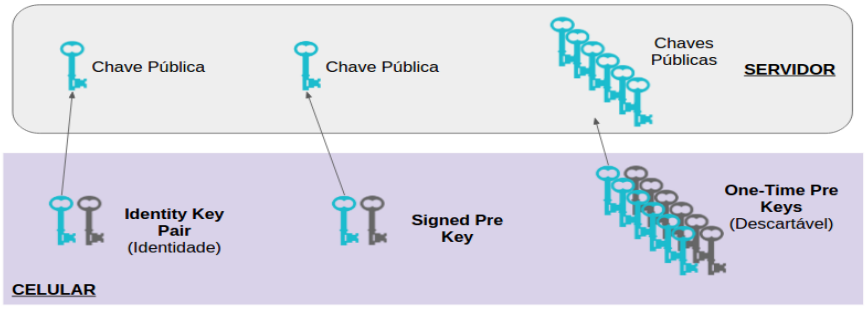


Figura 3: Processo de Estabelecimento da Sessão

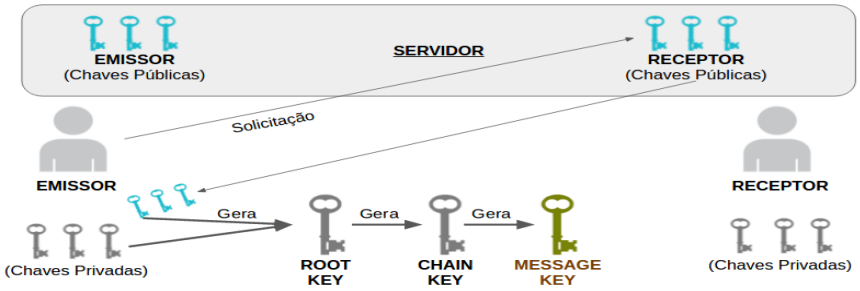
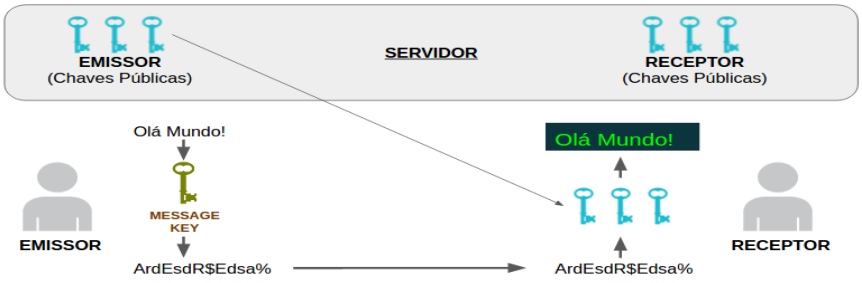


Figura 4: Processo de Troca de Mensagens



A pesquisa passa a responder o segundo e o terceiro quesitos da suprema corte do país. É importante antes tecer uma explanação sobre os algoritmos de encriptação. Neste sentido disse Stallings:

> "Afirma que não existe algoritmo de encriptação que seja incondicionalmente seguro (ou inquebrável). O que se pode obter é

> um esquema de encriptação considerado computacionalmente seguro, em que o algoritmo atende 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 (STALLINGS, 2015, p. 110)".

No *WhatsApp* o funcionamento da criptografia se dá por três pares de chaves assimétricas chamadas de *Identity Key Pair, Signed Pre Key e One-Time Pre Keys*, que preparam o canal de comunicação entre as pontas (a sessão) e três chaves privadas *Root Key, Chain Key,* e *Message Key*, sendo esta última que fará efetivamente a criptografia das mensagens[27].

A utilização de um *backdoor*[28] fragiliza de sobremaneira o mecanismo de segurança, uma vez que se cria um artifício que pode ser utilizado, por exploração de vulnerabilidades no dispositivo para a interceptação não intencional pela plataforma.

Em consonância com os problemas desta pesquisa, um pesquisador da área de segurança da informação da Universidade de Berkeley divulgou a existência de uma vulnerabilidade por meio da qual terceiros ou mesmo a própria empresa WhatsApp poderiam ter acesso às mensagens trocadas entre dois usuários no caso de retransmissão de mensagens quando o destinatário está *offline* ou desconectado da Internet.

Diante dessa manifestação do pesquisador, o jornal *The Guardian* (2017) noticiou que se tratava da existência de uma *backdoor* no aplicativo. Com isso, o argumento usado pela empresa para não fornecer dados ao Poder Judiciário brasileiro pode ser questionado, uma vez que o algoritmo criptográfico descrito pelo seu *technical white paper* (WHATSAPP, 2016) pode não estar corretamente implementado. Neste caso, é provável que contenha vulnerabilidades na segurança que podem ser exploradas para determinados fins.

De outra parte, institutos e pesquisadores da área de criptografia se posicionaram contra a versão mencionada pelo jornal britânico, e aduziram que se tratava de apenas de um *trade-off* para que o aplicativo apresentasse boa usabilidade (ELECTRONIC FRONTIER FOUNDATION, 2017; OPEN WHISPER SYSTEMS, 2017; TECHNOSOCIOLOGY, 2017).

[27] É importante reforçar que todas as chaves privadas, tanto de sessão quanto de criptografia, ficam armazenadas nos dispositivos das partes e não no servidor. Isso faz com que o acesso às mensagens por terceiros, em tese, dê-se da seguinte maneira: a) por interceptação da mensagem e quebra da criptografia por força bruta (adoção de poder computacional equivalente à força do algoritmo criptográfico); ou b) por alguma tratativa com o WhatsApp que permita solicitar previamente a desabilitação, por demanda, da criptografia ponta a ponta (inserção de *backdoor*). (Nota dos autores).

[28] É um método de transpor a autenticação normal em um produto, sistema de computador, cripto sistema ou algoritmo. São freqüentemente usadas para assegurar acesso remoto não autorizado a um computador ou obter acesso a textos em sistemas criptográficos. Pode assumir a forma de uma parte oculta de um programa ou um programa em separado, por exemplo, o *Back Orifice* pode subverter o sistema através de um tipo de código malicioso conhecido como *rootkit*, ou também pode ser um recurso de hardware.

Igualmente, os especialistas afirmam que a interceptação das mensagens só pode ser feita em um caso muito específico - retransmissão pelo fato do destinatário estar desconectado, e que a falha não é de fácil reprodução por usuários que não sejam especialistas em criptografia.

No que tange a desabilitação da criptografia ponta a ponta, considerando-se a natureza do código de desenvolvimento do aplicativo *Whatsapp* ser fechada, pode-se reputar a possibilidade de qualquer alteração no funcionamento do *software*.

Porém, qualquer interceptação ou monitoramento por terceiros no modelo *man-in-the-middle*[29], desde que não sejam as partes envolvidas na mensagem, seria impedido pelo próprio uso das chaves e algoritmos criptográficos que, além de tudo isso, produziria um alerta aos usuários do aplicativo[30].

É sabido que o aplicativo *WhatsApp* funcionou por muito tempo sem criptografia e, também, por algum tempo em dualidade[31]. Logo, é viável pensar que o *software* poderia funcionar em paralelo, ou seja, com e sem criptografia. Todavia, especialmente nesse caso, o conceito de criptografia ponta a ponta estaria comprometido.

Por exemplo, um cliente-usuário do *WhatsApp* pode receber mensagens criptografadas e não-criptografadas, pois depende da configuração do servidor e do suporte, com ou sem criptografia, estar presente nas últimas versões no aplicativo dele. Com isso, a empresa WhatsApp poderia desabilitar a criptografia sob demanda, mantendo-se o serviço operacional da mesma forma de 2015. Entretanto, julgando-se a implementação técnica natural do cliente-usuário, ele seria alertado, pois de outra forma haveria um *backdoor* no seu sistema[32].

Cabe ressaltar, ainda, que as informações estariam disponíveis tanto para interceptação legítima como para uma eventual interceptação mal intencionada e, provavelmente, não autorizada pelo cliente-usuário.

Por fim, é importante ressaltar a opinião de Tanembaum e Wetherall sobre a obscuridade ou não de um protocolo de chave de segurança criptográfica:

---

[29] É uma forma de ataque em que os dados trocados entre duas partes são de alguma forma interceptados, registrados e, possivelmente, alterados pelo atacante sem que a origem ou o destino dos dados tenham conhecimento. O atacante pode optar por retransmitir entre os legítimos participantes os dados inalterados, com alterações, ou bloquear partes da informação. (Nota dos autores).

[30] De acordo com o que é divulgado pela empresa WhatsApp e, também, com o atual estágio de funcionamento da criptografia de ponta a ponta. (Nota dos autores).

[31] Por um tempo o aplicativo WhatsApp operou com criptografia para alguns dispositivos celulares e para outros não. (Nota dos autores).

[32] Não é possível atestar se há ou não desvios implementados no código antes de a mensagem ser criptografada por se tratar de um código fechado. Em suma, uma aplicação tecnicamente adequada não aceitaria este tipo de artifício. (Nota dos autores).

> "Enfatizam que o caráter não sigiloso do algoritmo de encriptação a ser utilizado é importante. 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; caso muitos tenham tentado isso durante cinco anos após a sua publicação e nenhum tenha logrado êxito, há uma grande probabilidade de que o algoritmo seja sólido. Na verdade, o sigilo deve estar na chave, e seu tamanho é uma questão muito importante no projeto de um algoritmo de encriptação (TANEMBAUM E WETHERALL, 2011, p. 321)."

O pensamento exposto acima é bastante debatido no cenário computacional para uma Internet livre e aberta. Contudo, há uma resistência muito forte com as empresas que operam no segmento de segurança da informação.

Por último, a quarta pergunta do STF se dirige ao espelhamento de conversas para outros dispositivos digitais de comunicação. Para exemplificar o quesito, um dispositivo com o cliente *web* gera um par de chaves público-privadas que, ao ser lido pelo usuário, figura-se um QR-Code, que na seqüência o dispositivo envia sua chave pública para o aparelho de telefonia celular.

Conforme já foi mencionado anteriormente, o sistema é fechado. Então, um túnel TLS[33] entre o servidor do WhatsApp, o cliente web e o dispositivo. As mensagens são sempre criptografadas no dispositivo, sendo que o tráfego *web* é redirecionado até o dispositivo com a chave privada criptografada. Para, no final, enviar para os servidores de entrega de mensagem do aplicativo *WhatsApp*.

Com efeito, pode-se considerar que o espelhamento, neste caso, também não é praticável, pois a operação deste segue as mesmas tratativas do que o ocorre no dispositivo móvel, o aparelho celular.

8. A INTERPRETAÇÃO DO MARCO CIVIL DA INTERNET

A declaração de inconstitucionalidade do artigo 12, incisos III e IV da Lei 12.965/14[34] na ADI 5.527 fez levantar, mais uma vez, questionamentos sobre o Marco Civil da Internet (MCI)[35].

[33] *Transport Layer Security* é um protocolo que fornece confidencialidade e integridade nas comunicações entre um cliente e um servidor por meio de criptografia, podendo também ser usado para prover autenticação. É usado na Internet em conjunto com o protocolo HTTP, a fim de prover conexões seguras nas comunicações Web. (CERT.br, 2017).

[34] Texto da lei: "art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas

A utilização deste instrumento de lei para fundamentar os bloqueios do aplicativo *WhatsApp* trouxe dúvida sobre como o seu texto legal deve ser aplicado no poder judiciário. Deste modo, a pesquisa irá buscar entender a hermenêutica aplicada pelos juízes brasileiros nas sentenças de bloqueio e suspensão do aplicativo.

Antes é importante esclarecer a constitucionalidade ou não do MCI. O texto de lei em momento nenhum infringiu a Carta Magna, pois é notório dizer que é uma legislação contemporânea que serviu de modelo para o cenário internacional aprovada e sancionada pelas duas casas legislativas brasileiras. Além disso, a resolução do Comitê Gestor da Internet do Brasil (CGI.br) foi base para a construção desta lei[36]. É uma norma que tem como objetivo principal defender a Internet para que ela permaneça livre e aberta em todos os seus segmentos. É um mecanismo legal de complementação, e não sobreposição no ordenamento jurídico brasileiro. Portanto, não há inconstitucionalidade.

O texto do MCI pode não parecer ser unívoco para os operadores do direito, tanto que à aplicação da lei pelos juízos e desembargadores tem operado com ambigüidade causando excesso no seu poder geral de cautela.

A Lei 12.965/14 deve ser interpretada com base nos princípios basilares durante a sua criação. Provavelmente, a falta do reflexo desses princípios no texto do MCI de forma objetiva pode estar acarretando nessa dubiedade prática na decisão dos magistrados.

Apesar do MCI ter estabelecido princípios norteadores para o uso da Internet no país, o artigo 7º, incisos II e III, onde preconiza que as informações privadas podem ser violadas mediante ordem judicial e em consonância com o artigo 10, §§ 1º e 2º combinado com o artigo 22, em especial, o inciso II, no qual se refere a "ordem judicial com justificativa motivada", a pesquisa observou que as autoridades ao tomarem a decisão do bloqueio generalizado, com o viés de atacar a economia ou a imagem da empresa Whatsapp, descaracterizou a motivação justificada da ordem judicial do seu objetivo real.

Mais uma vez é mister dizer que o MCI não é um instrumento específico para as questões que a legislação especial já preconiza no país. Além disso, há pontos importantes para serem analisados e revistos em razão das decisões já tomadas pela justiça de primeira instância no bloqueio judicial do *Whatsapp*.

---

de forma isolada ou cumulativa: ... III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11".

[35] Hoje tramitam no Congresso Nacional dezenas de projetos de lei para alterar o texto do MCI. (GETSCHKO, 2016).

[36] Resolução CGI.br/RES/2009/003/P.

A primeira é com relação ao pedido judicial de informações ou dados pessoais para o servidor de conteúdo do aplicativo. Não há, até o presente momento, uma regulação que delimite quem poderá ter essas informações e será o responsável por elas. A lei de proteção de dados pessoais tramita no Congresso Nacional há 11 anos.

A interpretação que se quer chegar é o limite que um ator do poder judiciário terá com essas informações pessoais e a segurança delas para que não caiam nas mãos de terceiros. Por exemplo, a disciplina do artigo 23 do MCI, não é de todo uma segurança jurídica eficaz, pois é facultado ao juiz o pedido de segredo de justiça, um delimitador parcial das informações privadas.

A reflexão aqui é com base no estado democrático de direito, pois a exigência judicial de informações privadas nos meios de comunicações digitais com motivações claras ou sigilosas pode dar ensejo a um Estado de exceção.

Diante do exposto, é perceptível que o modo de aplicação dos dispositivos pelo judiciário está em discordância com os princípios da própria lei do MCI e a Carta da República. Na atual conjuntura dos fatos a transparência deve ser diretamente proporcional ao poder e a privacidade deve ser inversamente proporcional ao poder, assim, o poder público deve urgentemente se adaptar ao paradigma novo em prol do futuro da internet no Brasil.

9. CONCLUSÃO

A pesquisa encontrou respostas norteadoras para a reflexão que motivou essa investigação científica muito mais direcionada ao contexto tecnológico da criptografia do que jurídico. Isto, na verdade, é um resultado positivo porque a causa real do imbróglio jurídico envolvendo bloqueios e suspensões de bloqueios do WhatsApp são em razão da escrita, imagem e voz secretas do mundo virtual que propagam na Internet.

Neste sentido, é importante ratificar que quase todo o quadro da segurança da informação é baseado em princípios criptográficos, logo, a inserção de *backdoors* em algoritmos criptográficos não é recomendada, pois este estratagema facilitaria a ação de *hackers* ou qualquer outro indivíduo com más intenções para a usurpação ou alteração de dados e informações.

A pesquisa ratifica que a idéia de algoritmos criptográficos abertos seria mais bem-vinda ao modelo atual porque a comunidade técnica poderia com mais facilidade auditar o *software*. No caso do algoritmo de criptografia do *WhatsApp*, apesar dele ser baseado no

protocolo *Signal* - que é aberto, a sua implementação, contudo, é fechada, obstando, assim, a auditoria por *experts*.

Com efeito, a empresa WhatsApp se encontra em um dilema. Segundo esta pesquisa científica, há a impossibilidade da abertura do código devido a segredos de interesse da empresa responsável pelo aplicativo que utiliza os algoritmos criptográficos, ensejando, assim, na única saída para provar que a empresa não tem acesso à chave para poder fornecer os dados requisitados pela Justiça brasileira, seria a auditoria dos algoritmos criptográficos por especialista externos, já mencionados anteriormente.

Importante salientar que o aplicativo *WhatsApp* é apenas um dentre diversos outros tipos semelhantes utilizados atualmente para comunicação ponta a ponta. A possibilidade de interceptação de mensagens enviadas por meio desse aplicativo pode produzir um efeito em que eventuais interessados em cometer atos ilícitos passem a se utilizar de outros meios de comunicação. Por exemplo, o desenvolvendo de aplicativos próprios para tal fim, ou até mesmo criptografando a mensagem de qualquer outra forma antes da transmissão por qualquer aplicativo.

Já a posição do STF em direcionar os questionamentos apenas no debate da criptografia ponta a ponta do aplicativo *WhatsApp*, faz com que a análise do universo de troca de mensagens criptografadas seja analisado de forma parcial. O contexto é mais amplo porque se utiliza dessa ferramenta em muitos negócios do dia-dia, por exemplo, transações do setor financeiro e bancário. Assim, a insegurança na implementação desses algoritmos com o uso de chaves "fracas", mecanismos anacrônicos, vulnerabilidades e, inclusive, *backdoors* pode trazer conseqüências negativas para a sociedade civil.

É salutar pensar que a audiência pública proposta é apenas um começo, e não o fim da discussão. Há muito que alcançar o bem comum da sociedade sobre o tema, pois no mundo computacional, em especial da Internet, há processos que são impossíveis de serem regulamentados.

Assim, a presente investigação mostrou que a única transgressão contra a Constituição da República foi a maneira como o MCI foi utilizado para fundamentar um *enforcement* na relação econômica contra a empresa WhatsApp para obedecer uma ordem judicial de investigação criminal. Segundo a consultoria norte-americana *Venture Beat*, o déficit, por exemplo, do Facebook, empresa detentora do WhatsAPP, a cada minuto fora do ciberespaço é de aproximadamente 70 mil reais, sendo que numa paralisação de 24 horas o prejuízo giraria em torno de 1,6 milhões de reais.

A posição desta investigação científica é neutra e imparcial em relação as empresas em questão, mas a jurisprudência brasileira terá que atuar com maior prudência nas suas decisões sem causar impacto negativo na sociedade civil.

Os atores públicos do judiciário possuem condições técnicas para realizar uma persecução criminal na Internet apenas com o uso de metadados, ou seja, há outros meios pela Internet de realizar uma persecução criminal. A Internet é uma rede de controle e tudo que um usuário fizer nela deixará traços, tornando-se um bom meio de combater crimes. Todavia, a prudência deve ser revista para traçar um caminho eficiente e exitoso sem causar danos colaterais.

De outra parte, a pesquisa mostrou que para a empresa WhatsApp é possível realizar as contribuições para o poder judiciário, mas há obstáculos um tanto pouco tecnológicos e mais econômicos. Resta, apenas, saber como atuar em parceria com a justiça sem infringir a liberdade de comunicação e a privacidade das informações pelo poder público.

Por fim, a regulação jurídica de protocolos de criptografia poderá obstar a inovação tecnológica no país e construir com o tempo um arcabouço legal – como estão tentando fazer com a Lei 12.965/14. E contestar os artigos do MCI com o objetivo de transformá-los em leis inconstitucionais é pensar de forma retrógrada. O STF precisa atacar a causa, e não o efeito. Será esse o caminho da Internet no Brasil? Temos fé que não.

REFERÊNCIAS

ALMEIDA, Jansen Fialho de. *Sigilo das comunicações e o devido processo legal.* ADV advocacia dinâmica: informativo, v. 28, n. 07, p. 104-103, fev.

BRASIL. Poder Judiciário do Estado de Sergipe. Juízo de Direito da Vara Criminal de Lagarto. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11065213#23%20-%20Outras%20pe%E7as%20-%2026631/2016%20-%20Of%EDcio%20n.%20141-Gab/2016%2C%20Juiz%20de%20Direito%20da%20Vara%20Criminal%20da%20Comarca%20de%20Lagarto%20-%20presta%20informa%E7%F5es%20-%20decis%E3o%20whatsapp>. Acesso em: 12 dez. 2016.

BRASIL. Poder Judiciário do Estado de Sergipe. Juízo de Direito da Vara Criminal de Lagarto. Disponível em:

<http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11117613#29%20-%20Outras%20pe%E7as%20-%2029192/2016%20-%20Of%EDcio%20n.%20141-Gab/2016%2C%20Juiz%20de%20Direito%20da%20Vara%20Criminal%20da%20Comarca%20de%20Lagarto%20-%20presta%20informa%E7%F5es%20-%20Doc2>. Acesso em: 12 dez. 2016.

CERT.BR. Cartilha de Segurança para a Internet. Disponível em: <http://cartilha.cert.br/ataques/>. Acessado em 29 jan. 2017.

CRESPO, Marcelo Xavier de Freitas; SYDOW, Spencer Toth. *Novas Tendências da Criminalidade Telemática.* Revista de Direito Administrativo - RDA, Belo Horizonte, ano 2007, n. 246, set./dez. 2007. Disponível em: http://bidforum.com.br/bidBiblioteca_periodico_telacheia_pesquisa.aspx?i=68402&p=21 Acesso em: 10 set. 2016.

CRESWELL, John W. *Projeto de pesquisa:* métodos qualitativo, quantitativo e misto. Tradução: Magda Lopes. 3ª ed. Porto Alegre: Artmed, 2010.

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.

GIL, Antonio Carlos. *Como elaborar projetos de pesquisa*. 5ª ed. São Paulo: Atlas, 2010.

GLOBO. Portal G1. Disponível em: <http://g1.globo.com/pi/piaui/noticia/2015/02/juiz-do-piaui-diz-que-whatsapp-foi-arrogante-diante-da-justica-do-brasil.html>. Acesso em: 03nov. 2016.

GITHUB. Signal Protocol library for Java/Android. Disponível em: <https://github.com/WhisperSystems/libsignal-protocol-java>. Acesso em: 30 jan. 2017.

MADALENA, Juliano. *Regulação das fronteiras da internet: um primeiro passo para uma teoria geral do direito digital.* Revista dos Tribunais, v. 974, p. 81-110, dez. 2016. Disponível em: <http://revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srg

uid=i0ad81815000001588ce2073a8f8a2b39&docguid=I3be96480a27a11e6
96fc010000000000&hitguid=I3be96480a27a11e696fc010000000000&spos
=7&epos=7&td=8&context=13&crumb-action=append&crumblabel=
Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&end Chunk=1>. Acesso em: 15 set. 2016.

GUIMARÃES, Bruno Alberto Soares. *WhatsApp: até onde vai a inserção do direito nas novas fontes tecnológicas?* ADV Advocacia dinâmica: seleções jurídicas, n. 10, p. 24-37, out. 2015.

LONGHI, João Victor Rozatti. *Marco civil da Internet no Brasil: breves consolidações sobre seus fundamentos, princípios e análise crítica do regime de responsabilidade civil dos provedores.* In: Direito privado e Internet. São Paulo: Atlas, 2014, p. 109-145.

LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo: Saraiva 2012.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. *Técnicas de pesquisa.* 7ª ed. São Paulo: Atlas, 2008.

MIGALHAS. Portal Jurídico. Disponível em: <http://www.migalhas.com.br/arquivos/2015/2/art20150227-03.pdf>. Acesso em: 11 nov. 2016.

OMCI. Observatório do Marco Civil da Internet. Disponível em: <http://www.omci.org.br/m/jurisprudencias/arquivos/2015/tjsp_22714627720158260000_17122015.pdf>. Acesso em: 02 set. 2016.

OMCI. Observatório do Marco Civil da Internet. Disponível em: <http://www.omci.org.br/m/jurisprudencias/arquivos/2016/tjse_201600110899_03052016.pdf>. Acesso em: 02 set. 2016.

OMCI. Observatório do Marco Civil da Internet. Disponível em: <http://omci.org.br/m/jurisprudencias/arquivos/2016/rj_062001642016_19072016.pdf>. Acesso em: 02 set. 2016.

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.

QUINTIERE, Víctor Minervino. *Sobre as (i)legalidades no processo penal: breve reflexão a respeito do whatsapp a partir da lei 9.296/1996: um estudo de caso.* In: Crimes federais. 2. ed. Belo Horizonte: D'Plácido, 2016. p. 451-465.

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

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.

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>. Acesso 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>. Acesso em: 27 jan. 2017.

SOUZA, Carlos Affonso Pereira de. Advogado. *O progresso tecnológico e a tutela jurídica da privacidade*. Direito, Estado e Sociedade, v. 9, n. 16, p. 6-39, jan./jul. 2000.

REINALDO FILHO, Demócrito Ramos. *Code is not law - a empresa que controla o whatsapp precisa se submeter ao império das leis nacionais*. ADV advocacia dinâmica: informativo, n. 30, p. 428-424, jul. 2016.

STF. Supremo Tribunal Federal. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11398261&ad=s#44%20-%20Decis%E3o%20monocr%E1tica>. Acesso em: 12 dez. 2016.

STF. Supremo Tribunal Federal. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=11618229&ad=s#75%20-%20Peti%E7%E3o%20-%2049503/2016%20-%20Facebook%20Servi%E7os%20Online%20do%20Brasil%20Ltda.%20-%20Presta%20informa%E7%F5es%20em%20aten%E7%E3o%20ao%20of%EDcio%20n%BA%2015305/2016%20e%20encaminha%20m%EDdia>. Acesso em: 12 dez. 2016.

BRASIL. LEI 12.965/2014. Marco Civil da Internet. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 03 jan. 2017.

STF. Supremo Tribunal Federal. Disponível em: <http://www.stf.jus.br/portal/audienciaPublica/audienciaPublica.asp?tipo=prevista>. Acesso em: 01 dez. 2016.