EXCELENTÍSSIMOS SENHORES MINISTROS RELATORES DA ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL 403 E DA AÇÃO DIRETA DE INCONSTITUCIONALIDADE 5527

Min. Edson Fachin

Min. Rosa Weber

A **ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA,** pessoa jurídica de direito privado, sem fins lucrativos, inscrita no CNPJ sob o n. 20.069.623/0001-28, com sede à Rua Antonio Bicudo, n. 238, apartamento 4, Pinheiros, CEP 05418-010 São Paulo, SP (doc. 01), vem, respeitosamente, por meio de seus representantes legais e advogados que esta subscrevem, nos autos da **ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL 403** e da **AÇÃO DIRETA DE INCONSTITUCIONALIDADE 5.527**, em atenção ao despacho conjunto publicado em 25 de abril de 2017, que admitiu a sua participação na audiência pública a ser realizada nos dias 02 e 05 de junho de 2017, apresentar a sua

CONTRIBUIÇÃO POR ESCRITO

edifício itália
avenida são luís 50
1º andar conjunto 11b
1046-000 são paulo sp brasil
www.internetlab.org.br

1. A presente manifestação tem como objetivos *(i)* oferecer dados que permitam identificar as circunstâncias nas quais tem-se determinado a suspensão de aplicações de Internet no Brasil, medida comumente chamada de "bloqueio"; e *(ii)* esclarecer as razões por trás dos descumprimentos de ordens judiciais por parte da WhatsApp Inc., que motivaram as suspensões.

I. BLOQUEIOS E SUSPENSÕES DE APLICAÇÕES DE INTERNET NO BRASIL

2. O objetivo desta seção é colocar as ordens de bloqueio do aplicativo WhatsApp em perspectiva, apresentando dados sobre as circunstâncias nas quais outras ordens de bloqueios contra aplicações de Internet foram proferidas no Brasil. Com isso, pretende-se demonstrar que há diferentes motivações que podem ensejar o recurso a esse tipo de medida, não sendo adequado proibí-la de forma genérica.

3. Os dados apresentados a seguir são resultado de trabalho de pesquisa acadêmica realizada pela equipe do InternetLab, que mapeou e analisou todas as decisões judiciais publicamente acessíveis que continham medidas de bloqueio a aplicações de Internet no Brasil. Todo o material de pesquisa encontrado foi reunido de maneira organizada na página "BLOQUEIOS.INFO".

I.1. DOS TIPOS DE BLOQUEIOS

4. Como mencionado, a plataforma **BLOQUEIOS.INFO** catalogou ordens judiciais de bloqueio completo de aplicações de Internet no Brasil. Para tanto, foram considerados casos de ***bloqueio*** aqueles em que autoridades judiciais determinaram que intermediários – como provedores de conexão, provedores de lojas virtuais de aplicativos ou registradores de nomes de domínio – procedessem à indisponibilização **integral** do acesso a conteúdos, funcionalidades, informações e/ou serviços ofertados por aplicações de Internet, como páginas

e aplicativos. Não foram consideradas ordens que tinham como objeto bloqueios parciais, isto é, a indisponibilização de trechos, partes, conteúdos ou informações específicas contidas nas aplicações em questão.

5. Nesse levantamento, foi possível identificar dois tipos principais de bloqueios: *(i)* os relacionados a descumprimento de ordens judiciais, cujo caráter é de sanção, e *(ii)* os relacionados à incompatibilidade do produto ou serviço em si com o ordenamento jurídico brasileiro, cujo caráter é de proibição.

6. **Tipo 1: bloqueios por descumprimento de ordem judicial**

Data	Aplicação	Motivo da suspensão
09/01/2007	YouTube	descumprimento de ordem judicial de retirada de conteúdo
10/08/2012	Facebook	descumprimento de ordem judicial de retirada de conteúdo
25/02/2015	WhatsApp[1]	descumprimento de ordem judicial de entrega de dados
16/12/2015	WhatsApp[2]	descumprimento de ordem judicial de entrega de dados
02/05/2016	WhatsApp[3]	descumprimento de ordem judicial de entrega de dados

[1] A decisão do juiz Luiz de Moura Correia da Central de Inquéritos de Teresina (Piauí), julgada em 11/02/2015 e originada nas Ações Penais Públicas n. 0013872-87.2014.8.18.0140 e 007620-68.2014.8.18.0140.
[2] A decisão da juíza Sandra Regina Nostre Marques da 1ª Vara Criminal de São Bernardo do Campo (São Paulo), julgada em 16/12/2015 e originada do Procedimento de Interceptação Telefônica n. 0017520-08.2015.8.26.0564.
[3] A decisão do juiz Marcel Maia Montalvão da Vara Criminal de Lagarto (Sergipe), julgada em 26/04/2016 no processo nº 201655090027.

19/07/2016	WhatsApp[4]	descumprimento de ordem judicial de entrega de dados
05/10/2016	Facebook	descumprimento de ordem judicial de retirada de conteúdo

7. Nos casos apresentados acima, que envolvem as aplicações "YouTube", "Facebook" e "WhatsApp", a tabela demonstra que o que motivou as ordens de bloqueio foi o descumprimento de ordens judiciais, seja por falha em remover conteúdo íntimo (YouTube), em remover propaganda contrária à Lei das Eleições (Facebook) ou em entregar dados de usuários alvos de interceptação (WhatsApp). Todas as decisões foram reformadas por tribunais superiores.

8. **Tipo 2: bloqueios por incompatibilidade com o ordenamento jurídico brasileiro**

Data	**Aplicação**	**Motivo do bloqueio**
04/12/2013	Tubby	potencial exposição a danos à honra e violência psicológica
19/08/2014	Secret	violação da proibição constitucional ao anonimato e facilitação de danos à honra
28/04/2015	Uber	oferta de serviço de transporte clandestino
29/07/2015	Tudo sobre Todos	violação a normas de proteção de dados pessoais

[4] A decisão da juíza Daniela Barbosa Assumpção de Souza da 2ª Vara Criminal de Duque de Caxias (Rio de Janeiro), julgada em 19/07/2016 e originada no Inquérito Policial 062-00164/2016.

13/10/2016	Armagedomfilmes.biz, Filmesonlinegratis.net e Megafilmeshd20.org	divulgação de conteúdo em violação a direito autoral

9. Já em (ao menos) outras cinco diferentes oportunidades, autoridades judiciais brasileiras consideraram que as aplicações *Tubby*, *Secret*, *Uber*, *Tudo sobre Todos*, *Mega Filmes HD*, *Armagedom Filmes, Filmes Online Grátis*, estariam oferecendo serviços incompatíveis com o ordenamento jurídico brasileiro e, por essa razão, deveriam ser bloqueadas. Os motivos variam, como se pode ver na tabela acima. As ordens de bloqueio envolvendo *Secret* e *Uber* foram posteriormente revertidas, uma vez que os tribunais superiores reformaram os entendimentos de primeira instância, decidindo que não existia ilegalidade nos serviços oferecidos.

10. A existência desse segundo grupo de casos demonstra que há circunstâncias nas quais o bloqueio de aplicações pode ser legitimamente determinado. Isso porque quando houver comprovada incompatibilidade entre determinado produto ou serviço e o ordenamento jurídico brasileiro, o bloqueio ao seu acesso ou funcionamento pode ser a medida adequada para coibir violações de direitos. Seria o caso de uma aplicação que se destinasse exclusivamente à disseminação de conteúdos ligados à pornografia infantil, por exemplo.

11. Contudo, embora a taxonomia apresentada acima justifique o recurso à medida de bloqueio em alguns casos, os dados também apontam para um aumento significativo do número de ordens de bloqueio ligadas ao primeiro grupo de casos, que envolvem o descumprimento de ordens judiciais. A determinação de bloqueio de aplicações de Internet nesses casos é alarmante na medida em que a sua aplicação traz sérias repercussões para direitos humanos, para a economia e para a infraestrutura da Internet.

12. No que tange a direitos humanos, essas repercussões estão diretamente ligadas às restrições à liberdade de expressão do pensamento, de comunicação e de acesso à informação, mas, também, indiretamente relacionam-se a outros direitos sociais, políticos e econômicos. Todos

estes direitos podem ter sua tutela minorada por conta da indisponibilização do acesso a aplicações de Internet.

13. No que tange à economia, essas repercussões se relacionam a desincentivos à inovação e à atividade econômica que podem surgir em razão de eventuais intervenções excessivas no uso que agentes econômicos fazem de aplicações de Internet no curso de seus negócios, bem como na liberdade de iniciativa de criação de novas aplicações parecidas ou relacionadas a serviços que estejam em áreas povoadas por incertezas e impasses jurídicos.

14. Já no caso das repercussões atinentes à infraestrutura da Internet, pode-se dizer que ordens de bloqueio vão de encontro a aspectos próprios da arquitetura da rede, global e descentralizada. Isso significa que intervenções que inviabilizem completamente a atuação de determinados provedores de aplicações podem ter consequências para além dos provedores ou serviços em questão. Por exemplo, uma ordem judicial para bloquear uma aplicação pode impactar em outro serviço caso haja uma relação de dependência ou interconexão entre eles.

15. As ordens de bloqueio direcionadas ao aplicativo "WhatsApp", uma das quais constitui objeto de apreciação da ADPF 403, pertencem ao primeiro grupo de casos. Como demonstrar-se-á a seguir, **a determinação de bloqueio de aplicações de Internet como sanção a descumprimento de ordens judiciais de entrega de dados de usuários é inconstitucional**.

I.2. BLOQUEIOS CONSTITUCIONAIS E INCONSTITUCIONAIS

16. Como visto, bloqueios de aplicações de Internet, *per se*, impedem que usuários tenham controle completo sobre a sua experiência na Internet, afetando a sua liberdade de procurar, receber e comunicar ideias e informações.[5] Em outras palavras, a medida, por sua própria

[5] A Declaração Universal de Direitos Humanos, ao art. 19, dispõe que: "Todo ser humano tem direito à liberdade de opinião e expressão; esse direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e idéias por quaisquer meios e independentemente de fronteiras." Nesse sentido, todo bloqueio importa em limitação da liberdade de expressão e comunicação.

natureza, compromete o livre fluxo de dados em um país ou região e o acesso de milhões de pessoas a informações e serviços.

17. Ao interferir na capacidade dos usuários de Internet de poder navegar livremente por páginas ou aplicativos, os bloqueios de aplicações impõem, sempre, uma **restrição de sua liberdade de comunicação**, prevista no art. 5, inciso IX da Constituição Federal:

> "IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;".

18. Contudo, o mero fato de bloqueios representarem uma restrição a direitos fundamentais não significa que sejam necessariamente inconstitucionais. Há circunstâncias nas quais essa restrição à liberdade de comunicação pode ser considerada admissível e, portanto, constitucional. São os casos, por exemplo, de bloqueios decorrentes de incompatibilidade com o ordenamento jurídico brasileiro (tipo 2).

19. Em suma, nesses casos, a constitucionalidade da restrição decorre de três fatores principais:

i. **a ilegalidade das páginas ou aplicações bloqueadas:** as atividades desempenhadas por aplicações ou páginas de Internet que são primordialmente dedicadas a atividades ilícitas, como a divulgação de pornografia infantil ou de materiais protegidos por direitos autorais não são autorizadas de acordo com o ordenamento jurídico brasileiro, razão pela qual não há fundamento legal para sustentar a manutenção de seu acesso;

ii. **a inexistência de medidas efetivas menos gravosas:** para fazer cessar as violações de direitos ensejadas pelas páginas ou aplicações atacadas é necessário impedir o seu acesso de forma integral, não havendo mecanismos menos restritivos para se alcançar o mesmo resultado;

iii. **a legitimidade do propósito da medida:** tais ordens de bloqueio são emanadas para fazer cessar o funcionamento de páginas ou aplicações que são proibidas civil ou criminalmente, havendo, portanto, um fundamento legítimo para a sua determinação.

20. Nesse sentido, apesar de ordens de bloqueio de páginas que veiculam pornografia infantil ou dados pessoais ilegalmente coletados (como o "*Tudo Sobre Todos"*) acarretarem *restrição* na liberdade de comunicação, não há que se falar em inconstitucionalidade da medida.

21. Contudo, a conclusão é oposta nos casos de bloqueio de aplicações que servem como sanção ao descumprimento de ordens judiciais para entrega de dados de usuários (tipo 1). Isso porque, nesses casos, de acordo com os fatores elencados acima:

i. **não há ilegalidade nas atividades desempenhadas pelas páginas ou aplicativos:** quando determinadas como sanção ao descumprimento de ordens judiciais, os bloqueios não se baseiam na ilegalidade das atividades precipuamente desempenhadas; ao contrário, as plataformas já afetadas por ordens de bloqueios deste tipo (YouTube, Facebook e WhatsApp) não só encontram total respaldo na liberdade de iniciativa, como servem a finalidades que potencializaram o exercício de direitos fundamentais, sobretudo a liberdade de expressão.

ii. **há medidas alternativas, eficazes e menos gravosas:** o ordenamento jurídico brasileiro prevê outras medidas coercitivas para ensejar o cumprimento de ordens judiciais brasileiras como a imposição de astreintes, que, respeitados os procedimentos cabíveis, podem ser executadas perante ordenamentos jurídicos estrangeiros, ou ainda, no caso específico da entrega de dados de usuários para investigações criminais, a utilização dos procedimentos previstos nos acordos de cooperação judiciária internacional, segundo os quais ordens de autoridades brasileiras poderão contar com o poder coercitivo de autoridades estrangeiras;

iii. **a falta de legitimidade do propósito da medida:** como não se destinam a fazer cessar o acesso a atividades ilegais, mas sim de impor sanção pelo descumprimento de ordens judiciais, sanção essa que não encontra previsão legal expressa, não há fundamento legítimo para a utilização das medidas nesses casos.

22. Diante disso, ao contrário das ordens de bloqueio decorrentes de páginas e aplicações precipuamente dedicadas à realização de atividades incompatíveis com o ordenamento jurídico brasileiro que, em princípio, podem ser consideradas constitucionais, as ordens de bloqueio decorrentes do descumprimento de ordens judiciais de entrega de dados de usuários implicam restrições inconstitucionais da liberdade de comunicação, garantida pela Constituição Federal.

23. Vai nesse mesmo sentido a tese principal da ADPF 403, proposta pelo Partido Popular Socialista (PPS) contra a decisão do juiz Marcel Maia Montalvão da Vara Criminal de Lagarto, que proferiu a terceira decisão de bloqueio do WhatsApp, defendendo a existência de violação ao preceito fundamental à comunicação, protegido pelo art. 5, IX, da CF, quando o bloqueio do aplicativo WhatsApp é ordenado. A declaração de violação a preceito fundamental impediria novas decisões semelhantes, coibindo, portanto, que sejam impostas futuras restrições inconstitucionais à liberdade de comunicação.

I.3. DOS FUNDAMENTOS LEGAIS DOS BLOQUEIOS DE APLICAÇÕES POR DESCUMPRIMENTO DE ORDENS JUDICIAIS

24. A ADI 5527, proposta pelo Partido da República (PR), pugna pela declaração de inconstitucionalidade dos incisos III e IV do art. 12 da Lei n. 12.965/14 (“Marco Civil da Internet”), que prevê sanções como “suspensão” e “proibição” a provedores, ao lado da interpretação conforme do art. 10, §2º, que dispõe sobre a disponibilização de conteúdo de mensagens mediante ordem judicial.

25. Diante das questões levantadas na ADI, cabe resgatar as disputas interpretativas a respeito da existência de amparo legal para a determinação de ordens de bloqueio de aplicações no Brasil por parte do Poder Judiciário.

26. Especificamente em relação aos dispositivos do Marco Civil da Internet, da leitura do artigo 12, depreende-se que:

i. para que as sanções previstas sejam cabíveis, é necessária a existência de "infrações às normas previstas nos arts. 10 e 11; e
ii. as sanções de "suspensão temporária" ou "proibição" se referem às atividades que envolvam "operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet", como mencionado no art. 11.

27. Em relação ao ponto *(i)*, discute-se se o descumprimento de ordens judiciais de entrega de dados de usuários é infração que está abarcada pelos arts. 10 e 11, aos quais o *caput* do art. 12 faz clara referência.

28. Para aqueles que advogam por uma interpretação mais restritiva das sanções previstas pelo dispositivo, a sua aplicação somente poderia ser ensejada pelo desrespeito a normas de proteção de dados e da privacidade estabelecidas nos arts. 10 e 11. De acordo com essa linha de argumentação, nos casos envolvendo o aplicativo WhatsApp, como a empresa não teria violado nenhuma dessas normas propriamente, a sanção não seria cabível.

29. Em contraposição, para aqueles que defendem uma interpretação mais abrangente do dispositivo, qualquer violação à legislação brasileira seria suficiente para provocar a aplicação das sanções do art. 12. Isso porque o art. 11 estabeleceria a obrigação de respeito à legislação brasileira de forma geral, não estando adstrita aos casos de proteção de dados e privacidade. Nesse sentido, o art. 10, §2º, ao determinar que a entrega de dados de usuários se dê mediante

ordem judicial, também estabeleceria uma obrigação por parte das empresas de entregá-los quando houver ordem. Disso decorre que a não entrega de dados importaria violação à legislação brasileira, tornando aplicável, portanto, as sanções previstas no art. 12.

30. Em relação ao ponto *(ii),* a divergência está na extensão da "suspensão temporária" do inciso III (ou mesmo da "proibição" do inciso IV) ali prevista: admite o bloqueio completo de aplicação ou apenas de certas atividades? O WhatsApp pode ser suspenso completamente ou apenas a atividade que violaria a legislação brasileira?

31. O texto do dispositivo se refere a "atividades que envolvam os atos previstos no art. 11". Em face disso, muitos argumentam que o art. 12 autoriza apenas a suspensão de certas atividades de "coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet" que estiverem em desacordo com as normas de proteção de dados e da privacidade do Marco Civil da Internet.

32. Em contrapartida, outros afirmam que ordens de bloqueio são admissíveis pela legislação brasileira, sendo o disposto no art. 12 uma mera confirmação dessa prerrogativa. Além disso, no caso de muitas páginas e aplicativos, a suspensão de atividades de "coleta, armazenamento, guarda e tratamento …de comunicações", não poderia ser feita de maneira separada do oferecimento do serviço, culminando, invariavelmente, na restrição integral de acesso.

33. De fato, independentemente da resolução das controvérsias mencionadas, há outros fundamentos legais que poderiam amparar ordens de bloqueio de aplicações no Brasil, como o "poder geral de cautela", previsto nos arts. 139, IV e 536 § 3º do Novo Código de Processo Civil ou o art. 3º do Código de Processo Penal, em conjugação com o art. 297 do Novo Código de Processo Civil.

II. DAS IMPOSSIBILIDADES JURÍDICA E TÉCNICA ALEGADAS PELO WHATSAPP

34. Em todos os casos ocorridos até hoje, os bloqueios do WhatsApp foram determinados como medida de constrangimento para que a empresa Facebook Brasil cooperasse com a Justiça brasileira entregando dados de comunicações de usuários do aplicativo. À base da disputa[6] encontram-se duas questões principais: *(i)* uma de natureza jurídica, sobre os limites da jurisdição brasileira sobre uma empresa sediada no exterior; e *(ii)* uma de natureza técnica, sobre os obstáculos colocados pela criptografia de ponta-a-ponta ao acesso a informações de usuários. Essas questões podem ser assim resumidas:

- **Jurisdição.** Como a empresa WhatsApp Inc. não possui sede no Brasil, o Poder Judiciário tem oficiado a empresa "Facebook Serviços Online do Brasil Ltda." com os pedidos, entendendo que ela deve responder pela WhatsApp no Brasil, já que, desde a aquisição do aplicativo pela Facebook Inc., as empresas fazem parte do mesmo grupo econômico. A empresa brasileira responde aos pedidos informando que é pessoa jurídica distinta da WhatsApp Inc. e que não tem poder de controle sobre o serviço de mensagens ofertado por tal empresa. O argumento é recorrentemente rechaçado pelo Poder Judiciário. não aceitam tal argumento. Estes também se recusam a recorrer ao acordo de cooperação mútua em matéria penal (MLAT) entre Brasil e Estados Unidos para alcançar a WhatsApp Inc., afirmando que investigam crimes ocorridos no Brasil por brasileiros, e que a empresa deve se submeter à jurisdição brasileira se oferece serviços no Brasil, sem necessidade de seguir os procedimentos do acordo internacional com os Estados Unidos. Estes foram os termos principais da discussão nos dois primeiros casos de ordens de bloqueio contra o WhatsApp, anteriores à implementação de criptografia.

[6] Ver ABREU, Jacqueline de Souza, "From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp", *Columbia Journal of Transnational Law Online Edition*, 17.10.2016, disponível em http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/. Acesso em: 20.01.2017.

- **Criptografia de ponta-a-ponta.** Principalmente após a divulgação da implementação da criptografia de ponta-a-ponta pelo WhatsApp em abril 2016, essa técnica de proteção de confidencialidade de mensagens também se tornou uma das variáveis por trás das ordens de bloqueio. Já na terceira decisão de bloqueio, o juiz demonstrou duvidar da alegação da empresa de que seria impossível interceptar mensagens em razão da criptografia adotada, citando manifestações da polícia brasileira acerca da possibilidade. No quarto caso, a juíza ordenou explicitamente que a empresa deveria "desabilitar a chave de criptografia" e assim proceder à interceptação de mensagens. Segundo esses juízes, o interesse público na garantia da segurança pública se sobrepõe ao interesse privado na confidencialidade das mensagens em investigações. Para eles, uma tecnologia que impede a realização de interceptações contrariaria a Constituição brasileira.

35. Tais questões permanecem em aberto na doutrina e na jurisprudência. O foco da discussão tem se dado primordialmente em termos da correição das ordens de bloqueio. Sintomático disso é o fato de que, em todos os casos, a ordens de bloqueio do WhatsApp foram cassadas por tribunais superiores algumas horas depois com base em alegado desrespeito ao princípio da proporcionalidade, aos fundamentos do Marco Civil da Internet e, mais recentemente, em decisão desta C. Corte, por aparente violação da liberdade de comunicação.[7] Os tribunais superiores não tomaram posição quanto às disputas subjacentes, mas somente quanto à medida de bloqueio em si. Isso tem determinado o foco da discussão brasileira sobre o assunto.

[7] Nos dois primeiros casos, os desembargadores recorreram ao princípio da proporcionalidade para suspender a medida. No terceiro caso, além de apontar a desproporcionalidade, o desembargador contestou a adequação da medida com o Marco Civil da Internet. No caso mais recente, quando interveio o Supremo Tribunal Federal, o ministro concedeu a liminar também nesse sentido: é desproporcional e parece estar em desacordo com o Marco Civil da Internet e a liberdade de comunicação. Sobre isso, ver análises disponíveis em bloqueios.info, portal do InternetLab.

II.1. IMPOSSIBILIDADE JURÍDICA: QUESTÕES DE JURISDIÇÃO

36. O *caput* do art. 11 do "Marco Civil da Internet" determina que provedores de conexão e aplicações de Internet devem respeitar a "legislação brasileira e os direitos à privacidade, à proteção de dados pessoais e ao sigilo das comunicações privadas e dos registros" "em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações em que pelo menos um desses atos ocorra em território nacional". Nos parágrafos que seguem, a lei esclarece que a obrigação de respeitar a legislação brasileira no tratamento de dados se aplica

i. aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil (art. 11, §1º); e

ii. mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil (art. 11, § 2º).

37. O escopo delineado no artigo atinge empresas com sede fora do país e por isso se diz ter alcance extraterritorial. Literalmente, o artigo institui o dever de que mesmo essas empresas estrangeiras respeitem a legislação nacional em atividades de tratamento de dados. Na prática, entretanto, ele tem sido utilizado para exigir que também observem a legislação material e processual brasileira relativa ao acesso de autoridades a dados de usuários.[8] De fato, estudos sobre o processo de elaboração do Marco Civil da Internet indicam que essa redação abrangente tentou justamente endereçar dificuldades práticas para obtenção de acesso a dados por parte de autoridades, porquanto, sob o argumento de que os dados estariam guardados no exterior,

[8] Este argumento é elaborado, por exemplo, em BARRETO, Alesandro Gonçalves; WENDT, Emerson. "Marco Civil da Internet e Acordos de Cooperação Internacional: análise da prevalência pela aplicação da legislação nacional aos provedores de conteúdo internacionais com usuários no Brasil", Direito & TI, 30.08.2015, disponível em: http://direitoeti.com.br/artigos/mlat-x-marco-civil-da-internet/ Acesso em: 25.01.2017.

obedecendo, portanto, à legislação de outro país e só podendo ser obtidos por procedimento de assistência judiciária internacional específico, provedores não atendiam a ordens judiciais de quebra de sigilo.[9]

38. A inclusão desses dispositivos não estancou o problema e pode até tê-lo piorado. Afinal, uma das forças por trás de bloqueios do aplicativo WhatsApp, para além da criptografia, foi justamente a recusa da empresa em fornecer dados a autoridades brasileiras fora dos mecanismos de cooperação internacional.[10]

39. Empresas como Google,[11] Microsoft,[12] Yahoo[13] e Facebook[14] já estiveram envolvidas em disputas judiciais semelhantes.

[9] Segundo o relator do projeto, Deputado Alessandro Molon, "as modificações foram promovidas tendo em vista que já há questionamentos em relação a qual é a jurisdição aplicável quando os dados de brasileiros estão localizados no exterior. Não é incomum se ouvir que não se aplica a lei brasileira à nossa proteção quando nossos dados estão localizados no exterior. Para dirimir dúvidas, acolhendo sugestão do Governo, optamos por incluir este dispositivo no Marco Civil da Internet". Ver MADRUGA, Antenor; FELDENS, Luciano. Dados Eletrônicos e cooperação internacional: limites jurisdicionais in: MINISTÉRIO PÚBLICO FEDERAL, Temas de Cooperação Internacional, 2ª Edição revista e ampliada, vol. 2, Brasília: MPF, pp. 49-70, 2016, p. 64; BRITO CRUZ, Francisco de Carvalho. Direito, Democracia e Cultura Digital: a experiência de elaboração legislativa do Marco Civil da Internet. Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade de São Paulo, 2015, p. 114.

[10] Ver ABREU, Jacqueline de Souza, From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp", *Columbia Journal of Transnational Law Online Edition*, 17.10.2016, disponível em http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/. Acesso em: 20.01.2017.

[11] SUPERIOR TRIBUNAL DE JUSTIÇA, Inquérito n. 784-DF, Min. Laurita Vaz, julg. 17.03.13, decisão de processo em que a Google Brasil Internet Ltda. impetrou mandado de segurança contra ofício da Polícia Federal pelo qual se requisitou a quebra de sigilo telemático de contas do gmail.

[12] SUPERIOR TRIBUNAL DE JUSTIÇA, Recurso em Mandado de Segurança nº 46.685/MT. Min. rel. Leopoldo de Arruda Raposo, julg. 26.03.2015.

[13] MPF/SP pede condenação da Yahoo! Brasil por desobediência a ordens judiciais, JusBrasil, Procuradoria Geral da República. Disponível em: https://pgr.jusbrasil.com.br/noticias/147375302/mpf-sp- pede-condenacao- da-yahoo- brasil-por-desobediencia-a- ordens-judiciais. Acesso em: 19.01.2017; JUSTIÇA FEDERAL. Processo nº 0012450-95.2014.403.6100. Juíza Federal Sílvia Figueiredo Marques, julg. 13.05.2015.

[14] O processo nº 0013254-29.2015.4.03.6100 relativo à Ação Civil Pública proposta pelo MPF contra a Facebook Brasil pode ser acompanhado na plataforma Observatório do Marco Civil da Internet, em http://omci.org.br/jurisprudencia/117/descumprimento-de-ordem-de-autoridade/ . A decisão mais recente do Tribunal Regional Federal da 3ª Região é de 20 de julho de 2016. Em 26 de janeiro de 2017, foi admitido recurso especial do MPF ao STJ. Ver também "MPF deve obter dados do Facebook nos EUA por tratado", Jota, 02.12.2016. Disponível em: http://jota.info/justica/mpf-deve-obter- por-tratado- dados-de- rede-social- diz-juiz-02122016. Acesso em: 19.01.2017.

40. Para entender as origens do embate entre autoridades e empresas de Internet, é preciso considerar o fator da jurisdição, conceito básico de direito internacional público, que pode ser compreendido como a autoridade de exercer poder sobre pessoas e coisas em um determinado território.[15] Como um Estado detém jurisdição dentro de seus limites geográficos, tornou-se necessária a instrumentalização de meios de cooperação internacional para situações em que autoridades públicas de um Estado-nação esbarram nos limites de seu poder, como quando precisam extraditar suspeitos, ouvir testemunhas ou colher provas que se encontram no exterior.[16]

41. Para este fim, são tradicionalmente utilizadas cartas rogatórias e celebrados acordos de cooperação mútua entre países, por exemplo. O Brasil faz parte de mais de 30 acordos bilaterais e multilaterais de assistência judicial recíproca em matéria penal. Especificamente em relação aos Estados Unidos, o Brasil possui acordo bilateral de assistência judiciária em matéria penal, consubstanciado no Decreto nº 3.810/2001.

42. Esse modelo funcionou com sucesso – e, na maior parte das situações, ainda funciona – por duas razões centrais. Primeiro, porque, em geral, é um esquema idealizado para situações raras e excepcionais. Na grande maioria dos processos, não há que se realizar extradições, ouvir testemunhas estrangeiras nem obter provas no exterior. Segundo, porque a identificação dos limites da jurisdição e da necessidade de se recorrer a meios de cooperação é relativamente simples para meios físicos: se autoridades do país A precisam de pessoas ou documentos fisicamente localizados no território do país B, o país A necessariamente precisa solicitar cooperação do país B, já que não pode exercer poder fora de seu território.

43. A questão complexificou-se com a Internet. Primeiro, porque a necessidade de colheita de *provas digitais* armazenadas em computadores no exterior ou detidas por empresas sediadas

[15] Ver ACCIOLY, Hildebrando; SILVA, G. E. do Nascimento; CASELLA, Paulo Borba. Manual de Direito Internacional Público. 18ª Edição. São Paulo: Saraiva, 2010, p. 321.
[16] SOUZA, Carolina Yumi de. "Cooperação jurídica internacional em matéria penal: considerações práticas", *RBCCRIM*, vol. 71, pp. 297-325, 2008, p. 300.

no exterior se tornou atividade cotidiana. Segundo, porque "documentos digitais" (dados em geral como informações cadastrais, registros, conteúdo de comunicações), ao mesmo tempo em que de fato estão localizados em servidores físicos em (ao menos um) lugar certo, também podem ser acessados remotamente de diversos lugares do mundo.

44. Além disso, as "pessoas" que detém o controle sobre os servidores onde os dados estão armazenados e/ou sobre o acesso a eles, os provedores de aplicações de Internet, estão presentes multinacionalmente, seja por sedes e subsidiárias ou mesmo virtualmente.

45. Quando se recusam a fornecer dados de usuários mediante direta requisição e/ou ordem de autoridade brasileira, fora dos trâmites dos acordos de cooperação internacional, empresas de Internet se baseiam nas doutrinas clássicas a partir das quais se edificaram os limites jurisdicionais e a construção de acordos de cooperação mútua – os fatos de que os dados buscados como evidência digital estão fisicamente armazenados no exterior e/ou detidos por pessoa estrangeira. **Não se desafia a soberania nacional do país quando assim o fazem; pelo contrário, o modelo de cooperação internacional foi pensado para conciliar o respeito a diferentes nações**.

46. Ao mesmo tempo, fato é que os acordos de cooperação mútua, no molde como funcionam hoje, são burocráticos e demorados e intrinsecamente pensados na territorialidade *física.* Não atendem mais às necessidades legítimas de autoridades de segurança pública no âmbito de investigações criminais, cada vez mais dependentes de informações e dados em formato *digital* detidas por provedores de aplicações de Internet estrangeiras. Pedidos de cooperação podem levar anos para serem atendidos, se o forem, comprometendo severamente o sucesso de investigações.

47. É neste cenário que se compreende a emergência de leis *extraterritoriais* ou pelo menos de interpretações *extraterritoriais* do escopo de obrigações de cooperação com autoridades estatais na entrega de dados de usuários, como as relacionadas ao art. 11 do Marco Civil da

Internet. Autoridades enxergam nela a obrigação de cooperação *direta*, fora e independente dos acordos internacionais, mediante observância apenas da legislação processual brasileira.

48. Isto tem colocado provedoras transnacionais de serviços de Internet em situações delicadas, quando as diferentes legislações nacionais a que estão simultaneamente submetidas estão em conflito, isto é, quando obedecer a uma implica desrespeitar outra. É frequentemente este o caso do embate do Brasil com empresas estadunidenses, já que a legislação aplicável ao fornecimento de dados de usuários a autoridades naquele país **proíbe provedores de entregar *conteúdo* de comunicações sem a apresentação de uma ordem** emanada pelo Poder Judiciário estadunidense (*"warrant"*).[17]

49. Para remediar esta situação, é necessário reformular o atual modelo de cooperação judiciária internacional em matéria penal e repensar os fatores definidores de jurisdição sobre dados digitais como elementos de prova, atendendo às necessidades de autoridades de segurança pública ao redor do mundo e respeitando direitos humanos. Enquanto isso não ocorre, ameaças de multas, prisões, bloqueios, além de inúmeros acordos "informais"[18] entre

[17] Nesse sentido, a legislação estadunidense prevê, no "*Stored Communications Act (18 U.S. Code § 2702)": "(a)Prohibitions.—Except as provided in subsection (b) or (c)—(1)a person or entity providing an electronic communication service to the public* ***shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service****; (b)Exceptions for disclosure of communications.—A provider described in subsection (a)* ***may divulge the contents of a communication****— (8)****to a governmental entity****, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.". Complementarmente, prevê ainda que: "18 USC §2711 (4)* ***the term "governmental entity" means a department or agency of the United States*** *or any State or political subdivision thereof.*"

[18] Um exemplo disso é o acordo entre a Polícia Federal e a empresa canadense "Research in Motion", fabricante do celular Blackberry. Segundo notícias, no âmbito da Lava Jato, mensagens do doleiro Alberto Youssef, só foram acessadas "porque [a PF] conseguiu convencer a BlackBerry a franquear acesso às conversas feitas por BBM, serviço de mensagens instantâneas dos aparelhos da marca". Ver FOLHA DE SÃO PAULO, "PF quer instalar vírus em telefone grampeado para copiar informações", publicada em 27.04.15. Disponível em: http://www1.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml Acesso em 03.02.2017. Esse "canal direto" "dribla" acordos internacionais de cooperação mútua, já que sequer passam pelo Ministério da Justiça. Ver mais sobre a controvérsia em CANÁRIO, Pedro, "Relação direta entre PF e empresa canadense alarma advogados da 'lava jato'", Consultor Jurídico, 10.11.2015, disponível em: http://www.conjur.com.br/2015-nov-10/relacao-entre-pf-empresa-canadense-alarma-advogados-lava-jato Acessado em: 03.02.2017.

empresas e autoridades serão frequentes. É de suma importância que, em nome da resolução definitiva destes impasses entre empresas de Internet e autoridades brasileiras, o Judiciário nacional acene, em suas decisões, para a importância da participação do Estado brasileiro na negociação de arranjos jurídicos de direito internacional que dêem conta das novas inovações adotadas em larga escala pela população.

50. Por fim, vale destacar que Nota Técnica de autoridades do Ministério Público já relatou que "[o] argumento de que têm sede no exterior e que, por isto, só devem cumprir decisões judiciais emitidas por autoridades de seus países, tem sido reiteradamente utilizado por empresas como Facebook e WhatsApp."[19]

51. Em que pese o argumento da *impossibilidade técnica* - a criptografia de ponta-a-ponta - ter ganhado o centro do debate, o argumento da impossibilidade jurídica persiste e ainda é utilizado para casos em que não há obstáculos técnicos, como os que dizem respeito ao acesso a "metadados" (nome técnico de um tipo de informação sobre uma comunicação - como remetente, destinatário, horário etc -, não se confundindo com seu conteúdo), como aqueles definidos pelo Marco Civil da Internet como "registros de acesso à aplicação de Internet" ou "registros de conexão".

II.2. IMPOSSIBILIDADE TÉCNICA: CRIPTOGRAFIA DE PONTA A PONTA

52. A criptografia é uma técnica de segurança que garante a confidencialidade de dados contra terceiros, isto é, não-destinatários do conteúdo comunicado e, principalmente, daqueles mal-intencionados e bisbilhoteiros. Por ter como finalidade proteger informações sensíveis, aquelas

[19] Ministério Público e Conselho Nacional de Procuradores, "Nota técnica sobre o descumprimento da legislação brasileira que regulamenta o uso da internet", disponível em: http://www.mpm.mp.br/portal/wp-content/uploads/2016/07/nota-tecnica-sobre-crimes-ciberneticos.pdf Acesso em: 03.02.2017.

de cuja exposição pode decorrer dano, técnicas de criptografia foram desenvolvidas originalmente no âmbito de agências estatais para a proteção de comunicações e dados de Estados-nações contra vigilância alheia.

53. Uma vez que o interesse em proteger a confidencialidade e a segurança de dados extrapola as esferas estatais, o desenvolvimento e emprego desta tecnologia logo foram encampados por empresas privadas e indivíduos. Com isso, informações sensíveis comunicadas por empresas privadas e indivíduos, e não só de Estados, também passaram a poder ser protegidas contra terceiros mal-intencionados e bisbilhoteiros.

54. O efeito colateral dessa utilização por empresas e indivíduos é a imposição de um obstáculo a autoridades estatais para a coleta de informações antes disponíveis pelo emprego de métodos tradicionais de vigilância. Nesse sentido, os embates de autoridades brasileiras com o WhatsApp é reflexo da disponibilização de um tipo de criptografia que é empregado por mais de um bilhão de pessoas no mundo, e, no caso do Brasil, por 90% dos usuários de *smartphones*. A popularização do uso da criptografia não é recebida apaticamente por parte de autoridades cuja atribuição é a obtenção de informações no âmbito de atividades de inteligência e investigações criminais.[20]

55. O que agrava os embates de autoridades com o WhatsApp, além de sua própria popularidade no Brasil, é a estrutura de funcionamento aplicativo. Além de proteger as comunicações com criptografia de ponta-a-ponta, a empresa WhatsApp Inc. não guarda comunicações de usuários em servidores.[21] Em razão destas duas características, mesmo tendo preenchido os requisitos do que se considera uma quebra de sigilo legítima, que é a existência

[20] Ver "A relação do Brasil com a criptografia", apresentação de Jacqueline de Souza Abreu, no CGI, VII Seminário de Proteção à Privacidade e aos Dados Pessoais. Vídeo disponível: https://www.youtube.com/watch?v=iqkTwt55HPs Apresentação disponível: http://www.internetlab.org.br/wp-content/uploads/2016/08/cgi_critptografia_jsa.pdf Acesso 15.02.2017.

[21] Segundo a política de privacidade do WhatsApp, "Não guardamos suas mensagens durante a prestação dos Serviços. Depois que suas mensagens (incluindo conversas, fotos, vídeos, mensagens de voz e compartilhamento de informações de localização) são entregues, elas são excluídas de nossos servidores." Disponível em: https://www.whatsapp.com/legal/?l=pt_br#privacy-policy-information-we-collect Acesso em: 15.02.2017.

de uma suspeita individualizada de envolvimento em um crime atestada por ordem judicial, é impossível tecnicamente conseguir acesso ao conteúdo das comunicações.

56. A WhatsApp Inc., entretanto, não está sujeita a nenhuma obrigação legal explícita de criar seu aplicativo de forma a ser capaz de realizar interceptações, ou seja, de ter a possibilidade de capturar conteúdo de comunicações em tempo real.[22] Embora, no caso das empresas provedoras de serviços de telefonia, normas da ANATEL exijam que mantenham à disposição recursos tecnológicos e facilidades necessárias para a suspensão de sigilo das telecomunicações, decorrente e nos limites de ordem judicial, e que elas próprias devem arcar com os custos financeiros de tais tecnologias, tais obrigações não se aplicam a provedores de aplicações de Internet.

57. Não há, portanto, na legislação brasileira, qualquer vedação à utilização de tecnologias de criptografia ou qualquer obrigação de se criar mecanismos de acesso ao conteúdo das comunicações transmitidas.

58. Na prática, a empresa é apenas capaz de auxiliar autoridades com a entrega de informações cadastrais e metadados. Assim, apesar de a criptografia ser um obstáculo para interceptações de conteúdo, isto é, o monitoramento em tempo real de mensagens por cooperação do WhatsApp, tais informações cadastrais e metadados ainda podem ser obtidos.

WhatsApp	Informações cadastrais[23]	Metadados[24]	Conteúdo

[22] Ver ABREU, Jacqueline de Souza, From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp", *Columbia Journal of Transnational Law Online Edition*, 17.10.2016, disponível em http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/. Acesso em: 20.01.2017.

[23] Segundo a política de privacidade do WhatsApp são dados da conta o número cadastrado, o nome do perfil, foto do perfil e mensagem de status. Disponível em: https://www.whatsapp.com/legal/?l=pt_br#privacy-policy-information-we-collect Acesso em: 15.02.2017.

[24] Segundo a política de privacidade do WhatsApp, a empresa coleta automaticamente dados de uso e de registro, transações, dispositivos e conexões (como "modelo de hardware, dados do sistema operacional, dados sobre o navegador, endereço de IP, dados sobre a rede móvel, incluindo o número do telefone, e identificadores do dispositivo"), dados sobre a localização do dispositivo caso sejam utilizados os recursos de localização, dados de status (quando "visto pela última vez"), lista de contatos. Todas essas informações podem ser coletivamente

Retidos / armazenados em servidores?	sim	sim[25]	não
Podem ser interceptados?	N/A	sim	não

59. Vale ainda destacar que a realização de "interceptações" só é admissível quando a prova não puder ser feita por outros meios disponíveis (art. 2, II, Lei n. 9.296/96). Há inúmeras alternativas a serem exploradas por autoridades policiais no curso de investigações, antes de recorrer a interceptações.

60. Estas alternativas podem ser bastante efetivas. No âmbito e nos limites da legislação em vigor, com autorização particularizada, autoridades podem solicitar a quebra de sigilo de "metadados", e assim descobrir com quem um número suspeito está se comunicando, a que horas e com que frequência, ou mesmo a localização aproximada do dispositivo do qual se está fazendo uso. Estes inúmeros outros rastros sobre por onde passamos e o que fizemos, levam especialistas a dizer que ingressamos na "idade de ouro da vigilância".[26] Hoje o Estado é capaz de obter metadados que simplesmente não estavam à disposição anos atrás.

61. Ainda, com a emergência do que se convencionou chamar de "Internet das Coisas", que é a possibilidade de uma série de objetos domésticos e do mundo profissional serem equipados com sensores e conectados à Internet, muitos outros metadados vão passar a ser gerados, e

chamadas de "metadados", isto é, dados *sobre* dados de comunicações. Disponível em: https://www.whatsapp.com/legal/?l=pt_br#privacy-policy-information-we-collect Acesso em: 15.02.2017.

[25] Na medida em que a WhatsApp Inc. se apoia em metadados para prover seus serviços de publicidade, é de se assumir que eles ficam guardados. Na política de privacidade da empresa, não fica claro *quais* metadados e *por quanto tempo* são retidos. Ver https://www.whatsapp.com/legal/?l=pt_br#privacy-policy-information-we-collect Acesso em: 15.02.2017.

[26] Entrevista com Riana Pfefferkorn em ESPECIAL: O que dizem os especialistas em criptografia sobre o bloqueio do WhatsApp. Disponível: http://www.internetlab.org.br/pt/opiniao/especial-o-que-dizem-especialistas-em-criptografia-sobre-o-bloqueio-do-whatsapp/ Acesso 15.02.2017.

talvez esses registros já serão o suficiente para muitas investigações.[27] Criptografia não implica o fracasso de investigações.

62. Também no âmbito e nos limites da legislação, é possível recorrer a instrumentos clássicos de investigação, como a oitiva de testemunhas, o uso de informantes e a infiltração de agentes. A Polícia Federal, por exemplo, recorreu a um agente infiltrado para obter dados de grupos do Telegram e WhatsApp nos quais se comunicavam suspeitos de planejamento de atos terroristas.[28] Houve outro meio de conseguir as provas.

63. Assim, antes de se "quebrar" a criptografia de dispositivos ou ordenar a alteração do sistema operacional de qualquer sistema, é necessário investigar se as comunicações não podem ser obtidas de formas alternativas, como pela quebra de sigilo de dispositivos celulares ou computadores já apreendidos no curso de investigação ou pela cooperação com provedores de "backups" (no caso do WhatsApp e para portadores de iPhones, a cooperação com a Apple, que guarda o histórico de mensagens no serviço iCloud, por exemplo). Caso celulares de investigados sejam alvos de busca e apreensão, também será possível acessar o histórico de mensagens.

64. Porém, há quem defenda, no debate público atual, a implementação de formas técnicas de franquear a agentes estatais tal possibilidade de "interceptação". Estes defensores falam na necessidade de criação de um *backdoor*, de um acesso privilegiado, de desabilitação da chave de criptografia, ou mesmo de regulamentar o aplicativo. Essas podem ser alternativas catastróficas.

[27] É essa a conclusão do relatório Don't Panic, do Berkman Klein Center da Harvard University, por exemplo. Disponível: https://cyber.harvard.edu/pubrelease/dont-panic/ Acesso 15.02.2017.
[28] "Grupo simpatizante ao terrorismo cogitou usar arma química nos Jogos do Rio", FOLHA DE S. PAULO, 02 de setembro de 2016. Disponível em: <http://www1.folha.uol.com.br/esporte/olimpiada-no-rio/2016/09/1809421-grupo-simpatizante-ao-terrorismo-cogitou-usar-arma-quimica-nos-jogos-do-rio.shtml>. Acesso 15.02.2016.

65. No atual estado da arte da criptografia de ponta-a-ponta, a criação de *backdoor* em um programa de comunicações privadas comprometeria a capacidade do mecanismo de segurança de garantir a confidencialidade das mensagens contra terceiros mal-intencionados. Uma "chave especial" que permitiria acesso de órgãos com competências investigativas a conteúdo de mensagens transmitidas no uso do aplicativo é uma falha desenhada no próprio sistema que será inevitavelmente explorada por terceiros.

66. Deve-se considerar que no atual estado da arte da tecnologia, não é possível integrar em sistemas uma *backdoor* que somente será utilizada por autoridades do Estado legitimamente autorizados por ordens judiciais.[29] Sendo assim, institucionalizar a "quebra" de criptografia de ponta-a-ponta importa comprometer a segurança individual de todos os indivíduos. Isso efetivamente comprometeria toda a segurança do sistema, e assim, a confidencialidade e a privacidade das mensagens contra "ouvintes clandestinos", expondo as pessoas a diversos tipos de riscos.

67. Qualquer determinação judicial que dê ensejo à adoção deste tipo de prática deve ter em conta que pode ser potencialmente lesiva a direito, seja do provedor de aplicações de Internet, que não é impedido explicitamente pela legislação brasileira para oferecer este tipo de serviço, seja dos cidadãos brasileiros que, diferentemente dos cidadãos de outros países, passaria a estar com integridade e segurança de suas comunicações pessoais comprometidas.

III. CONSIDERAÇÕES FINAIS

68. Por fim, valorizando a convocação da referida audiência pública como essencial espaço de debate das questões constitucionais enfrentadas por esta C. Corte, a Associação InternetLab de

[29] Ver ABELSON, H., ANDERSON, R., BELLOVIN, S.M., BENALOH, J., BLAZE, M., DIFFIE, W., GILMORE, J., GREEN, M., LANDAU, S., NEUMANN, P.G. e RIVEST, R.L., 2015, "Keys under doormats: mandating insecurity by requiring government access to all data and communications", *Journal of Cybersecurity*, p.tyv009. Disponível em: https://dspace.mit.edu/handle/1721.1/97690 . Acesso em: 15.02.2017.

Pesquisa em Direito e Tecnologia **requer que a presente contribuição seja juntada aos autos da ADPF 403 e da ADI 5527 para que seja levada em consideração quando de seu julgamento.**

Termos em que
Pede deferimento.

São Paulo, 22 de maio de 2017.

Dennys Antonialli
OAB/SP 290.459
Diretor Presidente do InternetLab

Francisco Brito Cruz
OAB/SP 314.332
Diretor do InternetLab

Jacqueline de Souza Abreu
OAB/SP 356.941
Coordenadora de pesquisa no InternetLab

edifício itália
avenida são luís 50
1º andar conjunto 11b
1046-000 são paulo sp brasil
www.internetlab.org.br