Laboratório de Pesquisa
Direito Privado e Internet - LAPIN

SUPREMO TRIBUNAL FEDERAL

ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL N. 403

AMICUS CURIAE

REQUERENTE:

Instituto Beta para Democracia e Internet-IBIDEM

CONTRIBUIÇÃO ACADÊMICA

Laboratório de Pesquisa Direito Privado e Internet-LAPIN

da Faculdade de Direito da Universidade de Brasília

SUMÁRIO

TESE

O **IBIDEM**, em conjunto com o **LAPIN**, defende na condição de *amicus curiae* a violação do preceito fundamental da liberdade de comunicação e a constitucionalidade do Marco Civil da Internet. Argumenta que (i) a controvérsia envolve casos de equivocada interpretação e aplicação do Marco Civil; (ii) as decisões judiciais tem determinado a suspensão de serviços de comunicação virtual instantânea em inobservância da liberdade de comunicação; (iii) o Marco Civil representa um patamar regulatório democrático voltado à proteção dos dados e da privacidade do internauta, que comporta aplicação em harmonia com o cumprimento de decisões judiciais.

EXCELENTÍSSIMO SENHOR MINISTRO RELATOR DO SUPREMO TRIBUNAL FEDERAL

ADPF 403

O INSTITUTO BETA PARA DEMOCRACIA E INTERNET-IBIDEM, pessoa jurídica de direito privado, associação, sem fins lucrativos, inscrita no CNPJ n. 67.139.485/0001-70, registrada no Ministério do Trabalho sob o n. 24000.000490/92, com sede no SRTVS-Setor de Rádio e Televisão Sul Sul, Quadra 1, Conjunto L, Bloco 1, n. 38, sala 729, CEP 70.340-000, Brasília-DF, com o apoio dos pesquisadores do LABORATÓRIO DE PESQUISA DIREITO PRIVADO E INTERNET DA FACULDADE DE DIREITO DA UNIVERSIDADE DE BRASÍLIA-LAPIN, comparece, respeitosamente, à presença de Vossa Excelência, por meio do advogado subscritor, com fundamento no art. 6.º, §2.º, da Lei n. 9.882/99, e art. 138 do Código de Processo Civil, para requerer a admissão na presente ação direta de inconstitucionalidade na condição de AMICUS CURIAE, pelos fatos e fundamentos a seguir explicitados.

I. PRESSUPOSTOS PARA A ADMISSÃO DOS AMICI CURIAE: A REPRESENTATIVIDADE ADEQUADA E RELEVÂNCIA DA MATÉRIA

1. O INSTITUTO BETA PARA DEMOCRACIA E INTERNET-IBIDEM é uma associação civil sem fins lucrativos[1], que defende os valores democráticos da cibercultura, de maneira que vem atuar perante a jurisdição constitucional com o escopo de contribuir para a formação de um processo decisório plural, dialógico e centrado na proteção dos direitos e garantias fundamentais dos usuários da internet[2].

2. A evidenciar a representatividade adequada, vale ressaltar que o **IBIDEM** é uma entidade regularmente constituída cuja atuação envolve a promoção dos direitos dos usuários da internet[3], a produção de pesquisas e relatórios relacionados à cibercultura, a organização de eventos e manifestações sociais, culturais e políticas voltados a preservar os valores democráticos no ciberespaço[4]. Sua atuação incisiva para resguardar os preceitos da liberdade de expressão, manifestação do pensamento e livre acesso à internet revela a pertinência da intervenção nesta ação direta de inconstitucionalidade.

3. Para o ingresso nesta arguição de descumprimento de preceito fundamental, o **IBIDEM** conta com a contribuição acadêmica e científica dos alunos, professores e pesquisadores do **Laboratório de Pesquisa Direito Privado e Internet da Faculdade de Direito da Universidade de Brasília-LAPIN**, os quais atuaram na organização de

[1] Nos termos do art. 2.º do Estatuto Social, registrado no Cartório do 1.º Ofício de Notas, Registro Civil, Pessoas Jurídicas, Títulos e Documentos (anexo): "O IBIDEM tem como objetivos principais promover a defesa, garantia e promoção de bens e direitos sociais, coletivos e difusos relativos que venham ser afetados em decorrência de livre manifestação do pensamento, da cultura e dos direitos humanos, no ambiente da chamada cultura cibernética –ou cibercultura-, através da internet, perante a sociedade, utilizando-se dos espaços públicos de organização e ação social, comunitária, acadêmica e do Estado, através de seus Poderes Legislativo, Judiciário e Executivo".

[2] Sobre as características da cibercultura, cf. PIERRE LEVY. *Cibercultura*. Trad. Carlos Irineu da Costa. São Paulo: Editora 34, 2010; CASTELLS, Manuel. *The rise of the network society: The information age: Economy, society, and culture.* Londres: John Wiley & Sons, 2011.

[3] http://ibidem.org.br/cpiciber-eff-explica-as-perigosas-propostas-contra-o-cibercrime-no-brasil/

[4] http://ibidem.org.br/protecao-da-dados-pessoais-organizacoes-manifestam-apoio-ao-projeto-de-lei/

debates, coleta de informações e análise de dados como parte das atividades regulares de pesquisa e extensão[5].

4. O LAPIN é um laboratório acadêmico de composição plural (estudantes, pesquisadores e professores) e dentre as suas atividades se insere a pesquisa e a extensão universitária sobre temas relativos à influência da internet no Direito Privado, com destaque para a proteção de dados, a privacidade, a regulação do ciberespaço, as relações contratuais, a responsabilidade civil e os direitos da personalidade.

5. A atuação conjunta do IBIDEM e do LAPIN demonstra a relevância da participação na jurisdição constitucional das entidades da sociedade civil e dos pesquisadores acadêmicos. Por força de tais aspectos, resta evidenciado o interesse, a representatividade adequada, a relevância social da matéria e a pertinência do pedido de admissão do IBIDEM para atuar no processo na condição de *amici curiae.*

6. O Supremo Tribunal Federal tem "entendido que a presença do *amicus curiae* no momento em que se julgará a questão constitucional não só é possível como é desejável"[6], de sorte que este é o propósito da intervenção conjunta do IBIDEM e do LAPIN.

7. Além do pedido de ingresso ter sido realizado em momento oportuno, ou seja, ainda no curso da instrução e antes do julgamento, o art. 138 do Código de Processo Civil e o art. 7.º, §2.º, da Lei 9.868/99 admitem que pessoas naturais ou jurídicas, órgãos ou entidades especializadas sejam admitidos como *amicus curiae*.

8. Não há, portanto, qualquer identidade entre a relevante contribuição ora apresentada pelo IBIDEM, municiado pelo LAPIN, e a decisão do Supremo Tribunal Federal no AgRg/ADI 3.396, Rel. Min. Celso de Mello.

9. A desnecessidade de personificação jurídica e de constituição por determinado lapso temporal constante do art. 138 do novo Código de Processo Civil

[5] A atuação de clínicas e grupos de pesquisa de alunos universitários já foi admitida pelo Supremo Tribunal Federal em relação aos alunos da Núcleo de Prática Jurídica da Fundação Getúlio Vargas-FGV, na ADI 4.815, referente às biografias não autorizadas, e a Clínica de Direitos Fundamentais da UERJ, na ADPF 347, pertinente ao sistema prisional e o Estado de Coisas Inconstitucional.

[6] STF, RE 595.964, Rel. Minª. Cármen Lúcia, DJe 16.02.2011; RE 597.165, Rel. Min. Celso de Mello, DJe 12.04.2011.

justificaria a possibilidade de intervenção como *amicus curiae* também do **LAPIN**, na condição de associação de fato, considerada a contribuição social e científica que poderão dar ao julgamento desta ação.

10. No entanto, em virtude do posicionamento recente do STF proferido no AgRg/ADI 3.396, Rel. Min. Celso de Mello, nesta ocasião somente o **IBIDEM** requer a sua admissão, sem prejuízo do registro de que o Supremo Tribunal Federal deveria reconsiderar a sua posição para assegurar maior representatividade e participação dos *amici curiae* no processo decisório. A construção de uma sociedade aberta dos intérpretes na jurisdição constitucional não pode ser realizada apenas com os atores que o Supremo Tribunal Federal elege[7].

11. No tocante à relevância da matéria e a repercussão social da controvérsia, cumpre destacar que esta ação foi proposta para (i) **impedir a suspensão do aplicativo de mensagens Whatsapp "por qualquer decisão judicial" (fl. 9 da inicial)** e a (ii) **declaração de violação ao preceito fundamental da liberdade de comunicação**, a pretexto de evitar as sanções de suspensão e bloqueio de aplicativos, serviços e sites da internet, impostas em razão do descumprimento de decisões judiciais de fornecimento de dados de usuários suspeitos da prática de crimes.

12. Somente nos últimos dois anos, quatro decisões judiciais suspenderam o acesso de forma geral e irrestrita a um específico aplicativo de comunicação virtual, em prejuízo de milhões de usuários e serviços, por força da suposta recusa no fornecimento de dados[8].

13. A presente ADPF se vale exatamente de um destes casos concretos para justificar o pedido de violação a preceito fundamental, com o escopo de resguardar a

[7] Cf. LEAL, Saul Tourinho. O amigo que a Suprema Corte precisa. *Jota*, 23.06.2016, disponível em: http://jota.uol.com.br/o-amigo-que-suprema-corte-precisa.

[8] Cf. Justiça determina o bloqueio do aplicativo whatsapp, disponível em http://www.tjsp.jus.br/Institucional/CanaisComunicacao/Noticias/Noticia.aspx?Id=29056; Facebook Executive arrested in Brazil, disponível em: http://www.wsj.com/articles/facebook-executive-arrested-in-brazil-1456851506; WhatsApp: Justiça do RJ manda bloquear aplicativo em todo o Brasil, disponível em: http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-deve-ser-bloqueado-decide-justica-do-rio.html

liberdade de comunicação e a simultânea proteção dos dados e da privacidade dos usuários da internet[9].

14. Ao contrário do que se identifica na Ação Direta de Inconstitucionalidade 5527, Rel.ª Min.ª Rosa Weber, ajuizada pelo Partido da República, esta ADPF não se volta contra o Marco Civil da Internet propriamente dito, mas sim contra as interpretações equivocadas manifestadas em recentes decisões judiciais[10] que resultaram em suspensões irrestritas, indiscriminadas e desproporcionais.

15. O Supremo Tribunal Federal tem conferido ao *amicus curiae* um papel crucial no âmbito da jurisdição constitucional ao assegurar-lhe o direito de realizar sustentações orais, além da faculdade de propor ao relator a requisição de informações, designação de peritos e convocação de audiências públicas[11].

16. As incompreensões em torno das particularidades do regime jurídico de proteção de dados e da privacidade no ciberespaço demandam uma ampla participação dos pesquisadores, desenvolvedores, usuários, agentes estatais, associações civis e grupos de pesquisa como o IBIDEM e o LAPIN para que a controvérsia seja resolvida em patamares democráticos, técnicos e inclusivos. Por estas razões, requer-se que o IBIDEM seja admitido na condição de *amicus curiae*.

II. PRELIMINARMENTE

17. Embora a presente ADPF tenha natureza incidental, ou seja, tenha sido proposta em razão de controvérsia judicial acerca da suspensão dos serviços de aplicativo de mensagens pelo Juízo da Comarca de Lagarto e por outras decisões semelhantes, subsiste íntegro o objeto da presente ação uma vez que outras decisões lhe sucederam, como a proveniente do Juízo da 2.ª Vara Criminal da Comarca de Duque de Caxias-RJ.

---

[9] Observatório do Marco Civil da Internet. Histórico, disponível em: http://www.omci.org.br/historico-do-marco-civil/timeline/

[10] As decisões foram, invariavelmente, reformadas em nível recursal ou cassadas pela impetração de habeas corpus e mandado de segurança. Cf. http://www.jusbrasil.com.br/diarios/documentos/170898170/andamento-do-processo-n-20150001001592-4-do-dia-03-03-2015-do-djpi ; http://s.conjur.com.br/dl/liminar-whatsapp-tj-pi.pdf

[11] STF, ADPF 187/DF, Rel. Min. Celso de Mello, DJe 15.6.2011

18. A recente decisão proferida pelo Juízo da 2.ª Vara Criminal da Comarca de Duque de Caxias-RJ demonstra a inocorrência da perda do objeto desta ADPF e a reiteração da violação a um preceito fundamental.

19. Ademais, a propositura de uma ação direta de inconstitucionalidade contra o Marco Civil ou de uma ação declaratória de constitucionalidade que lhe dê suporte não evitará que novas decisões, fundadas em outros preceitos normativos sejam proferidas, como se demonstrará adiante. A via recursal tampouco tem sido hábil a impedir novas decisões judiciais de suspensão geral, irrestrita e indeterminada dos serviços de mensagens em todo o território brasileiro, o que demonstra a presença do requisito da subsidiariedade desta arguição de descumprimento de preceito fundamental.

20. O pedido formulado na ADPF não se reveste, portanto, de natureza genérica e futura; apenas compreende um espectro de reiteradas e múltiplas decisões de mesmo conteúdo que têm sido proferidas por juízes de todo o país.

III. O Regime Jurídico da Proteção de Dados e da Privacidade no Marco Civil da Internet

21. O projeto do Marco Civil da Internet no Brasil foi concebido pela Secretaria de Assuntos Legislativos do Ministério da Justiça em parceria com a Escola de Direito FGV Direito Rio com o objetivo de tornar-se um projeto colaborativo[12]. Para tanto, os debates foram realizados em plataformas digitais, as quais possibilitariam que diversos agentes sociais contribuíssem com sugestões, comentários e críticas[13].

22. Os textos apresentados para debate foram organizados em tópicos, proporcionando que as intervenções contribuíssem para a redação dos dispositivos legais correspondentes aos problemas propostos. A primeira fase dos debates resultou em mais de 800 contribuições, reunidas em um relatório disponibilizado no sítio eletrônico do Ministério da Justiça:

[12] http://direitorio.fgv.br/marco-civil-da-internet-evento-de-abertura-291009

[13] http://pensando.mj.gov.br/marcocivil/

> O primeiro eixo da discussão busca identificar direitos individuais e coletivos relacionados ao uso da internet atualmente não previstos de forma explícita no ordenamento jurídico nacional. Embora passíveis de proteção, por derivarem de princípios constitucionais, a ausência de previsão legal específica para sua proteção acaba por prejudicar sua tutela e exercício. Também busca adaptar os direitos fundamentais existentes a um contexto de comunicação eletrônica.[14]

23. Posteriormente, a partir das sugestões foi elaborada a primeira versão do Anteprojeto do Marco Civil, o qual foi submetido a consulta pública. Encerrada a fase de coleta de sugestões, o Poder Executivo enviou o anteprojeto de lei ao Congresso Nacional e os debates com a sociedade civil continuaram por meio do site e-Democracia até a aprovação em ambas as Casas Legislativas[15]. No início do mês de maio de 2016, após nova consulta pública, o Marco Civil foi objeto de regulamentação pelo Decreto 8.771/2016[16].

24. Este percurso democrático de elaboração do Marco Civil revela a importância da análise histórica de seu conteúdo, pois permite compreender as motivações subjacentes aos artigos 10, 11 e 12, objeto de interpretações equivocadas nas recentes decisões de suspensão e bloqueio. É imperativo, então, que também se analisem os debates realizados sobre a proteção dos dados e sobre a privacidade, dispostos no eixo 1 do debate, isto é, os "Direitos individuais e coletivos".

25. Da análise das contribuições, resta evidente a existência de grande preocupação com a proteção da privacidade e do anonimato na internet, assim como com sua compatibilização em relação aos demais direitos fundamentais[17]. Destaca-se, aqui, o debate acerca da real necessidade de armazenamento de logs, a modalidade de armazenamento permitida, o tempo de guarda e a atuação estatal na gestão, tratamento e proteção dos dados etc.

---

[14] Direitos Individuais e Coletivos (Eixo 1)". 2009. Disponível em: http://culturadigital.br/marcocivil/category/consulta/1-direitos-individuais-e-coletivos-eixo-1/ Acesso em: 21 jun. 16.

[15] http://edemocracia.camara.gov.br/web/marco-civil-da-internet/andamento-do-projeto#.V3E6ZbgrJPY

[16] http://www.justica.gov.br/noticias/marco-civil-da-internet-e-protecao-de-dados-pessoais-vao-a-debate-publico

[17] MURRAY, Andrew. *Information technology law: the law and society*. London: Oxford University Press, 2013.

26. Nesse contexto, a liberdade e o anonimato na internet receberam defesas efusivas por supostamente constituírem as principais garantias a serem resguardadas, o que significa que não se deveria permitir a autenticação obrigatória ou a associação entre os IPs e os usuários[18]. A tecnologia existente seria relativamente adequada para a identificação dos usuários responsáveis pela prática de crimes virtuais, sem que para tanto fossem armazenados ou utilizados logs de conexão por parte dos provedores.

27. Em outra medida, sustentou-se que o registro das informações deveria ser algo voluntário, não devendo constituir uma obrigação de armazenamento por parte dos provedores. As contribuições ainda indicaram que o armazenamento deveria ser temporalmente limitado e aos indivíduos deveriam ser assegurados recursos que lhes permitissem controlar as informações armazenadas nos logs (*accountability*)[19].

28. No que tange à responsabilidade pelo armazenamento dos dados, foi sugerida a obrigatoriedade de guarda dos registros pelos provedores de conexão e a faculdade dos provedores de conteúdo de fazê-lo. Por outro lado, tanto os provedores de conteúdo quanto os provedores de conexão deveriam obrigatoriamente armazenar os logs, entretanto bastava que estes logs guardassem a data de utilização e a origem do IP[20].

29. Muitas das contribuições, entretanto, demonstravam receio de que o sistema criado pelo poder público para o armazenamento de logs fosse potencialmente perigoso, facilitando a utilização indevida dos dados pessoais para o cometimento de crimes. Assim, em defesa da privacidade, o Estado deveria limitar sua atividade regulatória ao armazenamento de cadastros e não interferir nos logs de acesso, visto que o sigilo das comunicações de dados já era objeto de outras normas.

---

[18] O STJ tem entendido que a simples identificação de usuário pelo IP do computador por meio do qual foi praticado crime não afronta o sigilo constitucional de dados (STJ, AgRg na CR 5.694/EX, Rel. Min. Felix Fischer, Corte Especial, DJe 02.05.2013). No entanto, a medida tem sido severamente criticada porquanto a simples identificação do IP de um dispositivo não é capaz de comprovar, per se, a autoria de um crime, na medida em que um computador pode ser utilizado por vários indivíduos ou ter acesso remoto.

[19] A autonomia dos usuários tem sido objeto de estudos sob a perspectiva da *accountability* dos algoritmos. Cf. PASQUALE, Frank. *The black box society: The secret algorithms that control money and information*. New Haven: Harvard University Press, 2015.

[20] LEONARDI, Marcel. Responsabilidade civil dos provedores de serviços de internet. São Paulo: Juarez de Oliveira, 2005.

30. A partir da análise do relatório de contribuições para o Marco Civil, percebe-se a nítida preocupação com as garantias de autodeterminação informativa e de segurança das informações armazenadas, com frequentes questionamentos no sentido de que a guarda e o registro dos logs deveriam desestimulados para evitar abusos de vigilância em massa por parte dos agentes estatais[21].

31. De fato, o processo de debate e construção do projeto do Marco Civil, assim como sua aprovação e regulamentação, expressaram a necessidade de que a privacidade e os dados dos usuários fossem adequadamente protegidos. Isto significa que a atuação do Estado deveria ser pautada pela atuação mínima e a defesa dos valores democráticos[22].

32. O contexto anteriormente explicitado permite reconstruir a teleologia da norma de maneira a evidenciar que os artigos 10, 11, 12 se inserem na seção de proteção dos direitos do usuário da internet, intitulada "Da proteção aos registros, dados pessoais e comunicações privadas".

33. Ademais, as sanções previstas no art. 12[23], que remetem à inobservância de condutas descritas nos arts. 10 e 11, somente devem ser aplicadas como forma de punição da empresa que não promove o adequado gerenciamento, tratamento e

---

[21] A vigilância em massa e a proteção da privacidade é um dos principais temas de estudo de BAUMAN, Zygmunt. *Vigilancia líquida*. Rio de Janeiro Zahar, 2014; KERR, Orin S. Problem of Perspective in Internet Law, *The Georgetown Law Journal*, v. 91, p. 357, 2002; SCHWARTZ, Paul M.; SOLOVE, Daniel J. Pii problem: Privacy and a new concept of personally identifiable information, *The NYU Law Review*, v. 86, p. 1814, 2011; SCHWARTZ, Paul M. Privacy and democracy in cyberspace. *Vanderbilt Law Review*, v. 52, p. 1607, 1999.

[22] FARRANHA, Ana Claudia. Estado, sociedade e interações digitais: expectativas democráticas. *RP3-Revista de Pesquisa em Políticas Públicas*, n. 2, 2014.

[23] 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 de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

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.

manipulação dos dados do usuário. A incompreensão e má-aplicação do regime jurídico de proteção dos dados pessoais e da privacidade na internet, constante da Seção II "Da proteção aos registros, dados pessoais e comunicações privadas", não deve servir como fundamento enviesado para se declarar a inconstitucionalidade de um preceito normativo destinado a resguardar direitos, tal como requerido na ADI 5527.

34. Ainda que se cogite terem as decisões judiciais se fundado na expressão "*deverão ser obrigatoriamente respeitados a legislação brasileira"* para impor a sanção de suspensão e bloqueio de sites/aplicativos", presente no *caput* do art. 11 do Marco Civil da Internet, o argumento não merece prosperar.

35. E por uma razão simples: se alguma empresa realizar a "operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet" em desconformidade com a legislação brasileira, somente a ela devem ser impostas de forma gradativa, específica, individualizada e proporcional as sanções do art. 12 do Marco Civil.

36. A inversão de valores imprimida por decisões judiciais casuísticas, as quais impõem sanções do Marco Civil de forma descontextualizada, pode servir de parâmetro para uma ação de descumprimento de preceito fundamental incidental (incidental ou direta), mas não para a declaração de inconstitucionalidade em desfavor do patamar mínimo de salvaguarda do internauta.

IV. AS DECISÕES JUDICIAIS ANTES DO MARCO CIVIL DA INTERNET E O PRINCÍPIO DA PROPORCIONALIDADE E AS

37. Além da compreensão do processo dialógico de elaboração do Marco Civil e dos direitos do internauta, cumpre seja analisada a dimensão dos efeitos danosos das decisões judiciais que têm ensejado o bloqueio de sites e aplicativos no Brasil, em violação ao preceito fundamental da liberdade de comunicação.

38. Antes da entrada em vigor do Marco Civil, duas decisões judiciais haviam suspendido de forma irrestrita em todo o território brasileiro o funcionamento de dois sites: o *Youtube*, em janeiro de 2007, em decorrência do processo movido pela atriz

Daniella Cicarelli[24], e o *Facebook*, em agosto de 2012, em virtude da ação ajuizada por Dalmo Deusdedit Meneses[25].

39. Em ambos os casos, a suspensão dos serviços decorreu da negativa de cumprimento de ordens judiciais de retirada de conteúdo por parte das empresas. No entanto, o fundamento de cada uma delas foi distinto: no primeiro caso se utilizou o art. 461, §1º, do CPC/1973[26] (atual art. 536, §1º do NCPC) para realizar a suspensão; no segundo, a fundamentação da decisão envolveu o art. 57-I da Lei das Eleições (Lei n. 9.504/97)[27].

40. Sob outra perspectiva, após a entrada do Marco Civil, quatro decisões determinaram a suspensão do aplicativo de comunicação instantânea *Whatsapp*: a primeira foi determinada pela Central de Inquérito da Comarca de Teresina-PI, no processo 0013872-87.2014.8.18.0140[28]; a segunda, proferida pelo juízo da 1ª Vara Criminal de São Bernardo do Campo-SP, no procedimento de Interceptação Telefônica 0017520-08.2015.8.26.0564[29]; a terceira, no processo de nº 201555000783, proveio do juízo da Vara Criminal da Comarca de Lagarto-SE[30], e a mais recente, a decisão da 2.º Vara Criminal da Comarca de Duque de Caxias-RJ[31].

---

[24] TJSP, Agravo de Instrumento n. 0113488-16.2012.8.26.0000, Rel. Des. Enio Zuliani, https://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=6258764&cdForo=0&vlCaptcha=pwvazhttps://esaj.tjsp.jus.br/cjsg/getArquivo.do?cdAcordao=6258764&cdForo=0&vlCaptcha=pwvaz

[25] TRE-SC, Ação Cautelar n. 86-37.2012.6.24.0013, http://www.tre-sc.jus.br/site/fileadmin/arquivos/noticias/2012/08/decisao_26_de_julho.pdf

[26] CPC/1973, Art. 461. Na ação que tenha por objeto o cumprimento de obrigação de fazer ou não fazer, o juiz concederá a tutela específica da obrigação ou, se procedente o pedido, determinará providências que assegurem o resultado prático equivalente ao do adimplemento.

§ 1º A obrigação somente se converterá em perdas e danos se o autor o requerer ou se impossível a tutela específica ou a obtenção do resultado prático correspondente.

[27] Lei 9.504/97, Art. 57-I. A requerimento de candidato, partido ou coligação, observado o rito previsto no art. 96, a Justiça Eleitoral poderá determinar a suspensão, por vinte e quatro horas, do acesso a todo conteúdo informativo dos sítios da internet que deixarem de cumprir as disposições desta Lei.

[28] http://s.conjur.com.br/dl/liminar-whatsapp-tj-pi.pdf

[29] http://s.conjur.com.br/dl/tj-sp-suspende-bloqueio-whatsapp.pdf

[30] http://www.omci.org.br/m/jurisprudencias/arquivos/2016/tjse_201600110899_03052016.pdf

[31] http://omci.org.br/m/jurisprudencias/arquivos/2016/rj_062001642016_19072016.jpg

41. Dos quatro processos mencionados, apenas o terceiro fez referência ao Marco Civil da Internet para justificar o bloqueio geral e irrestrito do aplicativo em todo o país (arts. 10, 11, 13 e 15), e, por conseguinte, impor a sanção dos incisos II e III do art. 12.

42. Tal aspecto demonstra que, no universo de casos em que houve a determinação de bloqueio ou suspensão de algum site/aplicativo, apenas em uma oportunidade se recorreu ao inciso III do art. 12 do Marco Civil como fundamento para a imposição da medida. Nos demais processos, o principal fundamento utilizado para o bloqueio foi o antigo art. 461, §1.º, do CPC/73, conforme tabela a seguir:

Origem	Fundamento	Motivação da Reforma ou Cassação
Central de Inquérito da Comarca de Teresina-PI	Art. 461, §1º do CPC/73	Princípio da proporcionalidade
Vara Criminal de São Bernardo do Campo-SP		Princípio da proporcionalidade
Vara Criminal de Lagarto-SE	Art. 10, 11, 13 e 15 e 12, III, do Marco Civil	Princípio da proporcionalidade e Marco Civil
Vara Criminal de Duque de Caxias	Não explicitado	Liberdade de comunicação

43. E este é certamente o ponto central em torno do cabimento desta ADPF e da desnecessidade e impropriedade da declaração de inconstitucionalidade dos dispositivos impugnados na ADI 5527. Ainda que o §2.º do art. 10 e os incisos III e IV do art. 12 do Marco Civil sejam eventualmente declarados inconstitucionais, sem redução de texto, ou submetidos a interpretação conforme, isto não impedirá que decisões judiciais de bloqueio/suspensão sejam novamente proferidas com base em outros preceitos normativos, como também o foram antes e depois do Marco Civil da Internet.

44. Reitere-se, portanto, que este aspecto evidencia a presença do requisito da subsidiariedade desta ADPF, na medida em que nem uma ação direta de inconstitucionalidade nem uma ação declaratória de constitucionalidade do Marco Civil da Internet, ou ainda a via recursal, tem se demonstrado instrumentos aptos a fazer cessar com eficácia *erga omnes* e efeito vinculante a lesividade ao preceito fundamental da liberdade de comunicação provocada por reiteradas decisões judiciais de bloqueio e suspensão.

45. O emprego de outros fundamentos, pautados em atos normativos como o art. 536, §1º, do CPC/2015[32] (antigo art. 461, §1.º, do CPC/1973), o art. 139, IV do CPC/2015[33], ou o poder geral de cautela, continuarão a assegurar a possibilidade de imposição de medidas desta natureza, o que comprova não ser o Marco Civil da Internet o cerne do problema.

46. Assim, somente um julgamento amplo, sob o ditame da violação do preceito fundamental da liberdade de comunicação (art. 5.º, IX, da CF), preservada a integridade do Marco Civil da Internet, poderá evitar a reprodução de decisões judiciais de suspensão/bloqueio fundadas em outros preceitos normativos infraconstitucionais.

47. Basta observar que até os acórdãos dos Tribunais que reformaram ou cassaram as decisões de bloqueio/suspensão não utilizaram o Marco Civil da Internet como extrato normativo, mas exclusivamente o princípio da proporcionalidade, dada a desnecessidade, inadequação e violação à proporcionalidade em sentido estrito.

V. O Direito à Proteção de Dados Pessoais e à Privacidade na Internet no Direito Comparado

48. Para ingressar no cerne do debate em torno da proteção de dados pessoais e da privacidade na internet, um dos possíveis caminhos envolve a análise dos contornos jurisprudenciais e políticos da criptografia e do anonimato na década de 90 nos Estados Unidos, conhecida como *crypto wars*[34]. Afinal, a criptografia e o anonimato, enquanto mecanismos de expressão da liberdade de comunicação, pensamento e manifestação, estão

[32] CPC, Art. 536. No cumprimento de sentença que reconheça a exigibilidade de obrigação de fazer ou de não fazer, o juiz poderá, de ofício ou a requerimento, para a efetivação da tutela específica ou a obtenção de tutela pelo resultado prático equivalente, determinar as medidas necessárias à satisfação do exequente.

§ 1º Para atender ao disposto no caput, o juiz poderá determinar, entre outras medidas, a imposição de multa, a busca e apreensão, a remoção de pessoas e coisas, o desfazimento de obras e o impedimento de atividade nociva, podendo, caso necessário, requisitar o auxílio de força policial.

[33] Art. 139. O juiz dirigirá o processo conforme as disposições deste Código, incumbindo-lhe:

IV - determinar todas as medidas indutivas, coercitivas, mandamentais ou sub-rogatórias necessárias para assegurar o cumprimento de ordem judicial, inclusive nas ações que tenham por objeto prestação pecuniária;

[34] The Crypto Wars: Governments Working to Undermine Encryption, https://www.eff.org/document/crypto-wars-governments-working-undermine-encryption

no epicentro do problema acerca do descumprimento de decisões judiciais de bloqueio/suspensão[35].

49. Até meados de 1993, a criptografia era feita por meio de hardware. Como a internet ainda não havia se popularizado, a técnica era usada pelo governo em redes privadas. O padrão criptográfico mais utilizado era o *Data Encryption Standard* (DES), desenvolvido pela IBM[36], e posteriormente sucedido pelo Clipper[37].

50. Neste período, o Departamento de Estado dos EUA classificava a criptografia como munição militar e regulava sua exportação[38]. O governo americano exigia a obtenção de licenças de exportação para softwares de cifragem que estivessem ao alcance estrangeiros. As agências governamentais emitiam licenças de exportação de forma discricionária, sem prazos ou critérios pré-determinados[39].

51. Este procedimento subsistiu até o julgamento pela Suprema Corte americana do *leading case Bernstein v. United States Department of State*[40]. Durante seu doutorado em matemática pela Universidade de Berkeley, Daniel Bernstein desenvolveu um algoritmo criptográfico denominado *Snuffle*.

52. Submetido à classificação da criptografia como munição militar, Bernstein foi impedido de publicar seu código criptográfico em periódicos acadêmicos na internet sem antes se registrar como exportador de armas. Por esta razão, o matemático decidiu processar o governo americano sob o argumento de que, ao restringir o acesso às ferramentas que asseguravam maior proteção à privacidade, como a criptografia, os agentes estatais teriam violado o direito à ampla comunicação dos cidadãos:

---

[35] Revised U.S. Encryption Export Control Regulations, https://epic.org/crypto/export_controls/regs_1_00.html

[36] MENEZES, A. J.; VAN OORSCHOT, Paul C.; VANSTONE, Scott A. *Handbook of Applied Cryptography*. Boca Raton: CRC, 1996.

[37] PGP. An Introduction to Cryptography. jul. 2005. Disponível em: http://www.csc.gatech.edu/~copeland/6612/pgp/Intro%20To%20Cryptography.pdf. Acesso em: 21/6/16.

[38] International Traffic in Arms Regulations (ITAR), 22 C.F.R. §§ 120-30 (1994).

[39] ROSS, Patrick Ian. Bernstein v. United States Department of State. *Berkeley Technology Law Journal,* 13.1, Annual Review of Law and Technology, 1998, p. 405.

[40] https://www.eff.org/cases/bernstein-v-us-dept-justice

> Without cryptography, what people send via computers is the electronic equivalent of a postcard, open to view by many people while the message is in transit. With cryptography, people can put both messages and money into electronic 'envelopes,' secure in the knowledge that what they send is not accessible to anyone except the intended recipient.
> Continued development of cryptography promises to make it possible for the worldwide computer Internet to offer private, secure and protected communication among billions of people worldwide.[41]

53. O governo americano, por sua vez, sustentava que o Ato de Controle da Exportação de Armas (*Arms Export Control Act*) expressamente vedava o controle judicial do que era incluído no rol de munições. Na ocasião, o Tribunal do Distrito do Norte da Califórnia entendeu que a classificação da criptografia como munição era inconstitucional por violação à Primeira Emenda da Constituição americana, uma vez que o código criptográfico constituía uma manifestação do direito de liberdade de expressão:

> Even object code, which directly instructs the computer, operates as a "language." When the source code is converted into the object code "language," the object program still contains the text of the source program. The expression of ideas, commands, objectives and other contents are merely translated into machine-readable code.[42]

54. A decisão foi amplamente fundamentada em analogias com partituras musicais e direitos autorais. A Suprema Corte objetivou demonstrar que o caráter funcional do código fonte não o tornaria menos protegido que a partitura da música tocada por um piano automático.

55. A partir do precedente *Bernstein v. United States Department of State*, a criptografia foi reconhecida como uma manifestação da liberdade de expressão e a sua regulamentação por órgãos estatais foi considerada inconstitucional.

56. Superou-se, assim, a compreensão belicista da criptografia, substituída por uma posição mais próxima da sociedade civil. Era o primeiro passo para que o código pudesse ser utilizado como instrumento voltado à efetiva proteção de dados pessoais e da

[41] ROSS, Patrick Ian. Bernstein v. United States Department of State. *Berkeley Technology Law Journal,* 13.1, Annual Review of Law and Technology, 1998, p. 405.

[42] ROSS, Patrick Ian. Bernstein v. United States Department of State. *Berkeley Technology Law Journal,* 13.1, Annual Review of Law and Technology, 1998, p. 405.

privacidade dos usuários da rede. Entretanto, a criptografia representa apenas uma das vias de expressão dos mecanismos de proteção de dados e da privacidade na internet.

57. No âmbito da União Europeia, não apenas a criptografia tem suscitado expressivos embates, como também o anonimato, sobretudo após o episódio que envolveu Edward Snowden, a *National Security Agency* (NSA), alguns Primeiros Ministros de países europeus e a Presidente do Brasil. O fluxo transnacional de dados, que recentemente ensejou a celebração de um novo acordo entre União Europeia e Estados Unidos (*Privacy Shield*)[43], em função da declaração de nulidade do anterior (*Safe Harbor*) pela Corte Europeia de Justiça no caso *Max Schrems v. Data Protection Commissioner*[44], tem evidenciado a importância dos marcos regulatórios voltados à proteção dos dados pessoais[45].

58. O marco regulatório da proteção de dados e privacidade na União Europeia ocorreu com a entrada em vigor da Diretiva 46/95, conhecida como o Regulamento Geral sobre a Proteção de Dados, no qual foram definidos padrões mínimos de proteção, o que facilitaria a identificação de outros países que oferecessem níveis de proteção equivalentes aos europeus.

59. Transcorridos vinte anos desde a primeira diretiva e com o vertiginoso avanço tecnológico, a União Europeia se viu diante da necessidade de elaborar uma nova regulamentação da privacidade e proteção de dados pessoais. No final do mês de abril deste ano, o Parlamento Europeu promulgou o Regulamento 679/2016, que disciplina a proteção e a livre circulação de dados pessoais, bem como a Diretiva 680/2016, que dispõe sobre as autoridades competentes para promover a prevenção de infrações e imposição de sanções[46].

60. Com o objetivo de proteger a privacidade dos indivíduos, o art. 5º (1) (f) do Regulamento 679/2016 destaca a confidencialidade e a integridade como dois princípios essenciais para o tratamento de dados pessoais. A preocupação com este aspecto é tamanha

[43] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf

[44] http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[45] No Brasil, além do Marco Civil e o decreto que o regulamentou, acaba de ser enviado ao Congresso Nacional o Anteprojeto de Proteção de Dados Pessoais (PL 5.276/2016).

[46] Regulamento (UE) 679/2016, art. 4º (2) e Diretiva (EU) 680/2016, art. 3º (2).

que, no art. 25 (1), o Regulamento prevê que os dados devem ser protegidos desde sua concepção, ou seja, desde a definição dos meios de tratamento o responsável deverá prever formas adequadas de garantir a confidencialidade e integridade.

61. Ao contextualizar a proteção de dados pessoais realizada na União Europeia com as decisões judiciais proferidas no Brasil e citadas na presente ação, observa-se que os serviços de comunicação instantânea como o *WhatsApp*, ao adotarem a criptografia de ponta-a-ponta (*end-to-end)*, estão na verdade imprimindo um padrão de proteção elevado ao internauta. E um claro indicativo disso pode ser percebido pela previsão na nova Diretiva Europeia de que os dispositivos, serviços e plataformas na internet deverão garantir a proteção de dados e a privacidade por configuração e padrão de fabricação (*privacy by design* e *privacy by default*)[47].

62. A regulação do ciberespaço e as particularidades desta arena pública de interação social parecem ser algo de difícil compreensão para algumas autoridades estatais[48], as quais enxergam a arquitetura da rede apenas como um meio de obstaculizar investigações criminais e decisões judicias[49], ao invés de constituir um sistema de proteção do sigilo de comunicação e dos dados da grande maioria dos usuários[50].

---

[47] WILLIS, Lauren E. Why Not Privacy by Default. *Berkeley Technology Law Journal*, v. 29, p. 61, 2014; RUBINSTEIN, Ira S. Regulating privacy by design. *Berkeley Technology Law Journal*, v. 26, n. 3, p. 1409-1456, 2011; SCHAAR, Peter. Privacy by design. *Identity in the Information Society*, v. 3, n. 2, p. 267-274, 2010.

[48] A compreensão da regulação do ciberespaço perpassa pelo trabalho desenvolvido inicialmente pelos ciberlibertários John Perry Barlow, David Post e David Johnson, seguido dos ciberpaternalistas Joel Reidenberg, Lawrence Lessig e Yochai Blenkler, até se chegar aos network comunitaristas Andrew Murray, Colin Scott, Paul Bernal.

[49] Cf. http://jota.uol.com.br/os-rumos-da-agenda-de-protecao-de-dados-e-da-privacidade-na-internet. Neste artigo foram apontados os principais contornos da proteção de dados na atualidade, com destaque para uma decisão de um magistrado do Paraná, o qual determinou que um site hospedado na Austrália fosse submetido às sanções do Marco Civil da Internet por explorar os serviços de consulta de dados de sócios de empresas brasileiras cf. http://www.omci.org.br/jurisprudencia/111/domain-privacy-e-bloqueio-no-backbone/. O fato se repete a cada dia e os mecanismos convencionais como as cartas rogatórias e o Mutual Legal Assistance Treaty (MLAT) se revelam incapazes de tornar exequíveis decisões judiciais e leis quando diante do fluxo transnacional de dados.

[50] Diante da ocasional inadequação da lei para regular o ciberespaço, Reino Unido, Canadá, Austrália e França passaram a atuar na arquitetura da rede mediante ferramentas de bloqueio, filtragem e suspensão de acesso como o *Cleanfeed* e agências governamentais como a *HADOPI*. Medidas semelhantes têm encontrado resistência nos Estados Unidos em virtude Primeira Emenda, como se observa no julgamento do caso *Reno v. American Civil Liberties Union* (521 US 844, 1997).

63. Por sinal, o Supremo Tribunal Federal, em mais de uma ocasião, se manifestou no sentido de que a proteção constitucional do sigilo de comunicações de dados não se confundia com a proteção aos dados em si. Entretanto, o posicionamento da Corte, fruto de acórdão da lavra do eminente Ministro Sepúlveda Pertence, não mais reflete a realidade da evolução tecnológica e a relevância da proteção de dados pessoais no ciberespaço. Ainda assim, o precedente contém questões pertinentes para o cerne desta ação direta de inconstitucionalidade:

> Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que **a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a consequente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental.** 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. **Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial". 4. A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador**. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270).[51]

64. Por outro lado, vale observar que o Superior Tribunal de Justiça apreciou tema semelhante por ocasião da impetração de *habeas corpus* em favor do banqueiro Daniel Dantas, decorrente de busca e apreensão que resultou na coleta de dados de um *Hard Drive* (HD) do Banco Opportunity, nas Operações Satiagraha e Chacal. Na ocasião, o STJ analisou especificamente a proteção da garantia constitucional de inviolabilidade do sigilo dos dados em si considerados, com as possíveis consequências ao direito à privacidade de terceiros, correntistas do Banco Opportunity:

[51] STF, RE 418.416, Rel. Min. Sepúlveda Pertence, Tribunal Pleno, DJ 19.12.2006. Em precedentes mais antigos, o STJ também se limitava a proteger o sigilo do "fluxo de comunicações em sistema de informática e telemática" (STJ, HC 15.026/SC, Rel. Min. Vicente Leal, Sexta Turma, DJ 24.09.02; REsp 625.214/SP, Rel. Min. Hamilton Carvalhido, Sexta Turma, DJ 29.06.2007).

> Com o auxílio das atuais ferramentas de informática, é possível fazer a separação dos dados de um HD, evitando-se a eventual quebra do sigilo de dados acobertados pela garantia constitucional. O acesso a dados sigilosos de terceiros goza de proteção constitucional, não havendo ilegalidade na medida que autoriza o acesso aos dados pertinentes ao crime em apuração, desde que sejam utilizados instrumentos de informática específicos para a correta busca e separação somente dos dados pertinentes ao caso[52].

65. Curioso notar como na referida decisão o Superior Tribunal de Justiça demonstrou um profundo cuidado com o sigilo, a privacidade e a proteção de dados de terceiros não sujeitos à investigação criminal, enquanto que nas recentes decisões judiciais de suspensão dos serviços de comunicação instantânea sequer se atentou para esta possibilidade (grupos de mensagens compartilhadas, fotografias armazenadas em *cloud computing* etc.).

66. Em acórdão recente, o Superior Tribunal de Justiça teve a oportunidade de confirmar seu entendimento anterior em torno da proteção e inviolabilidade do sigilo dos dados em si, e não apenas da comunicação de dados. Ao analisar a ilicitude da prova decorrente da apreensão de um telefone celular, cujo acesso aos dados e às mensagens instantâneas ocorreu sem prévia autorização judicial, a Corte novamente afirmou serem também os dados sujeitos à proteção constitucional:

> Atualmente, o celular deixou de ser apenas um instrumento de conversação pela voz à longa distância, permitindo, diante do avanço tecnológico, o acesso de múltiplas funções, incluindo, no caso, a verificação da correspondência eletrônica, de mensagens e de outros aplicativos que possibilitam a comunicação por meio de troca de dados de forma similar à telefonia convencional. Deste modo, **ilícita é tanto a devassa de dados, como das conversas de whatsapp obtidos de celular apreendido, porquanto realizada sem ordem judicial.** Ante o exposto, voto por dar provimento ao recurso ordinário em habeas corpus, para declarar a nulidade das provas obtidas no celular do paciente sem autorização judicial, cujo produto deve ser desentranhado dos autos.[53]

67. O precedente reúne elementos muito semelhantes ao recente julgamento do caso *Microsoft Corporation v. United States,* pelo Tribunal de Apelação do 2.º

[52] STJ, HC 124.253/SP, Rel. Min. Arnaldo Esteves Lima, Quinta Turma, DJe 05.04.2010.

[53] STJ, RHC 51.531/RO, Rel. Min. Nefi Cordeiro, Sexta Turma, DJe 09.05.2016.

Circuito[54], e do caso *Riley v. California*, no qual a Suprema Corte dos Estados Unidos reconheceu a necessidade de prévia autorização judicial para o acesso aos dados armazenados em aparelho celular. A opinião da Corte foi pronunciada pelo *Chief Justice John Roberts,* que elucidou a necessidade de se separar o acesso físico a um celular do acesso ao conteúdo digital nele armazenado:

> Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon--say, to determine whether there is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.
>
> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life". The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.[55]

68. É certo que a garantia de inviolabilidade do sigilo de dados não é absoluta e a Constituição Federal veda o anonimato, todavia as decisões judiciais de intercepção para fins de investigação criminal devem ser proferidas em harmonia com a proteção dos direitos dos demais usuários, de modo a que não sejam prejudicados[56]. Quando veda o anonimato, a Constituição Federal o faz em associação à liberdade de manifestação do

[54] No dia 14 de julho de 2016, o Tribunal de Apelação do 2.º Distrito dos Estados Unidos julgou um recurso em favor da Microsoft para impedir que a empresa fosse obrigada a fornecer dados e emails de um traficante de drogas, os quais estavam guardados em uma nuvem hospedada em Dublin, na Irlanda. Cf. http://www.ca2.uscourts.gov/decisions/isysquery/3c2ad8d1-b716-49bc-b593-c62ea0d05922/9/doc/14-2985_complete_opn.pdf#xml=http://www.ca2.uscourts.gov/decisions/isysquery/3c2ad8d1-b716-49bc-b593-c62ea0d05922/9/hilite/

[55] *Riley v. California* (573 US 2014), http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf

[56] "O caráter fundamental de que se revestem as diretrizes que condicionam a atuação do Poder Público, em tema de restrição ao regime das liberdades públicas, impõe, para efeito de 'disclosure' dos elementos de informação protegidos pela cláusula do sigilo, que o Estado previamente demonstre , ao Poder Judiciário, a ocorrência de causa provável ou a existência de fundadas razões que justifiquem a adoção de medida tão excepcional , sob pena de injusto comprometimento do direito constitucional à privacidade. Nesse sentido, orientam-se diversas decisões proferidas pelo Supremo Tribunal Federal" (INQ 830/MS, Rel Min. Celso de Mello, DJ 1.02.95; INQ 899/DF, Rel Min. Celso de Mello, DJ 23.09.94; INQ 901/DF, Rel. Min. Sepúlveda Pertence, DJ. 23.02.95)

pensamento (art. 5.º, IV), o que não significa que em toda e qualquer interação no ciberespaço ele seja vedado[57].

69. Neste sentido, ganha relevo o princípio da proporcionalidade que atuará de maneira a estabelecer o equilíbrio entre as medidas restritas e o direito à proteção de dados pessoais. E com amparo nesta premissa o art. 23 (1) do Regulamento 679/2016 afirma que as atividades de prevenção, investigação, repressão e sanção criminal podem limitar o direito à proteção de dados pessoais desde que minimamente respeitem a essência dos direitos e liberdades fundamentais que dele decorrem. Percebe-se, portanto, que a proporcionalidade é a peça-chave para o alcance do equilíbrio entre o direito à proteção dos dados pessoais e a segurança pública[58].

70. Assim como o paradigma normativo europeu de proteção de dados e privacidade, as sanções previstas no art. 12 do Marco Civil da Internet também devem ser pautadas pelo princípio da proporcionalidade em sua cominação, tendo sempre em mira a adequação, necessidade, utilidade e proporcionalidade em sentido estrito do seu alcance.

71. Não parece plausível e muito menos proporcional que o descumprimento de uma medida judicial de quebra de sigilo bancário ou telefônico, por exemplo, atinja todos os demais correntistas de uma instituição financeira ou os usuários de uma operadora de telefonia. O Marco Civil constitui um importante patamar regulatório de proteção dos direitos do usuário da internet, porém ainda requer uma cautelosa compreensão de suas premissas e a das formas de implementação das suas sanções.

VI. PEDIDOS

72. Diante dos fatos e fundamentos anteriormente expostos, o **IBIDEM,** em conjunto com o **LAPIN,** acredita ter contribuído de forma singela para que Supremo Tribunal Federal tenha elementos para bem decidir a presente ação e, assim, requer a Vossa Excelência:

---

[57] QASIR, Sophia. Anonymity in Cyberspace: Judicial and Legislative Regulations. *Fordham Law Review*, v. 81, p. 3651, 2012.

[58] SHAH, Reema. Law Enforcement and Data Privacy: A Forward-Looking Approach. *Yale Law Journal*, v. 125, p. 543-543, 2015.

I. A admissão do IBIDEM na condição de *amicus curiae* na presente Arguição de Descumprimento de Preceito Fundamental, nos termos do art. 6.º, §2.º, da Lei n. 9.882/99, e do art. 138 do Código de Processo Civil;

II. Seja conhecida a ADPF incidental, na medida em que voltada à solução de controvérsia judicial causadora de lesão a preceito fundamental, provocada não apenas pela decisão do Juízo da Comarca de Lagarto-SE, mas também por outras que lhe sucederam como a decisão do Juízo da Comarca de Duque de Caxias-RJ;

III. Seja convocada audiência pública para que sejam ouvidas pessoas com experiência e autoridade na matéria, nos moldes do art. 6.º, §1.º, da Lei 9.882/99;

IV. No mérito, seja julgada procedente a ADPF quanto à lesão ao preceito fundamental da liberdade de comunicação, de modo a impedir que novas decisões judiciais suspendam de forma geral, irrestrita e indeterminada os serviços de comunicação de sites, aplicativos e plataformas digitais em razão do não fornecimento de dados de indivíduos determinados ou fatos específicos.

Brasília-DF, 22 de julho de 2016.

THIAGO LUÍS SOMBRA
OAB/DF 28.393
Professor e Coordenador do LAPIN

THIAGO GUIMARÃES MORAES
Acadêmico de Direito

MARCELLE MARTINS LEMES
Acadêmica de Direito

PEDRO LUZ DE CASTRO
Acadêmico de Direito

HENRIQUE BAWDEN CASTRO
Acadêmico de Direito

ANA CLÁUDIA FARRANHA
Professora de Direito

JULIANO ZAIDEN BENVINDO
Professor de Direito

VII. ANEXO

Esta petição de ingresso do *amicus curiae* é acompanhada de um memorial virtual gravado nos estúdios da UnB-TV, apresentado por **Paulo Rená**, Secretário do **Instituo Beta para a Democracia e Internet–IBIDEM**, e **Marcelle Martins**, acadêmica de Direito da Universidade de Brasília-UNB, juntamente com os demais integrantes do Laboratório de Pesquisa Direito Privado e Internet-LAPIN da Faculdade de Direito da Universidade de Brasília.

- Memorial Virtual
- Entrevista dos integrantes do LAPIN sobre o Memorial Virtual para a UnB TV