EXCELENTÍSSIMO SENHOR **MINISTRO EDSON FACHIN** DO EXCELSO SUPREMO TRIBUNAL FEDERAL

ADPF nº 403/SE

FRENTE PARLAMENTAR PELA INTERNET LIVRE E SEM LIMITES, entidade associativa sem fins lucrativos, constituída no âmbito do Congresso Nacional por **211 Deputados Federais,** representada por seu presidente, Deputado Federal João Henrique Holanda Caldas - JHC, com endereço funcional no Gabinete 958, Anexo IV da Câmara dos Deputados, vem respeitosamente perante Vossa Excelência, por meio de seus advogados regularmente constituídos (procuração anexa), com fulcro no art. 7º, § 2º, da Lei n. 9.868/1999, requer sua admissão na qualidade de

AMICUS CURIAE

nos autos da Arguição de Descumprimento de Preceito Fundamental nº 403/SE, em que se requer o reconhecimento da inconstitucionalidade da suspensão dos serviços do aplicativo de mensagens virtuais Whatsapp, e o faz pelas razões de fato e de direito a seguir expostas.

I. DA ARGUIÇÃO DE DESCUMPRIMENTO DE PRECEITO FUNDAMENTAL

O Partido Popular Socialista (PPS) ajuizou a presente arguição, com pedido de medida cautelar, para ver reconhecida a inconstitucionalidade das determinações judiciais de suspensão dos serviços do aplicativo virtual de mensagens Whatsapp.

Em breve síntese, alega o partido Autor haver controvérsia judicial sobre o tema, na medida em que as recentes decisões que suspenderam os serviços do aplicativo foram cassadas logo em seguida pelos respectivos Tribunais de Justiça, o que acabou gerando forte instabilidade e afetando interesses de milhões de pessoas em todo o país.

Sustenta ainda que as determinações de bloqueio violam os princípios da livre comunicação e da proporcionalidade, razão pela qual devem ser consideradas inconstitucionais por esta excelsa Corte Suprema.

Sabe-se que as decisões judiciais que determinaram o bloqueio do Whatsapp tiveram como fundamento dispositivos da Lei nº12.965/2014, notadamente seus arts. 10 a 12, que assim dispõem:

> Seção II
>
> Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas
>
> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7o.
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7o.
>
> § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
>
> § 4º As medidas e os procedimentos de segurança e de sigilo devem ser

> informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.
>
> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
>
> § 2º O disposto no caput aplica-se 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.
>
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
>
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.
>
> 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.
>
> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

Nesse contexto, dada a relevância da matéria versada na presente ADPF, especialmente a discussão tocante ao Marco Civil da Internet, esta Frente Parlamentar pela Internet Livre e Sem Limites pretende ingressar no processo, na qualidade de *amicus curiae*, a fim de contribuir com o debate,

oferecendo novos subsídios oriundos de sua ampla atuação na temática.

II. DO PREENCHIMENTO DOS REQUISITOS PARA INGRESSO NA QUALIDADE DE *AMICUS CURIAE*

A Frente Parlamentar pela Internet Livre e Sem Limites é entidade associativa sem fins lucrativos, constituída no âmbito do Congresso Nacional por **211 Deputados Federais**, que tem como finalidade contribuir para expansão, fortalecimento e aperfeiçoamento de iniciativas que visem à democratização do acesso à internet no País. É o que prevê seu Estatuto, nos seguintes termos:

> *"**Art. 2°**. São finalidades da Frente Parlamentar pela Internet Livre e Sem Limites:*
> *I – Acompanhar a política governamental, os projetos e programas direcionados à internet no País, a democratização e o aumento da qualidade do acesso;*
> *II - contribuir para a expansão, fortalecimento e o aperfeiçoamento de iniciativas que visem a expansão e **democratização do acesso à internet no País**, **visando a não limitação do acesso** e o aumento da qualidade e da velocidade disponibilizada para os usuários;*
> *XI – Zelar pelo cumprimento da legislação que visa regular a internet e seus mecanismos de acesso no País, seja internet fixa ou móvel;"*

No atual contexto comunicacional, predominam os serviços de comunicação eletrônica, que são utilizados por grande parte da sociedade brasileira e mundial, representando o principal meio de comunicação do mundo contemporâneo. Pessoas pertencentes às mais distintas classes sociais, habitantes dos mais diversos lugares do país e possuidoras dos mais diferentes hábitos culturais, utilizam-se preponderantemente de seus *smatphones* ou *tablets* para exercer a comunicação diária.

A presente arguição de descumprimento de preceito fundamental discute basicamente o tema da interrupção dos serviços de troca de mensagens *online* em razão do descumprimento de ordem judicial. Assim, denota-se que a matéria versada nesta ação é de **alta relevância nacional**, e seu resultado terá implicações na vida cotidiana de grande parte dos brasileiros.

Além disso, o tema guarda **pertinência temática** com os objetivos institucionais da Frente Parlamentar pela Internet Livre e Sem Limites, conforme estabelecido por seu Estatuto.

Com efeito, a Requerente vem adotando postura atuante nas discussões acerca da proteção dos direitos dos cidadãos que utilizam a internet. Nesse sentido, recentemente a Frente Parlamentar pela Internet Livre e Sem Limites participou intensamente do debate público acerca da limitação da franquia de dados dos usuários de internet fixa, travando discussões não apenas no Parlamento, como também no Poder Judiciário (por meio de ação popular, doc. 1), na ANATEL e até no CADE (representações, docs. 2 e 3), requerendo inclusive que fossem apuradas eventuais infrações por parte das operadoras.

Ou seja, esta Frente Parlamentar ocupa atualmente posição de destaque no debate acerca do controle estatal do tráfego na internet. Vê-se, portanto, que se trata de entidade dotada de **alta representatividade** em relação ao tema versado na presente arguição, o que autoriza seu ingresso na qualidade de amiga da Corte.

Ressalte-se que este excelso STF já reconheceu, em outras oportunidades, a **legitimidade da intervenção de Frentes Parlamentares**, na condição de *amicus curiae,* em ações constitucionais. A propósito, veja-se a decisão que admitiu a intervenção da Frente Parlamentar Mista da Família e Apoio à Vida na ADO n° 26/DF, de Relatoria do Min. Celso de Mello:

> "**Admito, na condição de "amicus curiae", a Frente Parlamentar "Mista" da Família e Apoio à Vida**, eis que se acham atendidas, na espécie, as condições fixadas no art. 7º, § 2º, da Lei nº 9.868/99. Proceda-se, em consequência, às anotações pertinentes.
> Destaco, ainda, por oportuno, a significativa importância da intervenção formal do "amicus curiae" nos processos objetivos de controle concentrado de constitucionalidade, tal como tem sido reconhecido pela própria jurisprudência desta Suprema Corte [...]
> (ADO 26/DF, rel. Min. Celso de Mello, DJ de 21/09/2015)."

Atendidos os requisitos do art. 7º, § 2º, da Lei nº 9.868/99, requer-se seja deferido o presente pedido de ingresso, admitindo-se a Frente Parlamentar Pela Internet Livre e Sem Limites na condição de *amicus curiae*.

Admitido o ingresso da Requerente, requer-se sejam levadas em consideração, no julgamento desta ADPF, as reflexões a seguir expostas.

III. DA ESSÊNCIA DO MARCO CIVIL DA INTERNET: PROTEÇÃO DA PRIVACIDADE E INTIMIDADE DOS USUÁRIOS DA REDE

De acordo com dados apresentados pelo IBGE (PNAD, 2015), o acesso à internet no Brasil atingiu a marca de 54,4% da população em 2014[1]. O crescimento dessa nova esfera pública de interação da sociedade, aliada à esparsa e, muitas vezes, insuficiente legislação civil e criminal para dirimir conflitos relacionados à internet, impulsionaram o início das discussões, no Congresso Nacional, sobre a regulação do espaço virtual no Brasil.[2]

Os debates sobre a aprovação de diploma que unificasse a regulação do uso da internet, não apenas sob o prisma dos crimes virtuais, mas também da proteção de liberdades civis no espaço cibernético, iniciaram-se em 2011[3] e contaram com significativa participação de diversos setores da sociedade civil. Os anseios da população usuária da internet e das empresas de aplicações virtuais transitavam entre a proteção das liberdades e a conformação adequada do ambiente concorrencial.

Todo esse complexo processo culminou na aprovação da Lei nº 12.965, de 23 de abril de 2014, o Marco Civil da Internet.

Vale destacar que o Brasil foi um dos países pioneiros na regulação da matéria de forma tão profunda[4]. A mencionada lei representa importante passo a caminho da efetivação da liberdade de expressão e proteção da privacidade e intimidade, tendo sido inclusive alvo de elogios por Tim Berners-Lee, um dos criadores da internet[5].

O que se percebe é que, diferentemente do que ocorreu em outros países, tais como EUA, Espanha e França, que possuem forte concepção intervencionista de segurança nacional (aprovando leis que aumentaram o

---

[1] Disponível em http://agenciabrasil.ebc.com.br/economia/noticia/2016-04/celular-e-principal-meio-de-acesso-internet-na-maioria-dos-lares, acessado em 27/05/2016.

[2] SOLAGNA, Fabrício; SOUZA, Rebeca Hennemann V; LEAL, Ondina Fachel. *Quando o Ciberespaço faz as suas leis: o processo do Marco Civil da Internet no contexto de regulação e vigilância global.* Revista Vivência, Ed. Nº 45, 2015, p. 133.

[3] Em 24/08/2011, foi apresentado o Projeto de Lei nº 2126/2011, pelo Poder Executivo, que: "Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil".

[4] Nesse mesmo espírito de busca pela neutralidade de rede e pelas garantias dos usuários, também é possível citar o exemplo do Chile, que aprovou a Lei n° 20.453/2010, a fim de unificar as questões envolvendo o uso de internet no País, ainda que o Código Processual Penal Chileno já estabelecesse regras para o armazenamento de informações pessoais dos usuários de internet.

[5] Disponível em http://exame.abril.com.br/tecnologia/noticias/criadores-da-internet-elogiam-o-marco-civil-da-internet. Acesso em 27/05/2016.

controle e a vigilância sob dados pessoais de usuários que trafegam pela rede[6]), **a tônica preconizada pelo Marco Civil da Internet foi a proteção das liberdades, a guarda da intimidade e da vida privada**.

O art. 3º da Lei nº 12.965/2014 logo deixa claro que o uso da internet no Brasil tem como princípios a proteção da privacidade e dos dados pessoas, senão vejamos:

> "Art. 3º. A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;"

Mais adiante, o art. 8º reitera a primazia do referido diploma legal pelo respeito à privacidade e intimidade dos usuários, *verbis*:

> "Art. 8º. A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet."

Interessante lembrar que em matéria publicada pelo portal Estado de São Paulo no dia 11/04/2010, noticiaram-se algumas posições do Ministério da Justiça acerca do projeto de lei do Marco Civil da Internet:

> "O texto do Marco Civil, bem enxuto perto das 580 páginas resultantes da primeira consulta pública, deixa claro: **provedores não podem monitorar o conteúdo postado por usuários**. **"A gente tenta coibir o vigilantismo. Você não pode obrigar as pessoas a fazer processos de monitoramento, só em caso de autorização judicial"**, diz Almeida (Guilherme Almeida, *assessor da Secretaria de Assuntos Legislativos do Ministério de Justiça).*
>
> (...)
>
> O ministério é contra a ideia da necessidade de identificação para o cidadão. "Não podemos abdicar do que é garantido pela Constituição pelo benefício da investigação criminal", disse ao Link Felipe de Paula, secretário de assuntos legislativos do Ministério da Justiça. "Se a gente trouxer para a vida prática, a necessidade de identificação é a mesma coisa que eu ter de telefonar para a polícia todos os dias ao acordar para informar o meu roteiro. Isso não faz sentido na vida prática nem na internet."[7]

---

[6] SEGURADO, Rosemary. *Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França.* Rio de Janeiro, vol. 22, supl., pp. 1551-1571, 2015. Disponível em http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-59702015001001551&lng=en&nrm=iso. Acesso em 27/05/2016.

[7] http://link.estadao.com.br/noticias/geral,projeto-de-lei-do-marco-civil-aumenta-as-

Vale dizer, trata-se importante diploma legal no contexto comunicacional brasileiro, com caráter fortemente protetivo dos atores que utilizam o espaço virtual como forma de se comunicar.

Assim, dado o contexto em que se insere a Lei nº 12.965/2014, bem como sua dimensão evidentemente protetiva, esta Frente Parlamentar pretende demonstrar a impossibilidade hermenêutica de utilizar o referido diploma como forma de limitar a privacidade dos usuários de internet.

IV. DA INTERPRETAÇÃO INCONSTITUCIONAL DE QUE O ART. 10 OBRIGARIA A GUARDA DE DADOS DE ACESSO E DE CONTEÚDO DE FORMA CONTÍNUA E SEM AUTORIZAÇÃO JUDICIAL

Levando em consideração os objetos da presente ação, bem como a causa de pedir aberta desse tipo de ação constitucional, planeia-se apresentar reflexões que contribuam com o debate sobre o controle judicial do tráfego de dados virtuais.

No entendimento da ora ingressante, antes de se discutir a constitucionalidade da suspensão de serviços de aplicativos de mensagens virtuais, **é fundamental problematizar a própria interpretação de que o art. 10 da Lei nº 12.965/2014 estabeleceria o dever de guarda contínua, antes de qualquer determinação judicial, de registros de acesso e de conexão e de conteúdos de mensagens,** conforme vêm interpretando alguns magistrados nos termos relatados na petição inicial.

Em outras palavras, deve-se questionar, inicialmente, a constitucionalidade dessa interpretação que seria imposta pelo art. 10 da Lei nº 12.965/2014 em prejuízo da privacidade e da intimidade.

De acordo com esse entendimento, o referido preceito legal supostamente imporia dois deveres às empresas de aplicação de mensagens virtuais: (i) o *caput* exigiria que fossem continuamente guardados registros de acesso e de conexão, bem como conteúdos das mensagens privadas trocadas pelos usuários das aplicações de internet; e (ii) o § 2º estabeleceria que, havendo determinação judicial, esses dados deveriam ser disponibilizados. *In verbis*:

---

responsabilidades-dos-usuarios,10000044597.

> Art. 10. A **guarda** e a disponibilização dos **registros de conexão e de acesso** a aplicações de internet de que trata esta Lei, **bem como de dados pessoais e do conteúdo de comunicações privadas**, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 2º O **conteúdo das comunicações privadas** somente poderá ser **disponibilizado mediante ordem judicial**, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

Esse entendimento de que o Marco Civil da Internet permitiria o constante monitoramento dos usuários normalmente tem sido sustentado com base, além do art. 10, também nos arts. 13 e 15 do referido diploma, que dispõem:

> "Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o **dever de manter os registros de conexão**, sob sigilo, em ambiente controlado e de segurança, **pelo prazo de 1 (um) ano**, nos termos do regulamento.
>
> § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.
>
> § 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput."

> "Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos **deverá manter os respectivos registros de acesso a aplicações de internet**, sob sigilo, em ambiente controlado e de segurança, **pelo prazo de 6 (seis) meses**, nos termos do regulamento."

Nesse contexto, é preciso questionar se, face à ordem jurídica vigente, seria constitucional a interpretação de que o legislador teria imposto às empresas de aplicações virtuais o dever de guarda geral e contínua, prévia a qualquer determinação judicial, de registros de acesso e, ainda, de conteúdos de mensagens privadas.

A questão assume especial relevância na medida em que Juízes têm se valido dessa suposta obrigação legal para determinar a suspensão dos serviços de aplicativos de mensagens virtuais como sanção por descumprimento judicial.

Vale dizer, tem-se interpretado o art. 10 do Marco Civil da Internet como fonte da obrigação legal de guarda contínua de registros de conexão e de conteúdo das mensagens privadas por parte por provedores de aplicações virtuais. Surge então o questionamento: **a existência do referido dever de armazenamento constitui interpretação possível do art. 10 do Marco Civil da Internet?**

Para responder ao questionamento, faz-se necessário analisar a questão tanto sob a perspectiva dos cidadãos usuários da rede, quanto das empresas responsáveis pelos aplicativos de troca de mensagens virtuais.

Sob o prisma dos usuários das aplicações de internet, cumpre definir os direitos fundamentais atingidos pela guarda geral dos registros e do conteúdo de todas as mensagens por eles enviadas.

No momento em que o legislador determina que os provedores armazenem todo o registro, inclusive de conteúdo, das mensagens que passam por seus servidores, faz com que as empresas de aplicações de internet (terceiros alheios à comunicação), sem qualquer autorização judicial para tanto, tenham acesso a informações privadas.

Isso viola frontalmente os direitos constitucionais à intimidade, à vida privada e ao sigilo de comunicações, assim enunciados:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Os direitos à intimidade e à vida privada consubstanciam-se na prerrogativa de, por opção própria, manter inacessíveis a outras pessoas as opções e as relações pessoais do indivíduo. Em sua essência, encontra-se o direito ao controle de informações sobre si mesmo[8].

[8] MENDES, Gilmar Ferreira. Op. Cit., p. 268.

Uma das principais maneiras de proteger a intimidade e a vida privada dos indivíduos é justamente garantir o sigilo das comunicações. Nesse sentido, a Constituição Federal prevê que se mantenham em sigilo as diversas modalidades de comunicação realizadas entre pessoas privadas, a fim de impedir que o Estado ou outros particulares tenham livre acesso a informações atinentes à esfera íntima dos cidadãos, o que seria absolutamente contrário à ordem democrática.

Sobre o tema, é de se ressaltar que este excelso STF concebe a proteção do conteúdo das comunicações como um dos pilares do Estado Democrático de Direito, a tal ponto que chega a considerar prova ilícita a escuta telefônica feita por terceira pessoa, sem autorização judicial, ainda que a conversa telefônica indique eventual autoria e/ou materialidade de delito[9]. Isso porque se trata de direito fundamental da mais alta importância no contexto democrático, o que certamente impõe especial resguardo por parte das autoridades estatais.

Nesse contexto, a interpretação de que o art. 10 da Lei nº 12.965/2014 exigiria que as empresas de aplicações virtuais guardassem os registros de acesso e o conteúdo das mensagens enviadas pelos usuários, além de contrariar o próprio espírito do conjunto do Marco Civil, revela-se medida extremamente ofensiva aos referidos direitos fundamentais.

Sob a ótica das empresas de aplicações virtuais essa interpretação do art. 10 do Marco Civil também se mostra inconciliável com os ditames da Carta Maior. Isso porque exigir o armazenamento de todo o conteúdo de todas as conversas de todos os usuários de seus aplicativos é impor ônus excessivamente gravoso às provedoras.

A medida criaria problemas de ordem física e econômica, uma vez que suportar a guarda prévia de escritos, de imagens, de sons e de vídeos da totalidade de usuários que se comunicam a todo instante na rede exigiria extraordinária capacidade de servidores que suportassem o astronômico volume de *bytes* gerado.

Ressalte-se que, apenas no Brasil, tem-se cerca de cem milhões de usuários de aplicativos de mensagens virtuais, que utilizam os serviços das

[9] Nesse sentido, a título de exemplo, vide HC 80.949, STF, Relator Ministro Sepúlveda Pertence, Primeira Turma, DJe de 14/12/2001.

provedoras para se comunicar nas relações pessoais e profissionais, diariamente, ao longo de praticamente todo o dia.

O volume dos dados a serem guardados é abissal, de modo que interpretar aquele dispositivo como sendo fonte da obrigação legal de retenção prévia do teor das mensagens mostra-se extremamente inconveniente e descabido, sobretudo se considerado que a esmagadora maioria do conteúdo não possui qualquer relevância para investigação de ilícitos. Tal compreensão da lei acabaria por comprometer a qualidade dos serviços prestados, além de torná-los mais caros, o que resultaria no repasse dos custos aos destinatários finais.

Além do prejuízo ao mercado como um todo, esses custos afetariam **especialmente as pequenas empresas e as "*startups*"**, que teriam de arcar com pesadas despesas de infraestrutura de armazenamento antes mesmo de terem um mercado consolidado.

Ademais, vê-se que o pesado ônus às empresas imposto por aquela interpretação normativa acabaria por violar o princípio fundamental da livre iniciativa (art. 1º, IV, e art. 170 da CF), segundo o qual a atividade estatal de regulação não pode ser exercida a ponto de inviabilizar o bom desempenho da atividade econômica.

Vale dizer, embora seja função do Estado estabelecer regras que protejam direitos dos consumidores e que conformem o espaço concorrencial, impedindo que a atividade econômica se desenvolva de maneira desenfreada, o princípio da livre iniciativa é violado quando o regramento estatal impõe encargos desnecessários e desarrazoados às empresas[10].

Portanto, tanto sob o ponto de vista dos usuários da rede, quanto sob o prisma das empresas provedoras de aplicações virtuais, conclui-se que, perante a ordem constitucional vigente, os registros de conexão e especialmente o conteúdo das mensagens virtuais exigem intensa proteção, **não se podendo conceber a existência de ato legislativo que estabeleça armazenamento da substância das comunicações**.

É nesse sentido que, além de ofender gravemente diversos direitos

[10] Nesse sentido, veja-se RE 422.941, STF, Relator Ministro Carlos Velloso, Segunda Turma, DJe de 24/03/2006. Veja-se também AI 683.098-AgR, STF, Relatora Ministra Ellen Gracie, Segunda Turma, DJe de 25/06/2010.

fundamentais explicitados *supra*, a interpretação do art. 10 do Marco Civil que estabeleça dever de guarda contínua de registros e de conteúdo privado merece ainda análise à luz do princípio constitucional da proporcionalidade.

Aqui não se trata, contudo, de avaliar se a aplicação de sanções de suspensão de serviços é proporcional – pois esse juízo já foi bem desenvolvido na petição inicial –, mas sim de verificar se seria razoável a imposição legislativa do dever de as empresas guardarem todos os registros de conexão e todo o conteúdo das comunicações privadas de seus usuários.

O princípio da proporcionalidade constitui fundamental ferramenta de aferição do **excesso de poder legislativo**. Com efeito, a discricionariedade do legislador não é ilimitada, devendo ser exercida dentro dos parâmetros instituídos pela Carta Magna, de modo a equacionar os valores constitucionais de forma adequada, necessária e proporcional. Nesse sentido, veja-se a lição do Exmo. Ministro Gilmar Mendes, em sede doutrinária:

> É possível que o vício de inconstitucionalidade substancial decorrente do excesso de poder legislativo constitua um dos mais tormentosos temas do controle de constitucionalidade hodierno. Cuida-se de aferir a compatibilidade da lei com os fins constitucionalmente previstos ou de constatar a observância do princípio da proporcionalidade (Verhältnismässigkeitsprinzip), isto é, de se proceder à censura sobre a adequação (Geeignetheit) e a necessidade (Erforderlichkeit) do ato legislativo.
>
> O excesso de poder como manifestação de inconstitucionalidade configura afirmação da censura judicial no âmbito da discricionariedade legislativa ou, como assente na doutrina alemã, na esfera de liberdade de conformação do legislador (gesetzgeberische Gestaltungsfreiheit).[...]
>
> O conceito de discricionariedade no âmbito da legislação traduz, a um só tempo, ideia de liberdade e de limitação. Reconhece-se ao legislador o poder de conformação dentro de limites estabelecidos pela Constituição. E, dentro desses limites, diferentes condutas podem ser consideradas legítimas[11].

Como é cediço, o princípio da proporcionalidade impede que, para atingir determinado fim, o Estado adote medida mais gravosa do que seria necessário (dimensão da necessidade)[12]. Quando a finalidade almejada pode ser alcançada por meio menos gravoso, o dispositivo normativo não preenche o requisito da necessidade, mostrando-se assim desproporcional e, portanto, inconstitucional.

Entende-se por meio menos gravoso aquele que, dentre todos os

[11] Idem, p. 214.
[12] Idem, p. 227.

que sejam aptos a atingir a mesma finalidade, seja o menos restritivo de direitos fundamentais. No tocante ao presente tema da comunicação de dados virtuais, seria o caso de se aplicar a mesma lógica que atualmente incide sobre as empresas de telefonia, segundo a qual as operadoras somente estão obrigadas a guardar conteúdo de comunicações telefônicas **após** a determinação judicial fundamentada, que aprecie os indícios de cometimentos de ilícitos e ordene a interceptação, nos termos da Lei nº 9.296/96 e das Resoluções nº 59/2008 e 217/2016 do CNJ.

Ou seja, a regra é que as empresas telefônicas não retenham o teor de quaisquer chamadas, respeitando assim o constitucional sigilo das comunicações. Demonstrado o extremo e iminente dano à ordem pública, o Poder Judiciário pode autorizar a quebra do sigilo, a fim de proporcionar a adequada apuração de ilícitos.

Essa dinâmica, além de prevista na mencionada Lei das Interceptações Telefônicas, foi confirmada pela Resolução nº 426/2005 da ANATEL, sobre telefonia fixa, e repetida em termos similares na Resolução nº 477/2007 também da ANATEL, que trata da telefonia móvel. Veja-se:

> Res. nº 426/2005 – ANATEL
>
> Art. 23. A prestadora é responsável pela inviolabilidade do sigilo das comunicações em toda a sua rede, exceto nos segmentos instalados nas dependências do imóvel indicado pelo assinante.
>
> Parágrafo Único. A prestadora tem o dever de zelar pelo sigilo inerente ao STFC e pela confidencialidade quanto aos dados e informações, empregando meios e tecnologia que assegurem este direito do usuário.
>
> Art. 24. A prestadora deve tornar disponíveis os recursos tecnológicos e facilidades necessários à suspensão de sigilo de telecomunicações, determinada por autoridade judiciária ou legalmente investida desses poderes, e manter controle permanente de todos os casos, acompanhando a efetivação dessas determinações, e zelando para que elas sejam cumpridas, dentro dos estritos limites autorizados.
>
> § 1º Os recursos tecnológicos e facilidades de telecomunicações destinados a atender à determinação judicial terão caráter oneroso.
>
> § 2º A Agência deve estabelecer as condições técnicas específicas para disponibilidade e uso dos recursos tecnológicos e demais facilidades referidas neste artigo, observadas as disposições constitucionais e legais que regem a matéria.

Esse procedimento consolidado no âmbito das telefônicas é perfeitamente apto a atingir as finalidades buscadas pelo Poder Público de investigação de ilícitos e possui plena possibilidade de aplicação ao contexto da comunicação de dados virtuais.

Nesse contexto, é possível perceber que a previsão do dever de guarda geral e contínua de registros e de conteúdo, estipulada para as comunicações virtuais, representa meio **mais gravoso do que seria necessário** para atingimento dos objetivos buscados com a norma. Portanto, o dispositivo em apreço não é capaz de ultrapassar o juízo de necessidade.

Pelos fatos e argumentos já colocados acima, fica claro que o dever de guarda prévia de registros e de conteúdo das comunicações *online* privadas, ao desrespeitar uma série de garantias constitucionais de usuários e de empresas, não equaciona bem o conflito de normas constitucionais que exsurge do cotejo entre meios adotados pela norma e os fins almejados.

Por tais fundamentos, entende-se que deve ser dada interpretação conforme a Constituição ao art. 10 da Lei nº 12.965/2014, a fim de impedir toda e qualquer interpretação a essa norma que estabeleça dever das provedoras de retenção, contínua e prévia à determinação judicial, de dados relativos aos registros de acesso e ao conteúdo das comunicações privadas dos usuários.

V. DA NECESSIDADE DE EXTREMA CAUTELA NA RESTRIÇÃO À PRIVACIDADE. HISTÓRICO BRASILEIRO DE ABUSOS EM INTERCEPTAÇÕES TELEFÔNICAS

É de se notar que, quanto a **outras modalidades de comunicação**, não há, no ordenamento jurídico brasileiro, qualquer dispositivo legal que determine a guarda geral e contínua de registros e/ou de conteúdo.

Conforme já mencionado *supra*, há previsão tão somente de interceptação das comunicações em hipóteses excepcionais, quando houver fortes indícios da prática de crimes, e sempre após a determinação judicial. É o caso, por exemplo, da Lei nº 9.296/96, que regulamenta a interceptação telefônica.

Por força da referida lei, as comunicações telefônicas são realizadas, como regra, em sigilo. A menos que o Poder Judiciário determine a interceptação, após demonstrados os requisitos legais (art. 2º da Lei nº 9.296/96)[13], as empresas de telefonia não guardarão o conteúdo das ligações.

[13] Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer

Sobre o tema da quebra de sigilo de comunicações, importante ressaltar que, em 2008, o **Conselho Nacional de Justiça**, sob a presidência Ministro Gilmar Mendes, ocupou-se de debater amplamente o cometimento de **abusos** por parte das autoridades policiais e judiciais, no tocante às interceptações telefônicas. Isso porque, conforme amplamente noticiado à época, somente no ano de 2007 haviam sido autorizadas mais de 409 mil interceptações telefônicas, sem contar os inúmeros – e absurdos – casos de grampos clandestinos que atingiram até mesmo Ministros do Supremo Tribunal Federal.

Verificou-se, naquele período, um quadro de **verdadeira banalização dos procedimentos de interceptação das comunicações telefônicas**, que colocava em cheque direitos e garantias fundamentais dos cidadãos, enfraquecendo assim o próprio Estado Democrático de Direito. Os números excessivos chegavam a incutir nas pessoas o temor de estarem constantemente "grampeadas", vendo assim ameaçada grande parte de sua intimidade.

Como resposta, o CNJ editou a Resolução nº 59/2008, que uniformizou a regulamentação dos procedimentos de interceptação telefônica, ampliando as exigências para autorização das quebras de sigilo. Atualmente, sobretudo após as alterações feitas pela recente Resolução nº 217/2016/CNJ, tem-se que a interceptação de comunicação telefônica é procedimento a ser adotado apenas em casos extremamente graves, nos quais os fundados indícios de cometimentos de crimes tornem efetivamente necessária a medida.

A postura do CNJ sobre a questão, no intuito de garantir o respeito ao sigilo das comunicações, demonstra a relevância do tema e indica que as instituições brasileiras estão comprometidas com a garantia dos direitos mais íntimos dos cidadãos.

Por certo, o raciocínio jurídico-constitucional precisa ser atualizado e aplicado às comunicações virtuais, de modo que, também para essa

---

qualquer das seguintes hipóteses:

I - não houver indícios razoáveis da autoria ou participação em infração penal;

II - a prova puder ser feita por outros meios disponíveis;

III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.

modalidade de interlocução, a fim de atender ao amplo e legítimo objetivo estatal de investigação de ilícitos, sejam respeitados os ditames constitucionais de proteção aos direitos fundamentais à intimidade, à vida privada e ao sigilo de comunicações.

Portanto, por ser extremamente restritiva de direitos fundamentais da privacidade e intimidade dos usuários, parece não haver dúvidas quanto à inconstitucionalidade da interpretação do art. 10 da Lei nº 12.965/2014 que imponha a obrigação de guarda de registros de acesso e de conexão, bem como do conteúdo de comunicações privadas, de forma contínua e prévia a qualquer determinação do Poder Judiciário.

VI. DO EXEMPLO EUROPEU: PREVALÊNCIA DA PROTEÇÃO À PRIVACIDADE MESMO NO CONTEXTO DE COMBATE AO TERRORISMO. PERSPECTIVA DOS *CHILLING EFFECTS*

Após os famigerados atentados terroristas de 11 de setembro de 2001, difundiu-se com bastante intensidade a concepção vigilantista do controle do tráfego de informações virtuais no mundo. A propósito, veja-se a narrativa que se encontra na doutrina:

> O 11 de Setembro criou na Europa a oportunidade para modificar a agenda política e incrementar mudanças que já vinham ocorrendo no sentido de uma **maior 'securitização' da sociedade europeia**. Tornou-se mais difícil para as forças políticas oporem-se à coleta, retenção e compartilhamento de informações pelas autoridades de segurança. Tal mudança foi acompanhada de uma **nova tendência na segurança pública denominada 'dataveillance' (vigilância de dados)**, que contempla a análise de dados por meio da convergência de tecnologias e bancos de dados para vigiar pessoas ou grupos suspeitos que possam representar risco potencial à segurança. A vigilância de dados usa novas tecnologias para identificar grupos de risco com base em diferentes padrões de 'comportamento suspeito' ao nível dos bancos de dados privados e públicos.[14]

Nesse contexto, no ano de 2006 o Parlamento Europeu aprovou a Diretiva 2006/24/CE, que impôs aos Estados europeus o dever de aprovar leis que determinassem a obrigação de conservação de registros de conexão e de acesso da comunicação virtual, pelo período de 6 (seis) meses a 2 (dois) anos. Confiram-se trechos da mencionada Diretiva Europeia (doc. 4):

[14] CHAVES, Christian Frau Obrador. *A luta contra o terrorismo e a proteção de dados pessoais: análise crítica de um precedente do Tribunal Constitucional Alemão (Bundesverfassungsgericht).* Disponível em www.agu.gov.br/page/download/index/id/5211353. Acesso em 27/05/2016.

> Artigo 5º
> Categorias de dados a conservar
> 1. Os Estados-Membros devem assegurar a conservação das categorias de dados seguintes em aplicação da presente diretiva:
> a) Dados necessários para encontrar e identificar a fonte de uma comunicação: [...]
> b) Dados necessários para encontrar e identificar o destino de uma comunicação: [...]
> c) Dados necessários para identificar a data, a hora e a duração de uma comunicação: [...]
> d) Dados necessários para identificar o tipo de comunicação: [...]
> e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento: [...]
> f) Dados necessários para identificar a localização do equipamento
> 2. Nos termos da presente diretiva, **não podem ser conservados quaisquer dados que revelem o conteúdo das comunicações**.
>
> Artigo 6º
> Períodos de conservação
> Os Estados-Membros devem assegurar que as categorias de dados referidos no artigo 5º sejam conservadas **por períodos não inferiores a seis meses e não superiores a dois anos, no máximo, a contar da data da comunicação**.
>
> Artigo 15º
> Transposição
> 1. Os Estados-Membros devem pôr em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva o mais tardar em 15 de Setembro de 2007 e informar imediatamente a Comissão desse facto. Quando os Estados-Membros aprovarem essas disposições, estas devem incluir uma referência à presente directiva ou ser acompanhadas dessa referência aquando da publicação oficial. As modalidades de referência são aprovadas pelos Estados-Membros.

Como se vê, a Diretiva 2006/24/CE previu o dever de guarda de dados virtuais privados pelo período de seis meses a dois anos, limitados, contudo, aos registros de acesso e de conexão, ficando a salvo o sigilo do conteúdo das comunicações virtuais.

Veja-se, portanto, que **nem mesmo no contexto da concepção vigilantista surgida na Europa** chegou-se a exigir a obrigação drástica de guardar o conteúdo das comunicações privadas virtuais, o que se vem tentando interpretar do art. 10 do Marco Civil da Internet, diploma cuja ideia central foi exatamente a de preservar a intimidade e a privacidade, ao contrário da lógica adotada na Diretiva europeia.

De qualquer maneira, nem mesmo a obrigação de guarda de registros de acesso e de conexão prevaleceu na Europa.

Com efeito, em 2014 o Tribunal de Justiça Europeu considerou inválida a Diretiva de Retenção de Dados 2006/24/CE por entender tratar-se de norma que **viola os diretos fundamentais à vida privada e à proteção de dados pessoais**. Para a Corte Europeia, a Diretiva não observou o princípio da proporcionalidade, pois ultrapassou os limites do que seria estritamente necessário para atingimento das finalidades investigativas pretendidas pelo Poder Público (doc. 5).

Mas antes mesmo da apreciação pelo Tribunal de Justiça Europeu, diversas Cortes Constitucionais nacionais já haviam declarado inconstitucionais as normais internas (leis de transposição) que, seguindo a Diretiva de Retenção de Dados 2006/24/CE, determinavam a retenção prévia de dados sobre fonte, destinatário, data, horário, modalidade, instrumento utilizado, e local das comunicações.

Por exemplo, em 2007 a Alemanha aprovou a lei de transposição da referida Diretiva Europeia 2006/24/CE para seu ordenamento jurídico[15] e em 2008 o tema foi levado à apreciação de seu Tribunal Constitucional. Em juízo preliminar, a Corte concedeu liminar para suspender imediatamente os efeitos da lei até julgamento final e, em 2010, julgou o mérito da ação, considerando **inconstitucional a guarda de dados virtuais** nos moldes estipulados pela Diretiva Europeia e pela norma alemã (doc. 6)[16].

A mais alta Corte da Alemanha entendeu que a norma que obrigava a retenção prévia de registros de conexão e de acesso (frise-se: sequer o conteúdo) ofendia o art. 10.1 de sua Constituição alemã, que estabelece a inviolabilidade e a privacidade da correspondência e das telecomunicações.

Na ocasião, o Tribunal Constitucional alemão considerou que a lei também violava o princípio da proporcionalidade, ao fundamento de que, carente de medidas de segurança de dados e de transparência, criava-se a **sensação de monitoramento permanente**, permitindo alto grau de conhecimento da vida privada dos cidadãos por parte das autoridades estatais, inclusive de questões altamente pessoais. *In verbis*:

---

[15] Act for the Amendment of Telecommunications Surveillance and Other Measures of Undercover Investigation and for the Implementation of Directive 2006/24/EC of 21 December 2007 (Federal Law Gazette part I 2007, p. 3198).

[16] Disponível, no idioma inglês, em http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html

> *A guarda preventiva sem justificativa de todo o tráfego de dados das telecomunicações, pelo período de seis meses, constitui séria invasão, porque pode criar a sensação de monitoramento permanente; de uma forma sem precedentes, permite alto grau de conhecimento da vida privada, sem que o recurso a estes dados seja diretamente perceptível ou visível pelos cidadãos. O indivíduo não sabe o que a autoridade estatal sabe sobre ele, mas sabe que possivelmente conhece grande parte de sua vida, incluindo questões altamente pessoais* (tradução livre) [17].

A Suprema Corte da Alemanha asseverou ainda que, em nome da prevenção/precaução, os dados pessoais somente podem ser utilizados em situações excepcionais, quando há perigo concreto à vida, à integridade física, à liberdade de uma pessoa ou um concreto risco à segurança pública. Somente nessas hipóteses seria possível quebrar o constitucional direito à privacidade/proteção de dados pessoais (the right of privacy)[18].

Assim, embora se soubesse que tais dados poderiam ser úteis no combate ao crime, a Corte alemã entendeu que **nem toda medida útil à persecução criminal é permitida constitucionalmente**.

Veja-se que o debate europeu sobre o tema concluiu que a guarda de dados de registro de acesso e de conexão a aplicações virtuais de comunicação é desarrazoada, representando medida violadora de garantias fundamentais e, portanto, meio mais gravoso do que o estritamente necessário para alcançar os fins almejados.

Atualmente, a questão da proteção de dados pessoais na Europa vem sendo discutida à luz dos chamados "***chilling effects***", ou dos efeitos inibidores. Por essa doutrina, a captura de dados pessoais, ou até mesmo a mera possibilidade de que informações pessoais sejam retidas, constitui intensa interferência na privacidade dos cidadãos, de modo a desencorajá-los de exercer direitos fundamentais, notadamente o direito à expressão e à comunicação privada. Nesse sentido, vem apontando a doutrina europeia:

---

[17] Trecho do original no idioma ingles: "§241 - a) Precautionary storage without cause of all telecommunications traffic data for a period of six months is such a serious encroachment *inter alia* because it can create a sense of being permanently monitored; in an unforeseen manner, it permits a high degree of knowledge of private life, without the recourse to the data being directly perceptible by or visible to the citizen. The individual does not know which state authority knows what about him or her, but knows that the authorities may know a great deal about him or her, including highly personal matters".

[18] CHAVES, Christian Frau Obrador, *Op. Cit. [A luta contra...]* p. 7.

> *Segue disso que qualquer captura de dados de comunicação é potencialmente uma interferência na privacidade e, além disso, que a coleta e retenção de dados de comunicações significa uma interferência na privacidade quer ou não estes dados sejam posteriormente consultados ou usados. Mesmo a mera possibilidade das informações de comunicação serem capturadas cria uma interferência na privacidade, com um efeito desencorajador (chilling effect) em direitos, incluindo aqueles à liberdade de expressão e associação. A própria existência de um programa de vigilância em massa então cria uma interferência na privacidade* (tradução livre)[19].

É dizer, a preocupação em impedir o avanço da concepção vigilantista, no que tange ao controle de dados virtuais, traduz-se na necessidade de que sejam efetivamente garantidos os direitos dos cidadãos usuários da rede mundial de computadores, como importante expressão do Estado Democrático de Direito.

Ao adotar a interpretação do art. 10 do Marco Civil da Internet que determina a guarda de dados de registro de acesso e de conexão de usuários e de conteúdo de comunicações privadas, de forma contínua e prévia à determinação judicial, o Brasil põe-se em completo desacordo com o que vem sendo construído no cenário jurídico internacional.

Portanto, esta ADPF possui **relevância histórica** no debate sobre controle estatal de dados pessoais eletrônicos. Daí a importância de se levar em consideração o debate europeu sobre o tema, sobretudo tendo em vista a repercussão que a decisão deste Supremo Tribunal Federal brasileiro seguramente alcançará nas Cortes Internacionais.

VII. DA *MENS LEGIS* DO ART. 12: IMPOSSIBILIDADE DE SUA APLICAÇÃO COMO PUNIÇÃO CONTRA AQUELE QUE PROTEGE A PRIVACIDADE DOS USUÁRIOS

Ficou demonstrada a inconstitucionalidade da interpretação dada ao art. 10 do Marco Civil da Internet, segundo a qual haveria dever de guarda contínua e sem autorização judicial dos registros de conexão, bem como do conteúdo das comunicações virtuais. Assim, são claramente indevidas determinações judiciais de disponibilização do teor de conversas pretéritas.

---

[19] PILLAY, Navi. The Right to Privacy in the Digital Age. Nações Unidas, Conselho de Direitos Humanos, 2015. Disponível em: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf. Acesso em 06/06/2016.

Dito isso, cumpre a esta Frente Parlamentar também discorrer acerca da problemática envolvendo o art. 12 da Lei 12.965/2014 – notadamente seus incisos III e IV.

Inicialmente, imprescindível que se faça análise topográfica do art. 12 dentro da estrutura normativa do Marco Civil da Internet: o dispositivo está inserido no Capítulo III, Seção II, intitulada "Da **Proteção** aos Registros, aos **Dados Pessoais** e às **Comunicações Privadas**".

Esta seção, por sua vez, é composta também pelos arts. 10 e 11 – aos quais o próprio art. 12 faz expressa referência –, de modo que se torna imperiosa sua leitura para compreensão do que está sendo regulado. Para tanto, transcrevem-se abaixo os *caputs* dos dispositivos, no intuito de promover interpretação sistemática e teleológica:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> 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:
> (...)
> 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.

Da leitura conjunta, percebe-se que, como já indicava o título da Seção II, os artigos visam a garantir o respeito à intimidade, à vida privada, à honra e à imagem de todos os usuários que tiverem seus dados coletados e armazenados pelos provedores e aplicativos, sob pena de sanções.

E, no que tange especificamente às sanções previstas nos incisos III e IV, estas são aplicáveis **somente aos casos que envolvam atos previstos no art. 11, vale dizer, somente que violem a privacidade, a proteção de**

dados pessoais e o sigilo das comunicações privadas.

Perante tais circunstâncias, surge a primeira questão: é possível se valer do art. 12, incisos III e IV, da Lei 12.965/2014 para fundamentar a suspensão das atividades de empresa que, resguardando a privacidade dos usuários, não atenda à ordem judicial que determine a apresentação de seus dados? Entende-se que não.

A bem da verdade, tal entendimento representaria verdadeira **subversão** do que fora normatizado. Isso porque as penas de suspensão temporária e proibição de exercício de atividades são aplicáveis àquelas empresas que, em desrespeito ao sigilo e à privacidade, divulguem dados pessoais de seus usuários, até mesmo como forma de obtenção de receita (como fazem, hoje, várias empresas na internet). **E não o contrário**.

Em termos simples: tal penalidade não serve para coagir ou punir determinada empresa por não apresentar os dados de seus usuários, mas sim penalizar a empresa que indevidamente os transmite ou publiciza.

O fato de a empresa não atender à decisão judicial, resguardando o sigilo dos dados de seus usuários de forma absoluta (resguardando-os, inclusive, da Justiça brasileira), pode até configurar algum excesso ou infração, **mas jamais violação ao art. 11, de modo a ensejar a aplicação das penas do art. 12**.

O cumprimento da norma, ainda que em excesso, não pode justificar a aplicação da penalidade atribuída ao seu descumprimento. Tal circunstância se traduziria em teratologia, na medida em que o jurisdicionado estaria sendo punido por cumprir o que lhe fora imposto.

Corroborando o que foi dito, destaca-se trecho de entrevista concedida à revista Época pelo Professor Ronaldo Lemos, advogado especialista em tecnologia e considerado um dos criadores do Marco Civil da Internet:

> Pergunta: Alguns lugares, até mesmo o site do TJ-SP que noticiou isso, cita que o prazo de 48 horas foi com base no Marco Civil. Qual a explicação?
>
> **Lemos -** Justamente, está errado. É curioso porque em tentativas anteriores de derrubar aplicativos no Brasil os tribunais submeteram as decisões com base no Marco Civil. Isso é que impressiona. O que acho que **está acontecendo é uma interpretação errada do artigo 12**, que prevê algumas sanções para sites, mas não prevê suspensão de serviço ou aplicativo. **Quando fala de suspensão, fala de suspensão das atividades previstas no artigo 11**, e o artigo 11 fala da atividade e tratamento, monitoramento de dados e comunicações. **Ou seja, a sanção que o Marco Civil estabelece é suspender a empresa de tratar e ganhar dinheiro com publicidade**

> **relativa a dados de usuários, que é a principal fonte de receita de muitas empresas na internet hoje. Mas isso é muito diferente de você suspender o serviço. Isso não está previsto em nenhum lugar**, então basta ler o artigo 11 e artigo 12 para ver que não tem nada a ver no Marco Civil com suspensão do serviço ou da atividade de empresas de internet. Acho que pode ter ocorrido uma interpretação equivocada desse artigo. Mas é um espanto, porque primeiro está claro no Marco Civil, e segundo também tem implicações constitucionais, e o que foi feito aqui é **totalmente inconstitucional**.[20]

Além disso, outro ponto crucial deve ser observado.

Quando a redação legal descreve como penalidades a "suspensão temporária das atividades que envolvam os atos previstos no art. 11" (inc. III) e a "proibição de exercício das atividades que envolvam os atos previstos no art. 11" (inc. IV), **não se quer dizer a suspensão ou proibição da prestação do serviço ou aplicação de internet**.

Conforme se extrai da própria redação legal, a penalidade é direcionada unicamente aos atos violadores da privacidade, da proteção dos dados pessoais e do sigilo das comunicações, e não às atividades da empresa por completo – vale dizer, ao serviço por ela prestado.

Se assim o fosse, a redação se restringiria a dizer "suspensão temporária das atividades da empresa", ou simplesmente "proibição de exercício das atividades". Mas salientou, de forma expressa, tratar-se das "atividades que envolvam os atos previstos no art. 11".

E quais são esses atos? São as operações de coleta, armazenamento, guarda ou tratamento de registros, dados pessoais ou de comunicações privadas, tais como previstas naquele dispositivo.

Desta forma, caso uma empresa divulgue indevidamente dados de um usuário, poderá ser suspensa ou mesmo proibida alguma atividade relacionada à coleta, armazenamento, guarda ou tratamento destes dados. Isto é **diferente de determinar suspensão total e irrestrita das atividades da empresa.**

Visando a esclarecer a diferença entre as duas medidas, interessante mencionar exemplo frequente no dia-a-dia.

---

[20] Disponível em: http://epoca.globo.com/vida/experiencias-digitais/noticia/2015/12/estamos-rasgando-o-marco-civil-e-constituicao-diz-ronaldo-lemos-sobre-whatsapp.htm. Acesso em: 25/05/2016.

Imagine-se que uma pessoa, interessada em planejar suas férias, pesquise nos sites de busca acomodações em hotéis no Caribe. Poucas horas depois, ao acessar sua conta em uma rede social, depara-se com publicidades, em sua página, de companhias aéreas anunciando passagens promocionais para o Caribe, bem como de companhias de turismo vendendo passeios nas mais belas praias daquela região.

Ao contrário do que parece, não se trata de mera coincidência. Tais ofertas só estão na página daquela pessoa porque os dados de sua pesquisa foram indevidamente fornecidos ou divulgados pelo site de buscas, que muitas vezes se utilizam destas informações como forma de obtenção de renda.

Neste caso, o que o art. 12 permite é a aplicação de penalidade para que se suspenda ou mesmo interrompa a atividade divulgadora destes dados, e não a retirada do ar da rede social ou do site de buscas por período determinado, prejudicando terceiros e impedindo que qualquer outra pessoa tenha acesso a elas e/ou às suas respectivas contas.

Nesse contexto, reiteram-se as seguintes conclusões: (i) a *mens legis* do art. 12 é proteger o sigilo e a privacidade dos dados dos usuários, punindo a empresa que indevidamente publiciza seus dados pessoais – e não aquela que os protege ou retém; e (ii) o Marco Civil da Internet não possui dispositivo algum prevendo a penalidade de suspensão ou impedimento **de serviço ou aplicativo**, mas apenas das atividades que envolvam atos previstos no art. 11, da Lei 12.965/2014.

Isto significa, em vias transversas, que o Judiciário está impedido de sancionar empresas que descumpram suas ordens e determinações? Por óbvio, não.

O que se quer demonstrar é que **não é do Marco Civil da Internet que o Judiciário retirará o substrato legal para tanto**, muito menos para aplicar a pena grave de suspensão ou impedimento de serviços ou aplicativos (haja vista que, como exaustivamente demonstrado, tal penalidade sequer é prevista na Lei 12.965/2014).

O descumprimento de ordem judicial pode ensejar multas cominatórias (como as *astreintes*, previstas no art. 537, §1º, do CPC); configurar, em casos mais graves, crime de desobediência, tipificado no art. 330 do Código Penal Brasileiro; dentre outras medidas. Não configura, contudo, ato violador do art. 11 hábil a ensejar a aplicação do art. 12, ambos do Marco Civil da Internet.

Em suma: a não disponibilização dos dados, diante de determinação judicial, poderá configurar alguma infração ao ordenamento jurídico vigente, mas jamais ao art. 11 do Marco Civil da Internet. A aplicação deturpada desse artigo, mormente no que tange à aplicação de pena gravosa e não prevista no ordenamento, configura ofensa aos princípios da legalidade e da proporcionalidade (arts. 5º, II e LIV, e 37, *caput*, da CF).

À legalidade, porque as penas exigem tratamento restritivo, bem como previsão legal para sua imposição. E à proporcionalidade, porque não apenas se estaria aplicando penalidade não prevista no ordenamento, como ainda o faria de forma extremamente gravosa para as empresas prestadoras de serviços e aplicações na internet, e em prejuízo aos usuários.

Por tais fundamentos, entende-se que deve ser dada **interpretação conforme a Constituição ao art. 12, incisos III e IV**, da Lei 12.965/2014, para que este excelso Supremo Tribunal Federal expressamente defina que o art. 12 não é hábil a fundamentar a aplicação de penas às empresas que descumpram ordem judicial de apresentação de dados, registros ou comunicações privadas.

VIII. DOS PEDIDOS

Diante do exposto, atendidos os requisitos do art. 7º, § 2º, da Lei nº 9.868/99, requer-se seja deferido o presente pedido de ingresso, **admitindo-se a Frente Parlamentar Pela Internet Livre e Sem Limites na condição de *amicus curiae***.

Admitido o ingresso da Requerente, espera-se que sejam levadas em consideração as reflexões ora apresentadas, a fim de que:

a. Por violação aos direitos fundamentais à intimidade, à vida privada e ao sigilo das comunicações, e pela ofensa ao princípio da proporcionalidade, seja dada **interpretação conforme a Constituição ao art. 10** da Lei nº 12.965/2014, a fim de impedir toda e qualquer interpretação a essa norma que estabeleça a obrigação de que as provedoras de aplicações virtuais retenham e guardem contínua e irrestritamente os dados relativos aos registros de acesso e de conexão, bem como

o conteúdo das comunicações privadas dos usuários;

b. Sucessivamente, caso se entenda existir o dever de guarda contínua de dados e conteúdo das comunicações privadas dos usuários de internet, seja dada **interpretação conforme a Constituição ao art. 12, incisos III e IV**, da Lei 12.965/2014, para que este excelso Supremo Tribunal Federal expressamente defina que o art. 12 não é hábil a fundamentar a aplicação de penas às empresas que descumpram ordem judicial de apresentação de dados, registros ou comunicações privadas.

Por oportuno, pede-se que seja cadastrado nos autos o advogado **Rafael de Alencar Araripe Carneiro, inscrito na OAB/DF sob o nº 25.120**, em nome do qual se requer sejam realizadas as intimações e demais comunicações processuais, sob pena de nulidade.

Nestes termos, pede deferimento.
Brasília, 05 de outubro de 2016.

Rafael de Alencar Araripe Carneiro
OAB/DF 25.120

João Otávio Fidanza Frota
OAB/DF 46.115

Luiz Philippe Vieira de Mello Neto
OAB/DF 50.312

Igor Suassuna Lacerda de Vasconcelos
OAB/DF 47.398