MEDIDA CAUTELAR EM MANDADO DE SEGURANÇA 38.187 DISTRITO FEDERAL

RELATOR	**: MIN. GILMAR MENDES**
IMPTE.(S)	: BRASIL PARALELO ENTRETENIMENTO E EDUCAÇÃO S.A
ADV.(A/S)	: SEM REPRESENTAÇÃO NOS AUTOS
IMPDO.(A/S)	: PRESIDENTE DA COMISSÃO PARLAMENTAR DE INQUÉRITO DO SENADO FEDERAL - CPI DA PANDEMIA
ADV.(A/S)	: CHRYSTIAN REIS DE FIGUEIREDO
ADV.(A/S)	: EDVALDO FERNANDES DA SILVA
ADV.(A/S)	: FERNANDO CESAR DE SOUZA CUNHA
ADV.(A/S)	: THOMAZ HENRIQUE GOMMA DE AZEVEDO

DECISÃO: Trata-se de mandado de segurança, com pedido liminar, impetrado por Brasil Paralelo Entretenimento e Educação S. A. contra a aprovação dos Requerimentos 1362/2021 e 1364/2021 pela Comissão Parlamentar de Inquérito do Senado Federal concernente ao enfrentamento da pandemia da Covid-19 no Brasil (CPI da Pandemia).

A impetrante narra que a CPI da Pandemia aprovou, em 3 de agosto de 2021, o Requerimento 1228/2021, item 106 (eDOC 4), cujo objeto consistia no afastamento dos sigilos telefônico, bancário e telemático da impetrante.

Contra esse ato, a autora impetrou o mandado de segurança autuado sob o nº 38.117. Na condição de relator, deferi parcialmente o pedido liminar então formulado, para restringir temporalmente as quebras de sigilo ao período de pandemia no Brasil.

Após a decisão liminar proferida naqueles autos, a CPI da Pandemia aprovou, em 19/08/2021, os Requerimentos 1362/2021 (eDOC 11) e 1364/2021 (eDOC 12), apresentados como aditamento ao Requerimento 1228/2021.

Os novos requerimentos, que constituem o objeto deste mandado de segurança, veiculam o afastamento dos sigilos telemático, telefônico, bancário e fiscal, fixando como termo inicial 1º de janeiro de 2019.

A impetrante alega na petição inicial que o ato coator carece de

fundamentação, uma vez que o requerimento aprovado na Comissão Parlamentar de Inquérito teria colacionado informações genéricas, sem relação concreta e específica com a atuação da sociedade empresária. Além disso, aduz que não houve a indicação das informações que se pretende obter com a quebra do sigilo.

Salienta "a ausência de qualquer elemento, nos Requerimentos, que materializasse qualquer tipo de relacionamento da Impetrante com o Governo, ou mesmo influência nas tomadas de 31 decisões por agentes públicos. Novamente, não houve qualquer tipo de fato individualizado que pudesse ao menos sugerir tal conexão".

Anota que tampouco foram especificados quais colaboradores da impetrante teriam os sigilos telefônico e telemático afastados.

Afirma que o afastamento dos sigilos telefônico e telemático viola direitos ostentados pela impetrante enquanto veículo de comunicação, especialmente o princípio da liberdade de imprensa. Articula ainda com a necessidade de resguardar o sigilo da fonte.

Tece considerações acerca do documentário "7 Denúncias: as consequências do caso Covid-19", produzidos pela impetrante, mencionado nos Requerimentos aprovados pela CPI da Pandemia, defendendo que não há ali qualquer notícia falsa no tocante ao enfrentamento da pandemia.

Por fim, alega que há incoerência temporal na quebra do sigilo e desrespeito à decisão liminar proferida no MS 38.117, já que alcança o ano de 2019, enquanto a pandemia de Covid-19 iniciou-se em 2020.

Requer, liminarmente, a suspensão dos efeitos da aprovação dos Requerimentos 1362/2021 e 1364/2021 pela CPI da Pandemia, até o julgamento definitivo deste Mandado de Segurança.

Subsidiariamente, pleiteou que seja determinada a limitação temporal da quebra a 20 de março de 2020 e a manutenção do sigilo absoluto sobre os dados da empresa eventualmente obtidos, "cominando-se multa por descumprimento da obrigação em caso de vazamento de dados e informações".

No mérito, pede a concessão da ordem, para confirmar a medida

acauteladora e "declarar a nulidade dos Requerimentos nº 1362/2021 e 1364/2021 (Aditamentos ao Requerimento nº 01228/2021, item 106), determinandose os seus arquivamentos em caráter definitivo".

A autoridade dita coatora prestou informações (eDOC 19). Defendeu a higidez do afastamento dos sigilos telefônico, telemático, bancário e fiscal. Discorreu sobre o papel constitucional das comissões parlamentares de inquérito e aduziu a adequação da fundamentação adotada para a aprovação da quebra dos sigilos. Quanto ao marco temporal, afirmou que os dados anteriores ao período de pandemia são necessários para comparação "entre os eventos diretamente afetados ao inquérito parlamentar e fatos anteriores".

É o relatório.

Passo a apreciar o pedido de tutela de urgência.

A questão controvertida nesta ação mandamental versa sobre a legalidade de atos da CPI da Pandemia que implicaram o afastamento dos sigilos bancário, fiscal, telefônico e telemático da impetrante.

Os argumentos veiculados na petição inicial cingem-se, em síntese, aos seguintes pontos: **(i)** ausência de fundamentação, consideradas (i.i) a falta de individualização das condutas imputadas à impetrante e de sua vinculação aos fatos investigados, (i.ii) a não delimitação dos sujeitos alcançados pelo afastamento do sigilo; **(ii)** incoerência temporal, tendo em vista o período de pandemia; e **(iii)** o caráter de veículo de comunicação, a exigir tratamento adequado ao direito à liberdade de expressão.

1 – Sindicabilidade do ato de investigação parlamentar

De início, e antes de analisar as alegações da impetrante, anoto que o Supremo Tribunal Federal há muito consolidou o entendimento de que os atos praticados pelas Comissões Parlamentares de Inquérito, malgrado sua estatura constitucional, estão sujeitos ao controle jurisdicional.

Embora a Constituição Federal tenha assegurado às Comissões poderes de investigação próprios das autoridades judiciais, é certo que não as eximiu da observância dos preceitos conformadores do próprio Estado Democrático de Direito, tendo em vista o controle permanente da autoridade estatal e a eficácia dos direitos fundamentais.

Nesse sentido, cabe ao Poder Judiciário garantir que o implemento dos atos de investigação das Comissões Parlamentares de Inquérito dê-se em conformidade com os quadrantes constitucionais.

Confira-se, a propósito, precedente do Tribunal Pleno, relatado pelo eminente Min. Celso de Mello:

> COMISSÃO PARLAMENTAR DE INQUÉRITO - QUEBRA DE SIGILO - AUSÊNCIA DE INDICAÇÃO CONCRETA DE CAUSA PROVÁVEL - NULIDADE DA DELIBERAÇÃO PARLAMENTAR - MANDADO DE SEGURANÇA CONCEDIDO. A QUEBRA DE SIGILO NÃO PODE SER UTILIZADA COMO INSTRUMENTO DE DEVASSA INDISCRIMINADA, SOB PENA DE OFENSA À GARANTIA CONSTITUCIONAL DA INTIMIDADE. - A quebra de sigilo, para legitimar-se em face do sistema jurídico-constitucional brasileiro, necessita apoiar-se em decisão revestida de fundamentação adequada, que encontre apoio concreto em suporte fático idôneo, sob pena de invalidade do ato estatal que a decreta. A ruptura da esfera de intimidade de qualquer pessoa - quando ausente a hipótese configuradora de causa provável - revela-se incompatível com o modelo consagrado na Constituição da República, pois a quebra de sigilo não pode ser manipulada, de modo arbitrário, pelo Poder Público ou por seus agentes. Não fosse assim, a quebra de sigilo converter-se-ia, ilegitimamente, em instrumento de busca generalizada, que daria, ao Estado - não obstante a ausência de quaisquer indícios concretos - o poder de vasculhar registros sigilosos alheios, em ordem a viabilizar, mediante a ilícita utilização do procedimento de devassa indiscriminada (que nem mesmo o Judiciário pode ordenar), o acesso a dado

> supostamente impregnado de relevo jurídico-probatório, em função dos elementos informativos que viessem a ser eventualmente descobertos. A FUNDAMENTAÇÃO DA QUEBRA DE SIGILO HÁ DE SER CONTEMPORÂNEA À PRÓPRIA DELIBERAÇÃO LEGISLATIVA QUE A DECRETA. - A exigência de motivação - que há de ser contemporânea ao ato da Comissão Parlamentar de Inquérito que ordena a quebra de sigilo - qualifica-se como pressuposto de validade jurídica da própria deliberação emanada desse órgão de investigação legislativa, não podendo ser por este suprida, em momento ulterior, quando da prestação de informações em sede mandamental. Precedentes. (MS 23851, Relator(a): CELSO DE MELLO, Tribunal Pleno, julgado em 26/09/2001, DJ 21-06-2002 PP-00098 EMENT VOL-02074-02 PP-00308)

Como se vê, a quebra de sigilo operacionalizada pela Comissão Parlamentar de Inquérito deve fundamentar-se em (a) causa provável, (b) adequada ao suporte fático até então coligido, cuja ocorrência deve ser contemporânea à (c) deliberação parlamentar.

Esses pressupostos constituem *standards* importantes para que se avalie, no âmbito jurisdicional, com coerência e respeitada a atuação do ente parlamentar, a relevância e a atualidade da quebra do sigilo que justifiquem a sua prevalência, na situação concreta, sobre os direitos à intimidade e à privacidade.

Evidentemente, a autoridade judiciária, ao exercer o controle constitucional da atuação do Poder Legislativo e de suas Comissões, deve considerar as peculiaridades do sistema de deliberação parlamentar, cujos contornos não se identificam com o processo de tomada de decisão judicial.

Isso significa que, embora os parlamentares estejam vinculados ao dever de fundamentação constitucional, é natural que as razões expostas para o afastamento não sejam apresentadas de forma exaustiva, até porque a dinâmica de deliberação parlamentar dificulta, em Colegiado amplo, a apresentação linear e inteiriça de argumentos e motivos.

Nessa linha, ao apreciar a medida cautelar no Mandado de

Segurança 23575, o eminente Ministro Nelson Jobim descortinou com precisão o ambiente decisório de Comissão Parlamentar:

> Por outro lado, sem razão as Informações quando refere a questão da fundamentação da decisão que tenha determinado medida acautelatória (fls. 69). Uma coisa é o fundamento político ou jurídico de uma decisão. Outra, é não ter fundamento algum. O que se exige é a fundamentação de uma decisão. O que não se permite, é a decisão arbitrária, porque sem fundamentação. No mesmo MS 23446-6 fiz distinção entre o processo decisório judicial e o processo decisório das Casas Políticas. Disse não se poder "... fazer uma paridade entre o processo decisório judicial e o processo decisório político no que diz respeito à fundamentação de suas decisões. ... Não se pode pretender ... que a fundamentação da decisão do parlamento tenha a mesma contextura, a mesma forma ou a mesma densidade das decisões do Poder Judiciário. ... o procedimento pelo qual agem os parlamentares é absolutamente distinto do procedimento judicial. ...". A fundamentação da decisão política se encontra em qualquer peça ou momento do procedimento. Pode se encontrar no próprio projeto, no requerimento, na indicação, no parecer e na emenda - que são os tipos de proposições parlamentares -. Pode decorrer do debate quando da votação da matéria. O certo é que as decisões parlamentares não estão sujeitas às regras que disciplinam as decisões judiciais que impõem relatório, fundamentos e dispositivo (CPC, art. 458). O procedimento parlamentar é outro. O procedimento de tomada de decisões é outro. Logo, não se lhe aplica as regras de processo judicial, que é diverso. No entanto, não se conclua que a decisão parlamentar possa ser arbitrária e sem nenhum fundamento. Não se confunda inexistência de fundamentação com topologia da fundamentação. Para as decisões judiciais, a lei impõe uma topologia própria e específica para os seus fundamentos. Não é o caso da decisões parlamentares. A localização dos fundamentos pode e é difuso. Os fundamentos podem se

> encontrar em diversos locus do processo decisório. (Decisão publicada no DJ de 01/02/2000).

Essas peculiaridades, inclusive, já foram consideradas pelo Plenário deste Tribunal no exame do Mandado de Segurança 24749, de relatoria do eminente Ministro Marco Aurélio (julgado em 29/09/2004, DJ 05-11-2004 PP-00019 EMENT VOL-02171-01 PP-00142 RTJ VOL-00196-01 PP-00186 LEXSTF v. 26, n. 312, 2005, p. 166-170), bem como no Mandado de Segurança 25668, de relatoria do eminente Ministro Celso de Mello (julgado em 23/03/2006, DJ 04-08-2006 PP-00027 EMENT VOL-02240-03 PP-00410 RTJ VOL-00200-02 PP-00778 RCJ v. 20, n. 129, 2006, p. 55-66).

Nesse contexto delineado pelos precedentes desta Corte, a fundamentação apresentada pela Comissão Parlamentar de Inquérito para aprovação dos Requerimentos nº 1362/2021 e 1364/2021, mostra-se suficiente, considerados os elementos coligidos neste momento preambular.

Colho do ato coator os seguintes trechos:

> A empresa Brasil Paralelo Entretenimento e Educação S/A é suspeita de integrar uma rede de mídias responsáveis por atentar contra a ciência, a saúde pública e a vida no contexto da pandemia de Covid-19 em razão da disseminação de fake news. A disseminação massiva de conteúdos contrários às medidas não farmacológicas adotadas no combate à pandemia, como o distanciamento social e o lockdown, pode ter contribuído sobremaneira para aumentar a mortalidade derivada da pandemia no Brasil.
>
> A Brasil Paralelo se apresenta como uma empresa de entretenimento e educação que produz séries, documentários e filmes gratuitos: "A missão da Brasil Paralelo é resgatar os bons valores, ideias e sentimentos no coração de todos os brasileiros, e o entretenimento é uma das principais ferramentas para esse resgate. Nossa orientação é sempre a verdade histórica, ancorada na realidade dos fatos e somos contrários à ideologização em produção de conteúdo"

(https://conteudo.brasilparalelo.com.br/quemsomos/). No documentário intitulado "7 DENÚNCIAS: AS CONSEQUÊNCIAS DO CASO COVID-19", produzido pela Brasil Paralelo e disponível em seu canal no YouTube – uma das fontes de receita da empresa é a monetização de vídeos no YouTube –, que já obteve mais de um milhão de visualizações somente na referida plataforma, as medidas restritivas adotadas por entes governamentais no enfrentamento à pandemia de Covid-19 são atacadas como medidas políticas, não científicas, autoritárias, que violentam as liberdades individuais e produzem desemprego e miséria.

Apesar de haver um aviso no início do documentário, ressaltando que a peça não é contra os métodos de prevenção à Covid-19, trata-se de uma obra cinematográfica, de elevado custo de produção, que conspira contra medidas verdadeiramente efetivas no combate à pandemia quando não se tem vacina para imunizar a população.

O documentário "7 DENÚNCIAS: AS CONSEQUÊNCIAS DO CASO COVID19" foi publicado no YouTube em junho de 2020. Em um fragmento da obra, o narrador verbaliza:

"O pânico social, o alarde midiático e o imanente risco à vida faz com que o povo aumente a aceitação do que o governante pode ou não fazer. É o momento onde a procuração estatal para agir em nosso nome tende a aumentar para enfrentarmos o desafio. Mas quando, por alegarmos defender as pessoas de um vírus, submetemos a sua liberdade e tiramos dela o direito ao trabalho e à tentativa de sustentar sua própria família, será que é correto dizer que estamos agindo em nome do bem comum? Quando, em troca de proteger as pessoas, as obrigamos a concordarem conosco, diminuindo a margem para agirem ou se manifestarem contra, será que a dignidade humana continua em cena? Ou se trata de uma outra maneira de governar a sociedade?" Fonte: https://youtu.be/-ugqbyDCamw

Em outro momento do documentário, Ricardo Gomes, apresentado como advogado e professor, ressalta:

"Essas decisões que estão sendo tomadas, de isolamento, de quarentena, de lockdown, são decisões profundamente políticas, não são decisões científicas. São escolhas tomadas por gestores públicos levando em consideração a opinião pública, levando em consideração as ferramentas que eles têm pra tomar decisão, os recursos que eles têm disponíveis. São decisões de política pública, não são decisões científicas. Aliás, nenhum cientista toma uma decisão global. A ciência encontra um conhecimento pra ser aplicada pelos tomadores de decisão. E a ciência tá dizendo: nós não temos o conhecimento." Fonte: https://youtu.be/-ugqbyDCamw

O tom negacionista, contrário à ciência, do documentário é reforçado por um artigo escrito e publicado pela Redação do site da Brasil Paralelo em 10 de março de 2021, intitulado "Quais são as consequências sociais do coronavírus?". No referido artigo, toda a semântica do documentário é resgatada e as medidas de distanciamento social adotadas no combate à disseminação do coronavírus voltam a ser direta ou indiretamente atacadas:

"Atualmente, uma das maiores consequências do coronavírus tem sido o sacrifício da economia. Muito se ouviu falar que as vidas são mais importantes do que a economia e que é necessário salvá-las e, só então, preocupar-se com valores econômicos. Tal ideia é contraditória, se, por exemplo, uma pequena empresa começa a enfrentar problemas financeiros, entre 22 e 28 dias sem vender, quando 75% dos empregos são gerados, no Brasil, por pequenos empreendedores. Em todos estes meses, com as consequências do coronavírus, o déficit sobre o PIB poderá ser o maior da história. A dívida pública atingirá níveis preocupantes. No início de tudo, nas primeiras 9 semanas daquilo que se chamou de pandemia, os Estados Unidos registraram 38 milhões de desempregados. Milhares de lojistas se viram sem condições de pagar os aluguéis. No Brasil, o Sebrae registrou a quebra de 600 mil empresas nas primeiras semanas e 9 milhões de desempregados.

A própria ONU afirmou que o número de pessoas que

> passam fome pode dobrar em função da crise do coronavírus. Aproximadamente 265 milhões serão atingidas. Segundo a Lancet Global Health, uma das mais famosas revistas científicas de medicina, cada ponto de desemprego no Brasil está associado a mais de 30 mil novas mortes todos os anos." Fonte: https://conteudo.brasilparalelo.com.br/politica/consequenciassociais-do-coronavirus/
>
> Faz-se importante destacar que o modus operandi da empresa Brasil Paralelo se diferencia daquele adotado por outras empresas e veículos de mídia que são alvos da investigação conduzida por esta Comissão Parlamentar de Inquérito, uma vez que o referido documentário é muito mais sofisticado e demanda muito mais investimento do que mensagens de texto propagadas em redes sociais.
>
> (...)
>
> A disseminação massiva de conteúdos contrários às medidas de distanciamento social pode ter contribuído sobremaneira para agravar a pandemia e a mortalidade derivada da pandemia no Brasil. Faz-se urgente e necessário, portanto, analisar os sigilos da empresa Brasil Paralelo Entretenimento e Educação S/A, de modo que a responsabilidade por milhares de mortes evitáveis seja devidamente apurada por esta Comissão Parlamentar de Inquérito.
>
> A análise dos sigilos requeridos será fundamental para verificar se a investigada foi financiada para disseminar os conteúdos mencionados ou se realizou operações financeiras suspeitas, bem como para verificar se a investigada integra alguma espécie de organização envolvendo agentes públicos e/ou empresários, responsável pela disseminação de Fake News relativas à pandemia. O período delimitado, de 2019 até o presente, permitirá uma análise comparativa entre o período anterior à pandemia e o período pandêmico.

Como se vê, há linha investigativa da Comissão Parlamentar de Inquérito que identificou correlação entre as ações do Governo Federal no

enfrentamento da pandemia e a disseminação de notícias falsas por pessoas físicas e veículos de comunicação durante o período.

E, nesse âmbito de atuação, relacionado ao fato determinado objeto da Comissão Parlamentar de Inquérito, surge pertinente o afastamento do sigilo de pessoas ou entidades potencialmente envolvidas na disseminação de notícias falsas no que tange à pandemia.

Contudo, o alcance material e temporal da quebra de sigilo deve ser objeto de ponderação cautelosa, consideradas as garantias constitucionais em jogo. Por essa razão, entendo oportuno examinar com maior verticalidade as determinações de afastamento dos sigilos telefônico e telemático.

2 – Afastamento dos sigilos telefônico e telemático

Colhe-se do Requerimento (eDOC 11) que a CPI determinou a transferência dos seguintes dados protegidos por sigilo, da empresa Brasil Paralelo Entretenimento e Educação S/A:

> a) **telefônico,** de 1º de janeiro de 2019 até o presente, incluindo-se todos os terminais cadastrados em nome da Brasil Paralelo Entretenimento e Educação S/A; IMEI, serial ou ID dos respectivos aparelhos telefônicos; dados cadastrais e de pagamento dos serviços; histórico de chamadas efetuadas / recebidas, acompanhadas da localização geográfica ERBs, e a duração das ligações telefônicas originadas e recebidas (remetente e destinatário); dados, inclusive o **conteúdo, relativos a mensagens SMS, MMS, WAP e WEB**; a completa identificação dos interlocutores (remetente e destinatário), oficiando-se as operadoras de telefonia Oi, Claro, Vivo, Tim, Nextel, Algar, Surf Telecom e demais em operação no país;
>
> (...)
>
> d.1) **telemático,** de 1º de janeiro de 2019 até o presente, oficiando-se a empresa Google Brasil Internet Ltda. (Endereço: Avenida Brigadeiro Faria Lima, 3477, 18º andar, CEP 04538- 133, São Paulo/SP), para que forneça: ● Dados cadastrais; ●

Registros de conexão (IPs, com data, hora, fuso e porta lógica), Informações de Android (IMEI), Cópia integral de todo conteúdo armazenado no Google Drive, incluindo o backup do WhatsApp; ● C**ópia integral de todo conteúdo armazenado no Google Fotos, com os respectivos metadados (EXIF)**; ● Lista de contatos vinculados as contas mencionadas, com números de telefones e nomes; ● **Cópia integral de todas as mensagens (Gmail) enviadas/recebidas/armazenadas (rascunhos e lixeira), com seus anexos, em formato originalmente salvo pelo usuário, preservando a estrutura de diretórios criada pelo mesmo**; ● **Cópia integral de todas as mensagens enviadas, recebidas e armazenadas, conteúdos multimídias (fotos, vídeos, áudios) e qualquer outro anexo compartilhado através do sistema de troca de mensagens instantâneas Hangout; ● Localizações pretéritas e atuais do uso da(s) conta(s) (Location History), incluindo localizações geográficas específicas, por meio de GPS, Bluetooth ou sinal Wi-Fi**; ● Relação dos locais salvos no GOOGLE MAPS e demais dados armazenados no aplicativo; ● Os históricos de pesquisas realizadas pelo usuário do dispositivo, incluindo pesquisas no Google Maps; ● Informações de pagamento, incluindo dados dos cartões de crédito (operadoras); ● Listagem das redes WI-FI acessadas pelas contas indicadas; ● Informações dos aplicativos baixados e instalados no Google Play;

d.2) **telemático, de 1º de janeiro de 2019 até o presente, oficiando-se empresa WhatsApp Inc.**, para que forneça: ● "User Info, IP Addresses, Sym Address Book, Account Notes, Full Group Memberships e Profile Picture" (dados cadastrais da conta, informações do aparelho, versão da APP, data e horário do registro, status de conexão, última conexão com data, hora e porta lógica, endereço de email, informações de cliente Web; ● registros de acessos IPs desde 2020 e IP da última conexão; ● histórico de mudança de números; ● perfil do usuário com foto; about - antigo "status"; ● Nomes dos grupos, seus administradores, integrantes dos grupos com seus respectivos números de telefones e fotos - lista de grupos; e ● agenda de

> contatos simétricos e assimétricos).
>
> d.3) **telemático,** de 1º de janeiro de 2019 até o presente, oficiando-se empresa Facebook para que forneça, a respeito das plataformas Facebook, Instagram e Facebook Messenger, todo o conteúdo relativo às contas de titularidade do investigado, em especial **mensagens privadas**, participação em grupos fechados, comentários e postagens, lista de amigos e toda atividade nelas realizada.
>
> d.4) telemático, de 1º de janeiro de 2019 até o presente, oficiando-se a empresa Apple Computer Brasil Ltda, por meio da Privacy & Law Enforcement Compliance (e-mail lawenforcement@apple.com) para que forneça todo o conteúdo relativo às contas e aparelhos de titularidade do investigado, especialmente **dados de localização, GPS, Bluetooth, endereço IP, localização de pontos de acesso Wi-Fi e torres de celular e outras tecnologias para determinar a localização aproximada de seu dispositivo**, bem como o **conteúdo armazenado no iCloud**.
>
> d.5) telemático, de 1º de janeiro de 2019 até o presente, oficiando-se à empresa Legalnotices@telegam.com, administradora da rede social **"Telegram",** que seja decretado o afastamento telemático de, devendo ser informado, no mínimo: a) logs de arquivos enviados e recebidos; b) dados de pagamentos; c) **preservação das conversas dos que participa (sic)**; d) dados cadastrais; e) dados de acesso; f) contatos; g) grupos que participa; h) conversas armazenadas; i) telefone e dados da localização, desde a data de sua criação até os dias atuais. (grifos nossos)

No caso em tela, a partir da leitura do Requerimento, depreende-se que o afastamento do sigilo telemático determinado determinado é bastante amplo e abrange não apenas simples registros de comunicações telefônicas, mas também **registros de conexão à internet, conteúdos de conversas, registros de atividades, dados de localizações atuais e pretéritas, dados multimídias (fotos, vídeos, áudios) e outros**.

De início, considero que os referidos registros de conexão, dados de

acesso e conteúdos de comunicações privadas são claramente albergados por proteção constitucional, seja essa proteção entendida a partir da cláusula de inviolabilidade do sigilo das comunicações (art. 5º, inciso XII, da Constituição Federal), seja tal proteção entendida, de forma mais ampla e consentânea com a evolução jurisprudencial, a partir da cláusula geral de proteção à intimidade (art. 5º, inciso X).

Se em uma perspectiva mais tradicional da compreensão do direito à privacidade, a doutrina e a jurisprudência entendiam que a proteção constitucional expressa no art. 5º, inciso XII não abrangia o conteúdo dos dados pessoais e dizia respeito tão somente ao fluxo de informações em meios comunicacionais (RE 418.416, Relator Min. SEPÚLVEDA PERTENCE, Tribunal Pleno, julgado em 10.5.2006, DJ 19.12.2006 PP-00037 EMENT VOL-02261-06 PP-01233), não há dúvidas de que esse entendimento foi superado a partir de decisões do Supremo Tribunal Federal que alargaram o âmbito de proteção do art. 5º, incisos X e XII, para afirmar a autonomia do um direito fundamental à proteção de dados (RE 673.707, Rel. Min. Luiz Fux, Tribunal Pleno, julgado em 17.6.2015, DJe 30.9.2015).

Mais recentemente, no julgamento da paradigmática ADI 6389 MC, o STF conferiu autonomia a esse direito fundamental, sagrando que a proteção constitucional envolve, em uma perspectiva subjetiva, a proteção do indivíduo contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais e, em uma perspectiva objetiva, a atribuição ao indivíduo da garantia de controlar o fluxo de seus dados. O acórdão restou assim ementado:

> MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO

> MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. 1. Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais. 2. Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, **o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos**. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados. (ADI 6387 MC-Ref, Relator(a): ROSA WEBER, Tribunal Pleno, julgado em 07/05/2020, PROCESSO ELETRÔNICO DJe-270 DIVULG 11-11-2020 PUBLIC 12-11-2020)

No caso em tela, portanto, tenho clareza de que os dados pessoais que são objeto do Requerimento formulado pela CPI são inequivocamente protegidos pelo direito fundamental à privacidade (art. 5º, inciso X, da CF).

A partir dessa premissa, há dois questionamentos relevantes para a compreensão da controvérsia. Em primeiro lugar, existe fundamento legal que obrigue empresas como Google, WhatsApp, Facebook e Apple a fornecerem acesso aos registros de conexão à internet e ao conteúdo das comunicações? Em segundo lugar, nessa hipótese específica, a Comissão Parlamentar de Inquérito deteria poderes investigativos suficientes para afastar o sigilo constitucional que recai sobre esses dados?

Conforme será discutido a seguir, esses dois questionamentos suscitam divergências importantes no âmbito doutrinário e estão sob a

luz de uma jurisprudência ainda em desenvolvimento acerca do alcance das garantias constitucionais individuais no contexto de investigações criminais baseadas em dados.

2.1 – Fundamentação legal do dever de disponibilização de dados pessoais armazenados por aplicações de internet

Como mencionado acima, uma vez que os dados de registros e de comunicações pessoais indubitavelmente são albergados pelo direito fundamental à privacidade (art. 5º, incisos X e XII, da Constituição Federal), é importante perquirir se existe previsão legal que define sob quais circunstâncias esse sigilo constitucional pode ser afastado.

A rigor, a Lei de Interceptações Telefônicas (Lei nº 9.926/1996), aplica-se tão somente às empresas prestadoras de serviços de telecomunicações. Embora no dia a dia possamos ter a impressão de que algumas aplicações de internet como Facebook, WhatsApp e Telegram, assemelham-se a um prestador de serviço de telecomunicações, do ponto jurídico, essas empresas estão sujetias a um um enquadramento legal e regulatório totalmente distinto.

A Lei Geral de Telecomunicações brasileira reflete uma dicotomia entre os serviços de telecomunicações, definidos no art. 60 da LGT, e os chamados serviços de valor adicionado legalmente definidos como "*a atividade que acrescenta a um serviço de telecomunicações que lhe dá suporte e com o qual não se confunde novas utilidades relacionadas ao acesso, armazenamento, apresentação, movimentação ou recuperação de informações*".

Como destacado na doutrina, aplicações de internet como Skype, WhatsApp, Youtube, Netflix, etc., conhecidas na literatura como Serviços Over-The-Top (OTT) são enquadrados no direito brasileiro dentro da categoria de Serviços de Valor Adicionado. Nessa lógica, "*os serviços OTT, redutíveis ao conceito de SVA constituem uma categoria que abrange todo e qualquer conteúdo, aplicativo e serviço que seja acessado por usuários finais por meio da internet e que sejam prestados por um agente de mercado que não detém o controle da respectiva rede de telecomunicações*". (FERNANDES, Victor

Oliveira. **Regulação de Serviços de Internet: desafios da regulação de aplicações Over-The-Top (OTT)**, Rio de Janeiro: Lumen Juris, 2018, p. 154 e 161).

A consequência dessa diferenciação é que as aplicações de internet constituem meros usuários dos serviços de telecomunicações, estando, portanto, fora do âmbito de incidência da LGT e da própria Lei de Interceptações Telefônicas (Lei nº 9.926/1996), cujo art. 7º, *caput*, estabelece que, para que a interceptação seja realizada, a autoridade policial poderá "*requisitar serviços e técnicos especializados às* ***concessionárias de serviço público***".

Não existindo dever de fornecimento dos dados acima mencionados no regime da Lei de Interceptação telefônica, seria possível cogitar ainda da aplicação da Lei 12.965/2014, o Marco Civil da Internet. Para os fins dessa lei, serviços OTT como o WhatsApp, Facebook e Google são considerados aplicações de internet (art. 5º, inciso VII).

Nesse diploma, o regime de proteção aos registros, aos dados pessoais e às comunicações privadas é disciplinado nos arts. 10 a 12, cujo teor transcrevo abaixo:

> 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.

A partir de uma interpretação sistemática desses dispositivos, percebe-se que os arts. 10 e 11 prescrevem obrigações aos provedores de conexão e de aplicações que estão relacionadas tanto ao regime de guarda e tratamento quanto ao regime de disponibilização dos dados.

O caráter atécnico da redação dos dispositivos legais sem dúvida dificulta a interpretação legal. Todavia, bem examinados, depreende-se que o único dispositivo que impõe alguma obrigação de ***disponibilização*** dos dados é o art. 10, já que o art. 11 refere-se tão somente às operações de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações.

O art. 10 entabula um dever de disponibilização dos registros de conexão e de acesso a aplicações de interne, bem como de dados pessoais e do conteúdo de comunicações privadas. Todavia, fica claro da leitura da lei que tanto o escopo do dever de disponibilização quanto as condicionantes dessa disponibilização assumem limites e critérios

diferenciados quando se trata de registros de conexão e de acesso *vis a vis* os conteúdos das comunicações privadas em si.

Os registros de conexão à internet equivalem, na forma da lei, simplesmente ao "*conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados*" (art. 5º, inciso VI). Trata-se, portanto, dos chamados **metadados,** os quais podem ser tecnicamente acessados por empresas de aplicativos sem que seja necessário violar o padrão de criptografia ponta-a-ponta. Esses dados, no entanto, não revelam qualquer elemento do conteúdo da comunicação.

Para esse subconjunto, registros de conexão, o dever de guarda e disponibilização imposto pelo Marco Civil da Internet é **autoaplicável**. Isso porque a lei deixa claro no art. 10, § 1º, que 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*". Assim, satisfeita a condição sagrada no dispositivo, qual seja, "ordem judicial", é inafastável o dever de **disponibilização** dos registros de conexão à autoridade.

Já o § 2º do art. 10, por sua vez, trata do conteúdo das comunicações privadas. Ocorre que esse parágrafo, diferente do anterior, não é autoaplicável, mas claramente carece de regulamentação. Depreende-se da sua redação que "*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*". Ao prever que o conteúdo poderá (e não deverá) ser disponibilizado, o Marco Civil da Internet remete o dispositivo a uma eventual regulamentação futura ("*que a lei estabelecer*").

O objetivo dessa regulamentação seria justamente o de estabelecer um regime seguro de interceptação que preservasse a inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, como se consagra no art. 7º, inciso II. Contudo, como já

destacamos, a Lei de Interceptações telefônicas não é aplicável para o tratamento dos conteúdos de comunicações privadas no âmbito de aplicações de internet.

A interpretação do Marco Civil da Internet aqui desenvolvida encontra amparo extenso na doutrina. Como bem destacado por **Jaqueline Souza de Abreu** ao tratar do tema:

> "O Marco Civil da Internet não institui, explicitamente, a obrigação de que aplicações de internet tenham habilidade de quebrar sigilo. Quando obriga que empresas retenham informações, o dever se estende apenas a registros (IP, data e hora de acesso), o que as obriga a, necessariamente, ser capazes de atender a pedidos de quebra de sigilo apenas desses metadados (art. 15). Portanto, o dever jurídico, extraído do direito brasileiro vigente, de que aplicações de internet sejam capazes de quebrar sigilo de conteúdo de comunicações não é evidente; carece de fundamentação — e pode muito bem ser que a conclusão seja de que não exista" (ABREU, Jacqueline de Souza. **Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação.** Revista Brasileira de Políticas Públicas, vol. 7, n. 3, 2017, p. 34).

Destaca-se ainda que se encontra pendente de julgamento neste STF a ADPF 403 e a ADI 5.527, ações em que se discute, em última análise, se o poder judiciário determinar a suspensão dos serviços de mensagens pela internet, como o aplicativo WhatsApp, pelo suposto descumprimento de ordens judiciais que determinem a quebra de sigilo das comunicações. Em seu voto-relator na ADPF 403, o Min. Edson Fachin concluiu que "*não há como obrigar que as aplicações de internet que ofereçam criptografia ponta-a-ponta quebrem o sigilo do conteúdo de comunicações, ao menos à luz das informações que traduzem o consenso científico atual sobre a matéria*" (ADPF 403, rel. Min. Edson Fachin). O julgamento dessas ações foi suspenso por pedido de vista em 28/05/2020.

Assim, podemos afirmar que, pelo menos no âmbito do Marco Civil da Internet, é discutível, ao menos em tese, se os provedores de aplicações

podem ou não ser obrigados, e sob em que circunstâncias, a disponibilizarem o acesso a dados pessoais e ao conteúdo de comunicações privadas armazenadas.

Destaca-se, ainda, que essa discussão sobre o art. 10, § 2º, do MCI não se confunde com o debate sobre a necessidade de autorização judicial para acesso a registros e informações contidos em aparelho de telefone celular apreendido pela autoridade policial ou em posse da vítima, qual discutido no julgamento do ARE 1.042.075, rel. Min. Dias Toffoli, pendente de julgamento (Tema 977 da Repercussão Geral).

Inexistindo resposta clara no Marco Civil da Internet, poder-se-ia cogitar ainda do endereçamento da questão no regime da Lei Geral de Proteção de Dados.

A despeito do claro avanço obtido com a sua promulgação, a Lei 13.709/2018 previu, no seu art. 4º, inciso III, que as suas disposições não seriam aplicáveis aos tratamentos de dados pessoais realizados para fins exclusivos de "segurança pública", "defesa nacional", "segurança do estado" ou "atividades de investigação e repressão de infrações penais".

Além disso, a LGPD expressamente consignou um dever ao legislador ordinário de editar legislação específica para o tratamento de dados pessoais nessas hipóteses. Destaca-se o teor do § 1º do art. 4º:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
>
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) **atividades de investigação e repressão de infrações penais**; ou
>
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do

titular previstos nesta Lei.

O motivo de a LGPD se escusar a reger essas formas de tratamento de dados pelo Poder Público tem relação não apenas com as mencionadas particularidades do tratamento de dados pessoais pelo Poder Público, mas principalmente com o contexto de edição da norma.

É que, do ponto de vista da sua própria estrutura, a LGPD foi bastante influenciada pela positivamente das normas de proteção de dados no Direito Europeu, em especial pelo chamado Regulamento Geral de Proteção de Dados, o GDPR, e pela Diretiva que o antecedia. O artigo 2º do GDPR (Regulamento EU 2016/679), de forma semelhante, excepciona da sua aplicação o tratamento de dados pessoas "efetuado pelas autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública".

Ocorre que, no contexto Europeu, antes mesmo de a GDPR ser sancionada, exarou-se a Diretiva EU 2016/680 do Parlamento Europeu e do Conselho de 26 de abril de 2016, que dispõe justamente sobre o regramento aplicável às operações de tratamento de dados para fins de persecução penal. Essa última diretiva estabelece, por exemplo, um conjunto de princípios relativos a essas modalidades de tratamento voltado à proteção dos direitos e das liberdades fundamentais das pessoas investigadas.

Esse é um exemplo paradigmático de como podem ser fixadas balizas normativas para o tratamento de dados pessoais para fins de investigação criminal.

De todo modo, a discussão candente no nosso ordenamento jurídico é justamente o que deve ser feito diante dessa lacuna normativa intencionalmente deixada pelo Marco Civil da Internet e pela LGPD.

Destaque-se que essa vertente específica do acesso a dados e comunicações pessoais para fins de segurança pública e investigação criminal foi objeto de projeto de lei recentemente apresentado ao Congresso Nacional, no qual são traduzidas as preocupações e as

garantias acima descritas (**Anteprojeto de lei disciplina proteção de dados em investigações criminais.** Portal Jurídico Conjur. 31.10.2020. Disponível em: https://www.conjur.com.br/2020-out-31/anteprojeto-disciplina-protecao-dados-investigacoes-criminais).

Apelidado de Anteprojeto de Lei Geral de Proteção de Dados para fins Penais (Anteprojeto de LGPD Penal), o referido projeto destaca, já em seu art. 2º, que a proteção de dados no âmbito da segurança pública objetiva proteger a dignidade da pessoa humana, a intimidade e a vida privada dos cidadãos, bem como a garantia "devido processo legal, da ampla defesa, do contraditório, da **motivação** e da reserva legal" (**Anteprojeto de lei disciplina proteção de dados em investigações criminais.** Portal Jurídico Conjur. 31.10.2020. Disponível em: https://www.conjur.com.br/2020-out-31/anteprojeto-disciplina-protecao-dados-investigacoes-criminais).

No que se refere à definição de dados pessoais sigilosos, o referido projeto densifica esse conceito para esclarecer que ele se aplica a operações financeiras, **registros e conteúdo de comunicações privadas e geolocalização** (art. 5º, III, do anteprojeto de lei), dados que integram o Requerimento da CPI impugnado neste mandado de segurança.

Destarte, embora o referido projeto de lei ainda não tenha sido objeto de deliberação e aprovação pelo Congresso, de modo que não há de se falar em norma vigente e vinculativa, não se pode deixar de considerar que referida proposta traz relevantes diretrizes interpretativas, em especial se considerarmos que a proposta foi formulada com base no trabalho de um conjunto de especialista sobre o tema.

Pois bem. Diante de todas essas considerações, verifico que é discutível, ao menos em tese, a extensão do dever jurídico de provedores de aplicações de disponibilizarem o acesso a registros de conexão, dados de comunicação e conteúdos de comunicações privadas dos seus usuários.

Ainda que entendamos que as aplicações de internet podem ser compelidas a conceder o acesso a esses dados para fins de instrução criminal quando houver ordem judicial expressa, remanesceria ainda a

questão de saber se as Comissões Parlamentares de Inquérito também deteriam o poder investigativo de ordenar essa disponibilização.

2.2 – Poderes investigativos das CPI e acesso a registros de conexão, dados pessoais e comunicações privadas armazenados pelas aplicações de internet

No caso em tela, mesmo que consideremos que há obrigação legal de disponibilização dos conteúdos das comunicações por ordem judicial, essa obrigação poderia ser imposta por ato de Comissão Parlamentar de Inquérito, no contexto dos seus poderes investigativos próprios de autoridades judiciais?

Ao meu ver, o estado atual do debate não nos permite dar uma resposta definitiva. É que a tradicional jurisprudência do STF assenta que, embora as Comissões Parlamentares de Inquérito detenham poderes investigativos para afastar o sigilo telefônico, tais poderes não são absolutos e, em alguma medida, são até mais restritos do que aquele detido pela autoridade judicial.

Nesse sentido, há diversas decisões da Corte que ressaltam que as CPI não podem determinar a interceptação de comunicações telefônicas em si. Destaco, a esse respeito, os seguintes precedentes:

> COMISSÃO PARLAMENTAR DE INQUÉRITO - PODERES DE INVESTIGAÇÃO (CF, ART. 58, § 3º) - LIMITAÇÕES CONSTITUCIONAIS - LEGITIMIDADE DO CONTROLE JURISDICIONAL - POSSIBILIDADE DE A CPI ORDENAR, POR AUTORIDADE PRÓPRIA, A QUEBRA DOS SIGILOS BANCÁRIO, FISCAL E TELEFÔNICO - NECESSIDADE DE FUNDAMENTAÇÃO DO ATO DELIBERATIVO - QUEBRA DE SIGILO ADEQUADAMENTE FUNDAMENTADA - VALIDADE - MANDADO DE SEGURANÇA INDEFERIDO. A QUEBRA DO SIGILO CONSTITUI PODER INERENTE À COMPETÊNCIA INVESTIGATÓRIA DAS COMISSÕES PARLAMENTARES DE INQUÉRITO. (...) - O sigilo bancário, o sigilo fiscal e o sigilo

> telefônico (sigilo este que incide sobre os dados/registros telefônicos e que não se identifica com a inviolabilidade das comunicações telefônicas) (MS 24817, Relator(a): CELSO DE MELLO, Tribunal Pleno, julgado em 03/02/2005, DJe-208 DIVULG 05-11-2009 PUBLIC 06-11-2009 EMENT VOL-02381-03 PP-00571).

No mesmo sentido, citem-se ainda os seguintes julgados: MS 234512, Rel. Min. CELSO DE MELLO, Tribunal Pleno, julgado em 16/09/1992, DJ 12-05-2000 e HC 75232, Rel. Min. Carlos Velloso, Redator p/ Acórdão: Maurício Corrêa, Tribunal Pleno, Julgado em 07/05/1997, DJ 24-08-2001.

O entendimento de que as CPIs não podem ter acesso ao conteúdo de comunicações telefônicas decorre de uma interpretação restritiva do art. 5º, inciso XII, do texto constitucional, o qual somente autoriza o excepcional afastamento do sigilo das comunicações "*por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de* ***investigação criminal*** *ou* ***instrução processual penal***".

Fora dessas duas finalidades expressas, que se referem tão somente a procedimentos investigatórios conduzidos por autoridade judiciária, o texto constitucional preserva o sigilo do conteúdo das comunicações. Tal entendimento encontra também assento na doutrina:

> O inciso XII do art. 5° somente contempla a hipótese excepcional de violação das comunicações telefônicas "para fins de investigação criminal ou instrução processual penal", **o que não valeria para uma investigação conduzida por comissão parlamentar de inquérito**. (BARROSO, Luís Roberto. Comissões Parlamentares de Inquérito e suas Competências: Política, Direito e Devido Processo Legal. Revista Jurídica Virtual - Brasília, vol. 2, n. 15, ago. 2000, p. 11).

Nesse ponto, portanto, só seria possível afirmar que a CPI detém legitimidade para requisitar os dados de comunicações de aplicações de internet se se entendesse que referidos dados não restariam protegidos pelo direito constitucional ao sigilo encartado no art. 5º, inciso XII, da

Constituição Federal.

Ante à impossibilidade de as CPIs afastarem o direito constitucional ao sigilo que recai sobre as comunicações telefônicas, **somente uma interpretação jurídica estagnada no tempo poderia chegar à conclusão de que essas comissões poderiam legitimamente ter acesso ao conteúdo de conversas privadas armazenadas em aplicativos de internet**.

De fato, a ausência de parâmetros objetivos e consentâneos com o contexto tecnológico vigente fragiliza a proteção de direitos fundamentais relacionados à comunicação social, inclusive, para abordar um aspecto do caso concreto, o sigilo da fonte, assegurado pelo inciso XIV do art. 5º da Constituição Federal.

Assim, entendo que o momento é adequado para que o Plenário do Supremo Tribunal Federal lance balizas sólidas e homogêneas para o controle dos atos praticados pelas comissões parlamentares de inquérito, de modo que parlamentares e sociedade vislumbrem com transparência a seara relevante da fiscalização operacionalizada pelo Poder Legislativo.

Mostra-se necessário harmonizar as premissas do debate constitucional, sob pena de as Comissões Parlamentares de Inquérito alcançarem poderes que extrapolam os limites impostos pela reserva constitucional de jurisdição.

No caso em tela, ao menos em um juízo de cognição sumária, parece de fato que o eventual afastamento do sigilo dos dados referenciados no Requerimento teria o potencial de gerar uma exposição bastante alargada da intimidade das pessoas naturais que estão por trás da pessoa jurídica.

A partir dos dados colhidos, a CPI poderia acessar uma infinidade de conversas privadas, além de fotos, vídeos e áudios e dados de localizações geográficas, tudo "*desde a data de sua criação até os dias atuais*", como o próprio Requerimento sugere.

A falta de delimitação temporal e, principalmente, a ausência de explicações na justificativa do Requerimento sobre porque cada um desses dados seriam afinal relevantes para a apuração dos fatos investigados na CPI também parece fragilizar a legitimidade do Requerimento, que, em uma avaliação sumária, afigura-se

desproporcional.

Portanto, a fim de evitar iminente violação aos direitos fundamentais à privacidade e à intimidade, é imperiosa a suspensão do ato coator no que tange ao afastamento dos sigilos telefônico e telemático até o julgamento definitivo deste mandado de segurança pelo Plenário do Supremo Tribunal Federal, tudo nos termos do art. 22, parágrafo único, alínea "b", do Regimento Interno.

3 – Sigilo fiscal e bancário

Saliento que o afastamento dos sigilos bancário e fiscal, demonstrada a fundamentação adequada pela CPI, deve ser mantido. As reflexões aqui desdobradas não infirmam a conclusão consolidada na jurisprudência desta Corte acerca da possibilidade de comissões parlamentares de inquérito avançarem sobre os sigilos bancário e fiscal.

No entanto, sob o ângulo temporal, a quebra do sigilo não se apresenta constitucionalmente justificável.

Isso porque a CPI da Pandemia foi criada "com a finalidade de apurar, no prazo de 90 dias, as ações e omissões do Governo Federal no enfrentamento da Pandemia da Covid-19 no Brasil e, em especial, no agravamento da crise sanitária no Amazonas com a ausência de oxigênio para os pacientes internados; e as possíveis irregularidades em contratos, fraudes em licitações, superfaturamentos, desvio de recursos públicos, assinatura de contratos com empresas de fachada para prestação de serviços genéricos ou fictícios, entre outros ilícitos, se valendo para isso de recursos originados da União Federal, bem como outras ações ou omissões cometidas por administradores públicos federais, estaduais e municipais, no trato com a coisa pública, **durante a vigência da calamidade originada pela Pandemia do Coronavírus**".

Perceba que o fato determinado a ser investigado pela Comissão Parlamentar de Inquérito, nos termos do § 3º do art. 58 da Constituição Federal, foi claramente delimitado pela vigência da calamidade pública causada pela Pandemia de Covid-19, cujo reconhecimento formal pelo

Estado brasileiro deu-se com a publicação do Decreto Legislativo nº 6, publicado em 20 de março de 2020.

Assim, extrapola o fato investigado e carece de causa provável a ordem de afastamento do sigilo relativamente a informações anteriores a essa data, uma vez que, por decorrência lógica, não guardam qualquer relação com o estado de pandemia.

O argumento consistente na necessidade de angariar dados para comparação de períodos não convence. Se o objetivo da CPI da Pandemia é verificar a disseminação de fake news no período pandêmico e eventual existência de esquema financeiro a sustentá-la, a coleta de dados relativos à calamidade pública é suficiente para elucidação dos fatos.

A ressaltar essa óptica, o eminente Ministro Edson Fachin, ao apreciar a Medida Cautelar no Mandado de Segurança 38114, processo cujas balizas fáticas são similares à deste feito, assentou que "a extensão do período de quebra para alcançar informações "desde o início de 2018" extrapola o objeto da Comissão Parlamentar de Inquérito, instaurada especificamente para apurar "as ações e omissões do Governo Federal no enfrentamento da Pandemia da Covid-19 no Brasil". São, portanto, informações extemporâneas e, assim, impertinentes ao objeto da CPI, devendo ser o seu sigilo preservado" (decisão publicada no DJe de 04/08/2021).

Portanto, merece parcial acolhida o pedido liminar, para que o termo inicial da quebra dos sigilos bancário e fiscal determinada pela CPI da Pandemia, em relação à impetrante, seja o dia 20 de março de 2020.

Por fim, os dados obtidos com a quebra de sigilo deverão receber o tratamento prescrito pelo art. 144 do Regimento Interno do Senado Federal.

Ou seja, as informações levantadas devem permanecer sob a guarda do Presidente da Comissão, que somente poderá franquear o acesso do Colegiado aos documentos relacionados à apuração da Comissão e em reunião secreta.

4 – Dispositivo

Ante o exposto, defiro em parte o pedido liminar, com fundamento no artigo 7º, inciso III, da Lei 12016/2009, para:

> **(i)** suspender a eficácia da aprovação dos Requerimentos 1228/2021 (item 106), 1362/2021 e 1364/2021, no que concerne ao afastamento dos sigilos telefônico e telemático da impetrante, até o julgamento definitivo deste mandado de segurança pelo Plenário;
>
> **(ii)** restringir a quebra dos sigilos bancário e fiscal da impetrante ao período posterior a 20 de março de 2020; e
>
> **(iii)** determinar que os dados obtidos pela Comissão Parlamentar de Inquérito sejam mantidos sob a guarda do Presidente da Comissão e compartilhados com o Colegiado apenas em reunião secreta e quando pertinentes ao objeto da apuração.

Notifique-se a autoridade coatora acerca desta decisão.

Após, dê-se vista à Procuradoria-Geral da República.

Publique-se.
Brasília, 02 de setembro de 2021.

Ministro **Gilmar Mendes**
Relator
Documento assinado digitalmente