HABEAS CORPUS 222.141 PARANÁ

RELATOR	**: MIN. RICARDO LEWANDOWSKI**
PACTE.(S)	**:----------**
ADV.(A/S)	**:**DANIEL GERBER E OUTRO(A/S)
COATOR(A/S)(ES)	**:**SUPERIOR TRIBUNAL DE JUSTIÇA

Trata-se de *habeas corpus* com pedido de liminar impetrado em favor de ---------- contra acórdão proferido pela Sexta Turma do Superior Tribunal de Justiça – STJ, que denegou a ordem no HC 626.983/PR, em acórdão assim ementado:

> "*HABEAS CORPUS*. MARCO CIVIL DA INTERNET. LEI 12.965/2014. MINISTÉRIO PÚBLICO. PROVEDORES E PLATAFORMAS DOS REGISTROS DE CONEXÃO E REGISTROS DE ACESSO A APLICAÇÕES DE INTERNET. REQUERIMENTO CAUTELAR DE GUARDA DOS DADOS E CONTEÚDOS POR PERÍODO DETERMINADO ALÉM DO PRAZO LEGAL. LEGALIDADE. EFETIVO ACESSO DEPENDENTE DE ORDEM JUDICIAL. AUSÊNCIA DE NULIDADE. ADPF 403/SE E ADI 5527/DF. INEXISTÊNCIA DE PERTINÊNCIA TEMÁTICA. *HABEAS CORPUS* DENEGADO.
>
> 1. A paciente (e outros imputados) responde a processo criminal pela prática de crimes relativos a fatos ocorridos no DETRAN/PR, atinentes ao Edital de Credenciamento n. 001/2018, que regulamentou o credenciamento de empresas para a prestação de registro eletrônico de contratos, e sustenta a nulidade das provas carreadas aos autos, porquanto, além de obtidas mediante 'verdadeira medida cautelar' em detrimento do direito à intimidade/privacidade, houve o congelamento do conteúdo telemático junto aos provedores de internet, a pedido do Ministério Público, sem autorização judicial.
>
> 2. A Lei nº 12.965/2014 (Marco Civil da Internet) dispõe que 'a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet', nela tratados, '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. 10).

3. Mas ressalva que o provedor responsável pela guardaestá obrigado a disponibilizar os registros (de conexão e de acesso a aplicações da internet), mediante ordem judicial (art. 10, §§ 1º e 2º), com a finalidade de 'formar conjunto probatório em processo judicial cível ou criminal, em caráter incidental ou autônomo' (art. 22), a pedido da parte interessada, desde que haja 'indícios fundados da ocorrência do ilícito', 'justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória' e 'período ao qual se referem os registros' (art. 22, incisos I, II e III).

4. Os impetrantes, em verdade, não discutem o fornecimento dos registros por ordem judicial, senão a nulidade das provas carreadas aos autos, porquanto, além de obtidas mediante 'verdadeira medida cautelar' em detrimento do direito à intimidade/privacidade, houve o congelamento do conteúdo telemático junto aos provedores de internet sem autorização judicial, congelamento de conteúdo que, na tese da impetração, extrapola os limites da legislação de proteção geral de dados pessoais.

5. Trata-se de matéria que recebe tratamento específico da Lei 12.965/2014, ao dispor que constitui dever jurídico do administrador do respectivo sistema autônomo manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano (art. 13); e, do provedor de aplicações de internet, por sua vez, manter os registros de acesso, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses (art. 15).

6. Dispõe, ainda, que a autoridade policial, administrativa ou o Ministério Público poderão requerer cautelarmente que os registros de conexão sejam guardados por

prazo superior a 1 (um) ano (art. 13, § 2º), e os registros de acesso a aplicações de internet por prazo superior a 6 (seis) meses (art. 15, § 2º), devendo, nas duas situações, e no prazo de 60 (sessenta) dias, contados do requerimento administrativo, ingressar com o pedido de autorização judicial de acesso aos (dois) registros (arts. 13, § 3º, e 15, § 2º).

7. A lei dispõe que a autoridade policial, administrativa ouo Ministério Público poderão requerer cautelarmente — que os registros de conexão sejam guardados por prazo superior a 1 (um) ano (art. 13, § 2º), e os registros de acesso a aplicações de internet por prazo superior a 6 (seis) meses (art. 15, § 2º) —, parecendo dizer menos do que pretendia.

8. É que, quem requer alguma coisa, pura e simplesmente pode tê-la deferida ou não, e, no caso, até mesmo pelo uso do termo 'cautelarmente', seguido da previsão de pedido judicial de acesso no prazo de 60 (sessenta) dias, contados do requerimento administrativo, sob pena de caducidade, tem-se que o administrador de sistema autônomo e o provedor de aplicações de internet estariam obrigados a atender à solicitações da autoridade policial, administrativa ou o Ministério Público.

9. Disso se infere que o pedido de 'congelamento' do Ministério Público, contra o qual se rebelam os impetrantes, e diversamente do que advogam, não precisa necessariamente de prévia decisão judicial para ser atendido pelo provedor, mesmo porque — **e esse é o ponto nodal da discussão, visto em face do direito à preservação da intimidade, da vida privada, da honra e da imagem das partes** (CF - art. 5º, X, e Lei 12.965/2014 - art. 10) — não equivale a que o requerente tenha acesso aos dados 'congelados' sem ordem judicial.

10. A jurisprudência do STF tem afirmado que o inciso XII do art. 5º da Constituição protege somente o sigilo das comunicações em fluxo (troca de dados e mensagens em tempo real), e que o sigilo das comunicações armazenadas, como depósito registral, é tutelado pela previsão constitucional do direito à privacidade do inciso X do art. 5º (HC nº 91.867 - Rel. Ministro Gilmar Mendes - 2ª Turma, julgado em 24/04/2012).

11. Mas, em verdade, a disponibilização ao requerente dos registros de que trata a Lei 12.965/2014 (dados intercambiados), em atenção à referida cláusula constitucional, deverá ser precedida de autorização judicial, sendo estabelecido, inclusive, um prazo de 60 dias, contados a partir do requerimento de preservação dos dados, para que o Ministério Público ingresse com esse pedido de autorização judicial de acesso aos registros, sob pena de caducidade (art. 13, § 4º).

12. No caso dos autos, o Ministério Público requereu apreservação de dados e conteúdos eletrônicos às plataformas em 22/11/2019, o que foi mantido em sigilo, e ingressou com pedido de quebra do sigilo desses dados em 29/11/2019, tendo o Juízo singular deferido fundamentadamente o pleito em 3/12/2019.

13. Esse tema, diversamente do que advogam os impetrantes, não se relaciona com a matéria da Arguição de Descumprimento de Preceito Fundamental - ADPF n. 403/SE, Ministro Relator Edson Fachin, com julgamento ainda não concluído, nem com a Ação Direta de Inconstitucionalidade - ADI n. 5527/DF, Ministra Rosa Weber, nas quais se discute a interpretação do inciso II do art. 7º e do inciso III do art. 12 da Lei 12.965/2014, que autorize ordem judicial que exija acesso excepcional a conteúdo de mensagem criptografada ponta-aponta ou que, por qualquer outro meio, enfraqueça a proteção

criptográfica de aplicações da internet, o que não tem pertinência nenhuma com o objeto do presente caso.

14. O Ministério Público solicitou 'a preservação dos dados e IMEI coletados a partir das contas de usuários vinculadas, tais como dados cadastrais, histórico de pesquisa, todo conteúdo de e-mail e *iMessages*, fotos, contatos e históricos de localização, desde a data de 01.06.2017 até o presente momento', pedido que, na tese dos impetrantes, exorbitaria os limites legais, porque o conteúdo de e-mail e *iMessages*, fotos, contatos e históricos de localização não fariam parte do conceito de '**registros de acesso a aplicações de internet' ou 'registros de conexão'**.

15. A Lei 12.965/2014, define que 'registros de acesso a aplicações de internet' são o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP' (art. 5º, VIII). Já o inciso VII define que 'aplicações de internet' são o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet.

16. A lei a fim de viabilizar investigações criminais, que, normalmente, são de difícil realização em ambientes eletrônicos, tornou mais eficiente o acesso a dados e informações relevantes ao possibilitar que o Ministério Público, diretamente, requeira ao provedor apenas a guarda, em ambiente seguro e sigiloso, dos registros de acesso a aplicações de internet, mas a disponibilização ao requerente dos conteúdos dos registros — dados cadastrais, histórico de pesquisa, todo conteúdo de e-mail e *iMessages*, fotos, contatos e históricos de localização etc. — deve sempre ser precedida de autorização judicial devidamente fundamentada, o que ocorreu no presente caso.

> 17. Não se perfaz a pretendida nulidade do pedido de 'congelamento' dos registros, além do tempo legal, pelo Ministério Público do Estado do Paraná, vindo o acesso aos respectivos dados a ser deferido, a tempo e modo, por ordem judicial, sob pena de caducidade (art. 13, § 4º).
>
> 18. *Habeas corpus* denegado." (doc. eletrônico 32, grifos no original).

Os impetrantes afirmam que,

> "[...] com o objetivo de angariar elementos para as investigações relacionadas à Operação Taxa Alta, o MPPR [Ministério Público do Estado do Parana] expediu ofícios às empresas Apple e Google, solicitando que preservassem os dados e IMEI coletados a partir das contas de usuários vinculadas aos sócios e diretores da INFOSOLO, tais como dados cadastrais, histórico de pesquisa, todo conteúdo de *e-mail* e *iMessages/hangouts*, fotos, contatos e histórico de localização […].
>
> 7. Procedeu com esta solicitação antes de apresentar o pedido de quebra de sigilo de dados telemáticos da Paciente, determinando que tais provedores impedissem a livre utilização, por parte de seus titulares, de todos os dados que estivessem armazenados em referidas plataformas […].
>
> 8. Somente uma semana depois da 'ordem' ministerial, o *Parquet* apresentou o pedido de quebra de dados telemáticos, sendo tal pleito concedido pelo Juízo de primeira instância em 03 de dezembro de 2019.
>
> [...]
>
> [o] Ministério Público, ao solicitar o congelamento de dados relativos aos 'registros de conexão e de acesso a aplicações de internet' diretamente aos fornecedores de serviços de armazenamento de dados, extrapolou suas atribuições, ao

> incluir, também, a preservação do conteúdo das contas dos usuários, congelamento esse que se reveste de verdadeira medida cautelar sob reserva de jurisdição.
>
> […]
>
> 24. A partir do momento em que o Ministério Público manipulou a possibilidade de acessá-lo (congelando-o sem autorização judicial), violou flagrantemente o disposto no artigo 5º, inciso XII, da Constituição Federal, com ressonância na Lei 12.965/2014, em termos de proteção aos direitos fundamentais da pessoa humana. Isso porque compete, única e exclusivamente ao Poder Judiciário, determinar o congelamento do CONTEÚDO armazenado pelos prestadores de serviço de modo que não compete ao Ministério Público assim fazê-lo, como o fez no caso ora em análise." (doc. eletrônico 1, fls. 2-11).

Requerem, assim, ao final,

> "(a) liminarmente, a concessão da medida liminar, inaudita altera partes, por seus próprios fundamentos, para a suspensão do trâmite da ação penal n. 0014768-70.2020.8.16.0013, que tramita perante a 12ª Vara Criminal de Curitiba/PR;
>
> (b) quando do julgamento do mérito, sejam declarados nulos os elementos de prova angariados em desfavor da Paciente a partir do congelamento prévio e despido de autorização judicial do conteúdo de suas contas, nos autos da ação penal ora em comento, tudo por violação ao princípio do juiz natural (CF, art. 5º, inciso LIII) e por violação ao princípio da jurisdicionalidade." (págs. 20-21 da petição inicial).

Por não verificar, naquele momento, os requisitos da medida de urgência, indeferi o pleito liminar (doc. eletrônico 35), decisão contra a qual se interpôs agravo regimental (doc. eletrônico 37).

A Procuradoria-Geral da República manifestou-se pelo não conhecimento da impetração. No mérito, posicionou-se pela denegação da ordem (doc. eletrônico 40).

É o relatório. Decido.

Acentue-se, de início, que embora o presente *writ* tenha sido impetrado em substituição a recurso ordinário, não oponho óbice ao seu conhecimento, na linha do que decidiu o Plenário deste Supremo Tribunal no julgamento do HC 152.752/SP, relator Ministro Edson Fachin.

Por esses motivos, passo ao exame do mérito desta impetração.

Preliminarmente, assinalo a desnecessidade do revolvimento de matéria fático-probatória, o que é vedado nesta via estreita. Sim, pois é incontroverso que o Ministério Público do Estado do Paraná expediu, em 22/11/2019, ofícios aos provedores Apple e Google, nos quais requereu a preservação dos dados e *IMEI*'s coletados nas contas vinculadas aos sócios da empresa INFOSOLO, tais como "informações cadastrais, histórico de localização e pesquisas, conteúdo de *e-mails* e *iMessages*/*hangouts*, fotos e nomes de contatos" (doc. eletrônico 2). Tal medida objetivava angariar elementos de prova na denominada "Operação Taxa Alta" (Procedimento Investigatório Criminal
0046.19.094917-5), por supostas irregularidades no Detran/PR quanto ao credenciamento de empresas para serviços de registro eletrônico de contratos.

Destaco, de saída, que o supracitado pedido formulado pelo *Parquet* não teve lastro em qualquer decisão judicial de quebra de sigilo telemático, muito embora, a rigor, isso significasse impedir a disponibilidade, por parte da investigada, de todos os dados que estivessem armazenados nas referidas plataformas, a contar do dia 1º/6/2017 até a data do requerimento. O pedido de quebra do sigilo da paciente, em verdade, foi apresentado à autoridade judicial somente em 29/11/2019, tendo o juízo singular deferido fundamentadamente o pleito em 3/12/2019 (docs. eletrônicos 3 e 4).

Assim, o ponto nodal da discussão consiste em saber se o "congelamento" - e consequente perda da disponibilidade - de todo o conteúdo de *e-mails*, mensagens, contatos e históricos de localização da paciente encontra-se albergado pela reserva de jurisdição, à vista do direito à preservação da intimidade, da vida privada, da honra e da imagem das pessoas (art. 5º, X, da Constituição Federal). Anoto, outrossim, que o inciso XII do Texto Maior igualmente estatui que "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".

A jurisprudência desta Suprema Corte tem afirmado reiteradamente que o inciso XII do art. 5º da Carta Magna protege o sigilo das comunicações em fluxo (troca de dados e mensagens). Assenta também que o sigilo das comunicações armazenadas, como depósito registral, é tutelado pela previsão constitucional do direito à privacidade, na forma do inciso X do art. 5º, CF (cito, *v.g.*, o HC 91.867/PA, relator Ministro Gilmar Mendes). No campo infraconstitucional, o Marco Civil da Internet

(Lei 12.965/2014) traça os princípios aplicáveis em nosso ordenamento, enumerados no art. 3º, tal como o da proteção da privacidade e dos dados pessoais, assegurando, outrossim, a inviolabilidade e sigilo do fluxo de suas comunicações e sigilo de suas comunicações privadas armazenadas, ressalvada ordem judicial de sua quebra (art. 7º da mencionada lei).

Partindo dessas premissas, tenho que o pedido de indisponibilidade dos registros de que trata a Lei 12.965/2014 (dados intercambiados), seja pelo Ministério Público, seja por autoridades policiais ou administrativas, em atenção à referida cláusula constitucional, deverá, a toda evidência, ser precedido de indispensável autorização judicial. Sim, pois, na forma do art. 5º, V, da supracitada legislação, os registros de conexão se referem, tão somente, ao conjunto de informações concernentes à data e hora de início e de término de uma conexão à internet, sua duração e o endereço de IP utilizado pelo terminal. Registros de acesso a aplicações de internet, por sua vez, previstos no inciso VIII do citado dispositivo, tratam apenas do conjunto de informações relativas à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço de IP. Confira-se:

> "Art. 5º Para os efeitos desta Lei, considera-se:
>
> [...]
>
> V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;
>
> VI - registro de conexão: o 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

> VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
>
> VIII **- registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP**." (grifei)

A referida legislação, no seu art. 10, § 1º, ao tratar de forma específica da proteção aos registros, dados pessoais e comunicações privadas, é clara quanto à possibilidade de fornecimento de informações de acesso (registro de conexão e registro de acesso a aplicações de internet), **desde que sejam requisitados por ordem de um juiz**. Veja-se:

> "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." (grifei)

Já a subseção I do mesmo texto cuida da "Da Guarda de Registro de Conexão", *verbis*:

> "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.
>
> § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
>
> § 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*."

Verifica-se que a autoridade requerente tem 60 dias para pleitear o acesso aos registros de conexão, quais sejam, tão somente o 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. Tais elementos, portanto, não se confundem com o material telemático, como, por exemplo, o conteúdo de *e-mail*, *iMessages*/*hangouts*, fotos e contatos.

Caso prevalecesse o entendimento esposado no acórdão combatido, toda e qualquer autoridade policial ou o próprio Ministério Público poderiam requisitar aos provedores da internet, sem a devida autorização judicial, a indisponibilidade de dados telemáticos de qualquer investigado, situação que, a toda evidência, não se concebe. Nesta senda, rememoro as palavras do Ministro Edson Fachin no julgamento da ADPF 403/DF, de sua relatoria, ao enfatizar que a privacidade é o direito de manter o controle

sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública. Veja-se:

> "1.1. Premissas
>
> [...]
>
> Terceira: 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
>
> **Quarta: a privacidade é o direito de manter o controle sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública**.
>
> […]
>
> 1.2. Base constitucional: o direito à comunicação (art. 5º, IX, da CRFB), à liberdade de pensamento e de sua expressão (art. 5º, IV, da CRFB) e à privacidade (art. 5º, X, XI, e XII); e base convencional (art. 5º, § 2º, da CRFB): a liberdade de opinião e de expressão (artigo 19 do Pacto Internacional de Direitos Civis e Políticos e artigo 13 do Pacto de São José da Costa) e o direito à privacidade (artigo 17 do Pacto Internacional de Direitos Civis e Políticos e artigo 11 do Pacto de São José da Costa Rica).
>
> 1.3. Base em precedentes: o voto se estriba em precedentes que formam jurisprudência deste Tribunal, do Conselho de Direitos Humanos das Nações Unidas, da Corte Europeia de Direitos Humanos e do Comitê de Direitos Humanos.
>
> 1.4. Base doutrinária: o voto faz referência ao Relatório The Effect of Encryption on Lawful Access to Communication and Data de autoria de James A. Lewis, Denis E. Zheng e William A. Carter; ao artigo On Balancing and Subsumption. A Strucutral Comparison de autoria de Robert Alexy; às obras de

> Stéfano Rodotà (Data Protection as a Fundamental Right); aos Comentários ao Pacto Internacional de Direitos Civis e Políticos, elaborado por Manfred Nowak; ao artigo *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda, de autoria de Laura Schertel Ferreira Mendes; aos Comentários à Constituição de João Barbalho; ao texto Passado, presente e futuro da criptografia forte de Jacqueline de Souza Abreu; e ao brilhante artigo de Harold Abelson *et al*. Intitulado Keys under doormats."

Em obra dedicada ao tema, Adriano Marteleto Godinho e Wilson Furtado Roberto ponderam o seguinte:

> "Da análise do texto dos incisos VI e VIII do art.5º, constata-se que o propósito do art. 13 do Marco Civil da Internet consiste em disciplinar, de forma exclusiva, a manutenção dos registros de conexão, **que abarcam apenas informações relativas ao termo inicial e final de uma conexão - e, consequentemente, sua duração - e o endereço IP, isto é, o endereço de protocolo da internet**, qualificado como 'o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais' pelo inciso III do mesmo art. 5º. **A disponibilização dos registros de conexão, pois, não revela dados pessoais do usuário responsável pelo acesso à rede, tais como nome, endereço e informações de identificação (CPF, RG e outras) - cabendo salientar, a propósito, que o Marco Civil da Internet sequer especifica quais dados cadastrais devem ser cobrados pelo utente no momento da contratação do serviço de acesso à Internet junto ao provedor**. Ademais, da guarda de registros de acesso a aplicações de Internet cuidam os arts. 14 e 15 da Lei, ficando sua análise à margem do escopo central deste capítulo, destinado a investigar de que modo se dará a guarda

> exclusiva de registros de conexão e o eventual requerimento judicial para o fornecimento de tais dados."(GODINHO, Adriano Marteleto e ROBERTO, Wilson Furtado, *in* LEITE, George Salomão e LEMOS, Ronaldo, *Coord. Marco Civil da Internet*. São Paulo: Atlas; 2 ed., 2015, págs. 744-745, grifei).

Os mesmos autores demonstram certa perplexidade com o risco de interpretações ampliativas dos poderes dados às autoridades públicas para requererem a preservação de dados sem que haja autorização judicial a este respeito, *litteris*:

> "Há, todavia, certos aspectos nebulosos relativamente ao modo que a lei regulamentou, em particular, a guarda dos registros de conexão. Sabe-se, do teor do já analisado art. 13 do Marco Civil, que a obrigação de manutenção destes dados perdura por um período de um ano, estabelecendo o § 2º do próprio dispositivo que tanto a autoridade policial ou administrativa quanto o Ministério Público podem requerer cautelarmente que os registros de conexão fiquem armazenados sigilosamente por lapso temporal mais extenso. E, para já, surgem algumas indagações acerca dos exatos contornos para a solicitação em questão. **Salta aos olhos a possibilidade de não apenas o órgão ministerial, como também a autoridade policial ou administrativa virem a solicitar a ampliação do aludido prazo**. E, à falta de previsão legal específica, resta indagar: **quem seria a tal 'autoridade administrativa' competente para tais fins? Diante da omissão legislativa, resta ainda questionar: por quanto tempo os dados continuariam a ser preservados? Não se estaria, afinal, conferindo amplíssima margem ao Estado para intervir nos domínios da internet?**"

(*Op. Cit.*, pág. 751, grifei)

Sobre o tema, extraem-se, ainda, informações do sítio oficial da Casa Civil acerca do sentido do termo "registros de conexão":

> "Registros de conexão - IP atribuído ao computador, hora e data de início e término de sua conexão à Internet: Cada vez que um computador é conectado à Internet, ele é identificado por um número de endereço IP, que identifica aquela conexão (em alguns casos, uma mesma conexão pode ser partilhada por mais de um terminal, sendo que todos eles serão identificados na Internet pelo mesmo número IP (este é o caso dos roteadores *wifi* domésticos, por exemplo). São as empresas que prestam o serviço de conexão que atribuem aos seus usuários os endereços IP. Essas empresas, como qualquer prestadora de serviço, mantêm cadastros de seus usuários. Logo, um provedor de conexão já é capaz, hoje, de identificar seus usuários a partir do endereço IP. (CASA CIVIL. Perguntas e respostas sobre Marco Civil da Internet. Disponível em: https:// casa- civil. jusbrasil.com.br/ noticias /2816963/ perguntas-e-respostas-sobre-marco-civil-da-internet >, Acesso em: 22 nov. 2022)

Assim, vê-se que cabe ao Ministério Público requerer cautelarmente que os registros de conexão sejam guardados por prazo superior a 1 ano, quais sejam, aqueles exclusivos a informações de data e hora de acesso, duração e IP de origem, o que, como afirmado alhures, não se confunde com o conteúdo telemático armazenado dentro dos sistemas autônomos, tais como históricos de pesquisa, todo o conteúdo de e-mail e *Imessages*, fotos e dados de localização. Entendimento diverso levaria à autorização para que houvesse a busca e apreensão prévia de conteúdos e seu congelamento, para posterior formalização da medida por ordem judicial,

em prática vedada por qualquer *stantard* que se extraia da ordem constitucional vigente.

Conclui-se, portanto, que, na hipótese sob exame, o Ministério Público do Estado do Paraná não observou a necessária reserva de jurisdição no que toca à ordem de indisponibilidade do conteúdo telemático por parte da sua legítima titular, contrariando, na forma acima delineada, a Constituição Federal e o Marco Civil da Internet, pois decretou verdadeira medida cautelar ao ordenar, *sponte propia*, o "congelamento" de todo o conteúdo de comunicações telemáticas da paciente. Em suma, retirou do seu legítimo proprietário o direito de dispor do conteúdo dos seus dados para quaisquer fins, sem que houvesse autorização judicial para tanto.

Isso posto, concedo a ordem a fim de declarar nulos os elementos de prova angariados em desfavor da paciente a partir do congelamento prévio, sem autorização judicial, do conteúdo de suas contas eletrônicas, bem como de todos os demais que dele decorrem, nos autos da ação penal ora em comento.

Fica, consequentemente, prejudicado o agravo regimental interposto pela paciente.

Publique-se.

Brasília, 1ª de dezembro de 2022.

Ministro **Ricardo Lewandowski**
Relator