



## **SUPERIOR TRIBUNAL DE JUSTIÇA**

**RECURSO EM HABEAS CORPUS Nº 214389 - PR (2025/0127658-3)**

**RELATOR : MINISTRO OTÁVIO DE ALMEIDA TOLEDO**  
**(DESEMBARGADOR CONVOCADO DO TJSP)**

**R.P/ACÓRDÃO : MINISTRO SEBASTIÃO REIS JÚNIOR**

**RECORRENTE : R D G**

**RECORRENTE : R M M**

**ADVOGADOS : SERGIO ROSENTHAL - SP114806**  
**JULIANO JOSE BREDAS - PR025717**  
**CARINA QUITO - SP183646**  
**NICOLE TRAUZYNSKI MUFFONE - PR041301**  
**ADRIANO SERGIO NUNES BRETAS - PR038524**  
**GABRIEL GARCIA SOARES - PR118659**  
**VALESKA TEIXEIRA ZANIN MARTINS - SP153720**  
**ANTONIO GLAUCIUS DE MORAIS - DF012308**

**RECORRIDO : MINISTÉRIO PÚBLICO DO ESTADO DO PARANÁ**

**ADVOGADO : JOAO PAULO DE OLIVEIRA BOAVENTURA - DF031680**

**INTERES. : T B L**

**INTERES. : W C M F**

**INTERES. : M D L E R J**

**ADVOGADOS : BENO FRAGA BRANDAO - PR020920**  
**EDUARDA CANDIDO ZAPPONI - DF064353**  
**IGOR ARTHUR RAYZEL - PR075656**  
**IGOR CUSTODIO DE ARAUJO FERREIRA - DF080602**  
**IGOR DOS SANTOS JAIME - DF054584**  
**JOAO PAULO DE OLIVEIRA BOAVENTURA - DF031680**  
**MATTEUS BERESA DE PAULA MACEDO - DF070111**  
**OTTO MEDEIROS DE AZEVEDO JUNIOR - DF047761**  
**THIAGO TURBAY FREIRIA - DF057218**  
**TRACY JOSEPH REINALDET DOS SANTOS - DF069913**

### **EMENTA**

DIREITO PROCESSUAL PENAL. RECURSO ORDINÁRIO EM *HABEAS CORPUS*. CRIMES LEI Nº 11.101/05 QUEBRA DE SIGILO TELEMÁTICO. PRAZO DE MONITORAMENTO IMPOSTO AO FLUXO DE COMUNICAÇÃO. ACESSO A DADOS PRETÉRITOS ARMAZENADOS NO ONEDRIVE. POSSIBILIDADE.

1. A questão formulada no presente recurso ordinário cinge-se em verificar se a autorização de interceptação das comunicações telemáticas por prazo determinado, conforme permitido pelo Juízo de primeiro grau, abrangeria o acesso aos dados telemáticos armazenados, relativos a período anterior à autorização judicial.
2. Embora coubesse ao Magistrado singular pormenorizar melhor a forma de efetivação da medida investigativa, a fim de evitar a presente controvérsia, o requerimento da autoridade policial e o parecer do Ministério Público não deixam dúvidas sobre a necessidade de concessão da medida.
3. Mostra-se correto o acórdão hostilizado ao reconhecer que a delimitação temporal exigida pela legislação vigente é imposta ao monitoramento do fluxo de comunicação, uma vez que a decisão atacada, além do monitoramento do fluxo de e-mails, também determinou ao final (e nos termos do requerimento da autoridade policial e manifestação do Ministério Público), o acesso aos arquivos armazenados no “OneDrive”, além dos registros de transações no mesmo dispositivo de armazenamento.
4. Recurso ordinário improvido.

## **ACÓRDÃO**

Vistos e relatados estes autos em que são partes as acima indicadas, acordam os Ministros da SEXTA TURMA do Superior Tribunal de Justiça, prosseguindo no julgamento, após o voto vista do Sr. Ministro Sebastião Reis Júnior negando provimento ao agravo regimental, sendo acompanhado pelos Srs. Ministros Joel Ilan Paciornik e Antonio Saldanha Palheiro, por maioria, negar provimento ao agravo regimental, nos termos do voto do Sr. Ministro Sebastião Reis Júnior, que lavrará o acórdão.

Votaram com o Sr. Ministro Sebastião Reis Júnior os Srs. Ministros Antonio Saldanha Palheiro e Joel Ilan Paciornik. Vencido o Sr. Ministro Otávio de Almeida Toledo (Desembargador Convocado do TJSP). Impedido o Sr. Ministro Rogerio Schietti. Afirmou suspeição o Sr. Ministro Og Fernandes. Não participou do julgamento o Sr. Ministro Carlos Pires Brandão.

Brasília, 11 de novembro de 2025.

Ministro Sebastião Reis Júnior  
Relator



## SUPERIOR TRIBUNAL DE JUSTIÇA

**RECURSO EM HABEAS CORPUS Nº 214389 - PR (2025/0127658-3)**

**RELATOR : MINISTRO OTÁVIO DE ALMEIDA TOLEDO (DESEMBARGADOR CONVOCADO DO TJSP)**

RECORRENTE : R D G

RECORRENTE : R M M

ADVOGADOS : SERGIO ROSENTHAL - SP114806  
JULIANO JOSE BRED A - PR025717  
CARINA QUITO - SP183646  
NICOLE TRAU CZYNSKI MUFFONE - PR041301  
ADRIANO SERGIO NUNES BRETAS - PR038524  
GABRIEL GARCIA SOARES - PR118659  
VALESKA TEIXEIRA ZANIN MARTINS - SP153720  
ANTONIO GLAUCIUS DE MORAIS - DF012308

RECORRIDO : MINISTÉRIO PÚBLICO DO ESTADO DO PARANÁ

ADVOGADO : JOAO PAULO DE OLIVEIRA BOAVENTURA - DF031680

INTERES. : T B L

INTERES. : W C M F

INTERES. : M D L E R J

ADVOGADOS : BENO FRAGA BRANDAO - PR020920  
EDUARDA CANDIDO ZAPPONI - DF064353  
IGOR ARTHUR RAYZEL - PR075656  
IGOR CUSTODIO DE ARAUJO FERREIRA - DF080602  
IGOR DOS SANTOS JAIME - DF054584  
JOAO PAULO DE OLIVEIRA BOAVENTURA - DF031680  
LUCAS FISCHER DE MORAES - PR106737  
MATTEUS BERESA DE PAULA MACEDO - DF070111  
OTTO MEDEIROS DE AZEVEDO JUNIOR - DF047761  
THIAGO TURBAY FREIRIA - DF057218  
TRACY JOSEPH REINALDET DOS SANTOS - DF069913

### EMENTA

DIREITO PROCESSUAL PENAL. RECURSO ORDINÁRIO EM *HABEAS CORPUS*. INTERCEPTAÇÃO TELEMÁTICA. QUEBRA DE SIGILO DE DADOS. MEDIDAS DISTINTAS E INCONFUNDÍVEIS. AUSÊNCIA DE FUNGIBILIDADE. FALTA DE REQUERIMENTO E AUTORIZAÇÃO JUDICIAL ESPECÍFICOS. ILICITUDE DAS PROVAS. RECURSO PROVIDO.

#### I. Caso em exame

1. Recurso ordinário interposto contra acórdão do Tribunal de Justiça do Estado do Paraná que denegou *habeas corpus*, o qual alegava serem nulos os elementos colhidos em medida cautelar de interceptação telemática, sob alegação de que a ordem judicial não autorizava a captura de material telemático fora do período de 15 (quinze) dias subsequentes à sua implementação (dados estáticos já armazenados anteriormente).

## **II. Questão em discussão**

2. A discussão consiste em saber (i) se houve requerimento e autorização judicial de quebra de sigilo de dados e (ii) se a autorização de interceptação telemática, por si só, justifica também o acesso aos dados estáticos (quebra de sigilo).

## **III. Razões de decidir**

3. As medidas de interceptação telemática e quebra de sigilo de dados telemáticos são distintas, incidindo sobre contextos e objetos diferentes, com graus diversos de afetação do resguardo à intimidade e ao sigilo das comunicações e regência por normativas que não se confundem.

4. A interceptação telemática tem incidência *ex nunc*, implicando no monitoramento em tempo real das comunicações (no caso, *e-mails*), incidindo sobre fluxo dinâmico de dados e encontrando disciplina na Lei n. 9.296/1996.

5. A quebra de sigilo de dados tem incidência *ex tunc*, viabilizando o acesso à comunicação realizada antes da autorização, incidindo sobre dados estáticos já armazenados e extraíndo seus contornos legais da Lei n. 12.965/2014.

6. Tais medidas cautelares são técnica e legalmente inconfundíveis, de modo que o requerimento e o deferimento de cada uma delas deve ser, de igual modo, inequívoco, uma vez que inexiste uma formatação jurídica híbrida a abarcar ambas.

7. Em caso de frustração ou insuficiência na realização de uma dessas medidas, não se cogita de fungibilidade automática, sem ordem judicial prévia e indubitosa, a autorizar a realização da outra.

8. Caso concreto em que foi requerida pela autoridade policial, com manifestação favorável do Ministério Público e deferimento judicial, a medida de interceptação telemática, sem referências à Lei n. 12.965/2014. As referências normativas e fixação de prazo de 15 (quinze) dias tornam clara a circunscrição da medida à interceptação. A

menção ao acesso a arquivos se deu no contexto das providências a serem tomadas pela empresa destinatária da ordem para viabilizar o monitoramento requerido.

9. A captura de dados estáticos sem autorização judicial específica é ilícita, conforme o art. 157 do Código de Processo Penal.

#### **IV. Dispositivo e tese**

10. A ordem deve ser concedida para declarar nulos os elementos colhidos a partir da quebra de sigilo telemático dos recorrentes e determinando seu desentranhamento do inquérito.

11. Ordem concedida.

*Tese de julgamento:* 1. As medidas de interceptação telemática e quebra de sigilo de dados telemáticos são distintas e inconfundíveis técnica e juridicamente, de modo que a decisão judicial que as autoriza deve ser específica e expressa quanto a cada uma delas. 2. Não há fungibilidade entre as medidas de interceptação telemática e quebra de sigilo de dados telemáticos, sendo inviável a transmutação de uma em outra sem prévia e inequívoca autorização judicial. 3. A quebra de sigilo de dados telemáticos realizada no contexto da frustração da interceptação telemática, somente esta autorizada judicialmente, é ilícita, devendo os elementos colhidos a partir dela serem desentranhados dos autos.

*Dispositivos relevantes citados:* Lei n. 9.296/1996; Lei n. 12.965/2014; CPP, art. 157.

*Jurisprudência relevante citada:* STJ, RMS n. 62.143/RJ, Rel. Min. Rogerio Schietti Cruz, Terceira Seção, julgado em 26/08/2020; STJ, AgRg no RHC n. 189.011/SP, Rel. Min. Ribeiro Dantas, Quinta Turma, julgado em 18/03/2024; STJ, AgRg no RHC n. 215.014/SC, Rel. Min. Reynaldo Soares da Fonseca, Quinta Turma, julgado em 20/5/2025; STJ, AgRg no RHC n. 200.321/PR, Rel. Min. Sebastião Reis Júnior, Sexta Turma, julgado em 26/02/2025; STJ, RHC n. 99.735/SC, Rel. Min. Laurita Vaz, Sexta Turma, julgado em 27/11/2018.

### **RELATÓRIO**

Cuida-se de recurso ordinário, com pedido de liminar, interposto por R D G e R M M, do TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ no HC n. 072261-05.2024.8.16.0000, em acórdão assim ementado (fl. 731):

*HABEAS CORPUS – CRIMES LEI Nº 11.101/05 – QUEBRA DE SIGILO TELEMÁTICO – LEGALIDADE DA PROVA – OBSERVADOS OS REQUISITOS LEGAIS PARA DEFERIMENTO DA ORDEM – PRAZO*

*PARA ACESSO A E-MAILS – ACESSO DETALHES DO REGISTRO DA CONTA E DO NÚMERO DO IP DE ACESSO QUANDO DO REGISTRO DA CONTA, CONTEÚDOS DE E-MAIL, CONTATOS DE E-MAIL, DETALHES DE REGISTRO DO ONEDRIVE, LOGS DE IP DE ACESSO AO ONEDRIVE, ARQUIVOS ARMAZENADOS NO ONE DRIVE E REGISTROS DE TRANSAÇÕES NO ONEDRIVE – POSTULADO DA PROPORCIONALIDADE – IMPOSSIBILIDADE DE PRODUÇÃO DE PROVAS NA VIA DO WRIT– ORDEM DENEGADA.*

Consta dos autos que os pacientes são investigados pela suposta prática do delito capitulado no art. 168 da Lei n. 11.101/2005.

Foi impetrado, na origem, *habeas corpus* questionando a legalidade dos elementos colhidos no bojo da medida cautelar de interceptação telemática sob alegação, em síntese, de que a ordem judicial que foi deferida para o monitoramento, pelo período de 15 (quinze) dias, dos *e-mails* dos investigados, não continha *qualquer comando explicitando a violação do sigilo telemático de comunicações previamente transmitidas* (fl. 4).

Denegada a ordem pelo Tribunal *a quo* (ementa transcrita *supra*), houve a interposição do recurso ordinário (fls. 955/971 - em 28/10/2024). Com a oposição de embargos de declaração por terceiros, não conhecidos, mas ensejando a correção de erro material (fls. 937/346 - em 07/03/2025), integrada a decisão, novamente ocorreu, após a intimação eletrônica (fls. 951 - em 20/03/2025), a interposição de recurso ordinário (fls. 1010/1026 - em 21/03/2025).

Os recorrentes **reprisam** as teses ventiladas na origem, salientando, em síntese, que

*[n]ão há como se extrair do pedido formulado pela Autoridade Policial, assim como da decisão judicial de primeiro grau que deferiu a interceptação telemática (monitoramento em tempo real dos e-mails dos recorrentes), qualquer autorização para a captura de material telemático (mensagens de e-mail) que não fosse relativo ao período de 15 dias subsequentes à sua implementação.*

Argumentam, pela natureza prospectiva da medida deferida, que o acesso ao material telemático armazenado no sistema OneDrive da Microsoft (que, conforme os recorrentes, não se trata de mensagens de e-mail, mas de dados) restou deferido no mesmo contexto, ou seja, no período delimitado de 15 (quinze) dias.

Reputam, assim, inquinadas de nulidade as

*mensagens de e-mail relativas ao período de um ano pretérito àquela data (armazenadas em suas caixas de e-mail - sistema Exchange - e ilegalmente juntadas aos autos pela Autoridade Policial* (fl. 1018).

Requerem que seja dado provimento ao recurso

*para o fim de declarar a nulidade da quebra do sigilo telemático dos recorrentes efetuada ilegalmente pela Autoridade Policial nos autos da medida cautelar de interceptação telemática nº 0016436-71.2023.8.16.0013, instaurada perante a 5ª Vara Criminal de Curitiba, Estado do Paraná, determinando-se, em consequência, o desentranhamento e a inutilização do material juntado aos autos do inquérito policial nº 0026936-36.2022.8.16.0013 (fl. 1026).*

Em petição às fls. 1914/1916, os recorrentes, informando a realização de oitivas pela autoridade policial no bojo do inquérito subjacente, requerem a concessão de medida liminar

*determinando o acautelamento do material telemático (e-mails) ilegalmente obtido pela autoridade policial, juntado aos autos da medida cautelar de interceptação telemática nº 0016436-71.2023.8.16.0013, bem como proibindo sua utilização no âmbito do inquérito policial nº 0026936-36.2022.8.16.0013, assim como de qualquer outro procedimento, até o julgamento do recurso interposto.*

Indeferida a liminar (fls. 1928/1931), vieram informações (fls. 1939/1941 e 1947/1962), ao que se seguiu a manifestação do Ministério Público Federal, às fls. 1965/1972, pelo conhecimento e não provimento do recurso ordinário.

Às fls. 1979/1982, os recorrentes informaram quanto ao andamento do inquérito, reiterando os termos do pedido no RHC.

É o relatório.

## **VOTO**

O recurso merece provimento.

Ao julgar o *writ* originário, o Tribunal *a quo* assim se manifestou (fls. 733/739 - grifamos):

*Em breve síntese, em 21/12/2022 instaurou-se inquérito policial (nº 0026936- 36.2022.8.16.0013 - 260057/2022) para apurar a prática, em tese, do crime tipificado no artigo 171, da Lei nº 11.101/05, por parte dos pacientes, dentre outros, com base em notícia crime apresentada perante a Divisão Estadual de Combate à Corrupção em Curitiba por W F, proprietário da Cervejaria Petrópolis.*

*A fim de prosseguir nas investigações, considerando a existência de indícios contundentes acerca da existência de conduta criminosa e de sua autoria, a autoridade policial elaborou relatório sobre o caso e **representou ao juízo pedido de interceptação telemática, "uma vez que as tratativas e respectivas apreciações estão sendo mantidas por e-mails, o que dificulta a obtenção de elementos de informação por outros meios"**, mencionando o provedor de hospedagem dos e-mails como sendo da Microsoft (mov. 1.2):*

*"A presente interceptação, uma vez deferida, deverá ser atendida pela Microsoft que fornecerá os dados das contas, por meio de seu portal, detalhes de registro, informações de faturamento e transações de faturamento, acaso existentes, registros dos*

números de IP (Internet Protocol) no momento do login dos usuários, serviços da Microsoft utilizados, detalhes do registro da conta e do número do IP de acesso quando do registro da conta, conteúdos de e-mail, contatos de e-mail, detalhes de registro do OneDrive, logs de IP de acesso ao OneDrive, arquivos armazenados no One Drive e registros de transações no OneDrive".

O d. **Magistrado deferiu o pedido, delimitando-o nos seguintes termos** (mov. 1.6):

"4.1. Autorizo a **interceptação telemática pelo prazo de 15 (quinze) dias** passível de prorrogação, **dos endereços de e-mails abaixo listados**, determinando a expedição de **ofício à MICROSOFT para que**, no prazo de 24 (vinte e quatro) horas, **inicie o monitoramento dos e-mails e forneça** os dados das contas - por meio de seu portal - detalhes de registro, informações de faturamento e transações de faturamento acaso existentes, registros dos números de IP (Internet Protocol) no momento do login dos usuários, serviços da Microsoft utilizados, detalhes do registro da conta e do número do IP de acesso quando do registro da conta, **conteúdos de e-mails**, contatos de e-mails, detalhes de registro do OneDrive, logs de IP de acesso ao OneDrive, **arquivos armazenados no OneDrive** e registros de transações no OneDrive, ficando expressamente vedada a interceptação de endereços eletrônicos não discriminados na presente decisão".

A **decisão judicial foi cumprida pela empresa Microsoft** (mov. 52.1 - 0016436-71.2023.8.16.0013), a qual **informou acerca da impossibilidade da interceptação telemática dos e-mails futuros por meio de "conta espelho"**, em razão de os dados solicitados serem de uma "conta Enterprise", a qual não permite seu compartilhamento por blocos. **Todavia forneceu acesso aos dados contidos em arquivo remoto "OneDrive" da data do recebimento da ordem até em um ano pretérito.**

É em relação a esses dados contidos no arquivo remoto "OneDrive" que se insurgem os impetrantes.

No **juízo a quo**, requereram "a declaração de ilicitude e desentranhamento dos elementos probatórios obtidos nos autos da medida cautelar de interceptação telemática (processo nº 0016436-71.2023.8.16.0013), bem como a declaração de nulidade da medida cautelar de busca e apreensão (processo nº 0001909-80.2024.8.16.0013) fundada nesses elementos" (mov. 1.47), o que restou indeferido nos **seguintes termos** (mov. 1.75):

"Com efeito, **a pretensão de acesso aos arquivos armazenados, notadamente aos e-mails trocados entre os investigados, não só consta da representação da Autoridade Policial, como foi expressamente autorizada na decisão do movimento 24.1, o que se denota da simples leitura do item 4.1 de seu dispositivo.**

Neste aspecto, cumpre destacar que a concomitante autorização para a interceptação telemática exigiu análise criteriosa para a verificação da adequação do caso sob investigação aos requisitos da lei de regência.

Logo, **se os elementos que subsidiaram a representação foram suficientes para justificar o monitoramento do**

**fluxo das comunicações, as exigências da Lei nº 12.965/2014 restaram automaticamente preenchidas** - já que essencialmente menos rigorosas e, diante da natureza jurídica das cautelares de obtenção de prova, nada obsta que se aplique analogicamente a Lei nº 9.296/1996.

No mais, e diferentemente do monitoramento do fluxo das comunicações, **não há qualquer irregularidade na ausência de delimitação temporal relativamente à quebra de sigilo de dados previamente armazenados** e não criptografados, consoante exemplifica a ementa de acórdão proferido no âmbito do E. Superior Tribunal de Justiça.

[jurisprudência]

Por fim, a alegação no sentido de que o acesso e a extração de dados somente foram autorizados na decisão dos autos nº 0001909-80.2024.8.16.0013 não prospera, pois o objeto daquela é o material arquivado em nuvem e/ou em dispositivos eletrônicos que fossem apreendidos durante o cumprimento dos mandados de busca, não se confundindo com o conteúdo armazenado pela Microsoft.

3. Pelo exposto, rejeito a tese de nulidade das provas obtidas e indefiro os pedidos dos movimentos 107.2 e 107.4."

No caso o que se verifica é que **ambas as plataformas "One Drive" e "Exchange" fazem parte do pacote de serviços "Microsoft 365", contudo** da atenta leitura da decisão atacada neste writ, **apenas a plataforma "One Drive" está contida, tanto na decisão quanto no requerimento da Autoridade Policial.**

De fato, o que se verifica é a **inexistência de nulidade em relação aos dados fornecidos pela empresa Microsoft** referente a detalhes do registro da conta e do número do IP de acesso quando do registro da conta, **conteúdos de e-mails**, contatos de e-mails, detalhes de registro do OneDrive, logs de IP de acesso ao OneDrive, **arquivos armazenados no OneDrive** e registros de transações no OneDrive, **no período de um ano pretérito à data da decisão atacada, porquanto abrangidos pelo teor da decisão judicial proferida, exceto o serviço Exchange, não abarcado pela decisão.**

Ao reverso do que apregoa a Defesa, a delimitação temporal exigida pela legislação vigente é imposta ao monitoramento do fluxo de comunicação, uma vez que **a decisão atacada, além do monitoramento do fluxo de e-mails, também determinou ao final (e nos termos do requerimento da autoridade policial e manifestação do Ministério Público), o acesso aos arquivos armazenados no "OneDrive", além dos registros de transações no mesmo dispositivo de armazenamento.**

[...]

A Lei nº 9.296/96, especificadamente no artigo 2º, dispõe que, para deferimento da interceptação telemática, é necessária a presença de indícios razoáveis de autoria ou participação em infração penal punida com reclusão, além da demonstração de que seja o único meio de prova disponível:

[...]

In casu, os requisitos foram atendidos, considerando a indicação da existência de indícios da prática do crime de fraude a credores (artigo 168, da Lei de Falência), o qual é punido com pena de reclusão, além de o meio de prova requerido ter se mostrado necessário para

apuração e elucidação dos fatos, considerando a forma de comunicação estabelecida entre as partes. Ainda, **estabeleceu-se a limitação temporal para a interceptação no fluxo de e-mails pelo prazo de 15 (quinze) dias**. Por fim, a decisão que decretou a medida se encontra devidamente fundamentada pelo juízo a quo.

A alegação de que a medida cautelar de quebra de sigilo telemático não foi requerida pela autoridade policial ou pelo Parquet, nem autorizada pelo Juízo a quo não encontra respaldo na realidade dos autos.

**Observando-se o teor da representação policial e da manifestação ministerial, bem como da decisão questionada, verifica-se expressa menção (e deferimento) de acesso aos arquivos pretéritos armazenados no "OneDrive". Reitera-se que os arquivos fornecidos datados de momento pretérito não se referem a fluxo de comunicações em curso.**

Consoante bem observado pelo d. Procurador de Justiça (mov. 36.1):

Segundo afirmam os impetrantes, o material telemático trazido ao feito contém e-mails trocados em período anterior ao deferimento da medida, resultando na ilegalidade das provas obtidas pela autoridade policial, pois em descumprimento à decisão judicial que autorizou a interceptação telemática pelo prazo de 15 (quinze) dias, a contar do início do monitoramento.

Assim, alegam a existência de constrangimento ilegal no fato de terem sido fornecidos e utilizados como meio de prova, dados telemáticos armazenados em arquivo remoto junto a empresa Microsoft em prazo diverso do determinado na decisão que autorizou a interceptação telemática.

Pois bem.

"Diferentemente do que ocorre em relação aos dados telemáticos da interceptação (fluxo de comunicações), os arquivos armazenados em sistema 'nuvem' ou 'drive' são regidos pela Lei nº 12.965/14 (Lei do Marco Civil da Internet), cujo regramento é menos rigoroso do que aquele apresentado pela Lei nº 9.296/96 e, por certo, como destacou a autoridade coatora, se preenchidos os requisitos dessa lei, consequentemente também preenchidos os daquela (Lei nº 12.965/14)".

[...]

Reitera-se que **a definição de prazo para observância da medida refere-se ao monitoramento do fluxo de comunicação**, porquanto para o armazenamento de dados adota-se o critério da razoabilidade e proporcionalidade, os quais, dentro dos limites da decisão atacada, não foram violados no presente caso.

[...]

Outrossim, a alegação de que o parecer técnico (mov. 38.2) anexado pela Defesa concluiu no sentido de que os e-mails pretéritos obtidos pela autoridade policial (de 2022 a 2023) não foram extraídos do sistema "One Drive" e sim, do sistema "Microsoft Exchange", pelo que constituíram elementos ilícitos, já que não abarcados pela decisão do Juízo, não tem o condão de macular a presente decisão.

Além de se referir a documento ao qual o juízo a quo não teve acesso, tratando-se de inovação recursal, reforça a ideia de que se concedeu acesso a registros de e-mails pretéritos, não vinculados ao fluxo de informações, dispensando a delimitação temporal.

Consoante bem delineado pela d. Procuradoria Geral de Justiça (mov. 50.1):

*"É que nos parece ser clara a conclusão de que o Juízo, ao deferir medida cautelar que concede acesso aos registros (e-mails) passados do investigado, não possui conhecimento técnico – e nem precisa ter – para determinar em que local (forma de armazenamento) estão acondicionados os arquivos cujo acesso se autoriza. Ou seja, parece-nos não ser possível exigir que o Juízo saiba que (ou se) os e-mails estão armazenados em 'One Drive' ou no 'Microsoft Exchange' ou em qualquer outra plataforma. Aliás, é de se observar que nem mesmo a Defesa possuía essa informação, vindo a apresentá-la apenas agora, em pedido de reconsideração não previsto em lei, com produção pericial, estranha à fase cognitiva do writ".*

Por fim, giza-se que o Habeas Corpus não se presta à produção de provas.

Nesses termos, **existindo expresse pedido policial e ministerial de acesso aos dados armazenado e tendo o Magistrado deferido a medida em observância a esses limites, não havendo que se falar em prazo para a medida impugnada, a decisão atacada se reveste de legalidade, estando em observância aos ditames da Lei nº 9.296/96, assim como da Lei do Marco Civil da Internet, inexistindo nulidades a serem reconhecidas.**

Portanto, inexistente constrangimento ilegal na decisão que autorizou o acesso ao registro da conta e do número do IP de acesso quando do registro da conta, conteúdos de e-mails, contatos de e-mails, detalhes de registro do OneDrive, logs de IP de acesso ao OneDrive, arquivos armazenados no OneDrive e registros de transações no OneDrive, exceto o que pertine ao serviço Exchange, posto que não abarcado pela decisão atacada.

Diante do exposto, é de se denegar a ordem, nos termos da fundamentação.

Sobreveio, ainda, o acórdão em embargos de declaração (fls. 937/946) que, a despeito de inadmitir o recurso oposto por terceiros, corrigiu erro material que reputou evidente. A ementa é a seguinte (fls. 937/938):

EMBARGOS DE DECLARAÇÃO EM HABEAS CORPUS. PROCEDIMENTO INVESTIGATÓRIO CRIMINAL. CRIMES, EM TESE, DE SONEGAR OU OMITIR INFORMAÇÕES OU PRESTAR INFORMAÇÕES FALSAS NO PROCESSO DE RECUPERAÇÃO JUDICIAL OU DE RECUPERAÇÃO EXTRAJUDICIAL, COM O FIM DE INDUZIR A ERRO O JUIZ, O MINISTÉRIO PÚBLICO, OS CREDORES, A ASSEMBLEIA-GERAL DE CREDORES, O COMITÊ OU O ADMINISTRADOR JUDICIAL (ART. 171 DA LEI Nº 11.001/2005) – NO ÂMBITO DO PROCESSO DE RECUPERAÇÃO JUDICIAL DO GRUPO IMCOPA. ALEGAÇÃO DE CONTRADIÇÃO ADVINDA DE ERRO MATERIAL.

INADMISSIBILIDADE: OPOSIÇÃO POR TERCEIROS INTERESSADOS. ILEGITIMIDADE EM SEDE DE HABEAS CORPUS, NÃO OBSTANTE O TEOR DA DECISÃO VICIADA POR ERRO MATERIAL AFETAR DIRETAMENTE INTERESSE JURÍDICO DO TERCEIRO PREJUDICADO: VÍTIMA. NÃO CONHECIMENTO DO RECURSO.

ERRO MATERIAL. OCORRÊNCIA. CORREÇÃO DE OFÍCIO. EQUÍVOCO PERCEPTÍVEL "PRIMO ICTU OCULI" EM MAIS DE UM PONTO DO

ACÓRDÃO. TEOR DEBATIDO EM PLENÁRIO E DEFINITIVAMENTE JULGADO PELO QUÓRUM NÃO REDUZIDOS A TERMO NA REDAÇÃO FINAL DO ACÓRDÃO. JULGAMENTO DO HABEAS CORPUS PELA INTEGRAL DENEGAÇÃO DA ORDEM, PARA DECLARAR A LICITUDE INCONDICIONAL DAS PROVAS OBTIDAS EM SEDE DE CAUTELAR DE QUEBRA DE SIGILO TELEMÁTICO, MAIS ESPECIFICAMENTE OS E-MAILS ACONDICIONADOS TANTO NO SISTEMA "ONE DRIVE" QUANTO NO "EXCHANGE", ESTE ÚLTIMO AUSENTE EM ALGUNS TRECHOS E REAFIRMADO COMO EXCLUÍDO DA DENEGAÇÃO NO DESFECHO DA FUNDAMENTAÇÃO EMBARGOS DE DECLARAÇÃO CRIME Nº 0110763-13.2024.8.16.0000 4 (INFORMAÇÃO INCORRETA). EXCLUSÃO DE PALAVRA RELEVANTE E IMPRESCINDÍVEL E INFORMAÇÃO INCORRETA QUE DEVEM SOFRER CORREÇÃO. ERRO, TAMBÉM, NA GRAFIA DO SOBRENOME DE UM DOS PACIENTES. NECESSIDADE DE CORREÇÃO IGUALMENTE. DENEGAÇÃO DA ORDEM INTEGRAL MANTIDA. EMBARGOS NÃO CONHECIDOS E, DE OFÍCIO, CORRIGIDO O ERRO MATERIAL.

#### *I. CASO EM EXAME*

1. Embargos de declaração opostos em face de acórdão que denegou a ordem em habeas corpus, no qual se discutiu a validade da quebra de sigilo telemático e a legalidade das provas obtidas, com alegação de contradição entre a fundamentação e o dispositivo da decisão, especialmente em relação à inclusão dos serviços "OneDrive" e "Exchange" da Microsoft.

#### *II. QUESTÃO EM DISCUSSÃO*

2. A questão em discussão consiste em saber se há contradição no acórdão que denegou a ordem de habeas corpus, relacionada à validade da quebra de sigilo telemático e à inclusão dos serviços "OneDrive" e "Exchange" na decisão judicial.

#### *III. RAZÕES DE DECIDIR*

3. Os embargantes, na condição de terceiros interessados, não têm legitimidade para opor embargos de declaração em habeas corpus, conforme jurisprudência do STJ, razão pela qual o recurso não deve ser conhecido.

4. O acórdão embargado apresenta erro material ao excluir a palavra "Exchange" e ao afirmar que a quebra de sigilo se restringe apenas ao serviço "OneDrive".

5. A correção do erro material é necessária para alinhar a fundamentação e o dispositivo do acórdão, garantindo a coerência da decisão.

6. O erro na autuação do nome do paciente também foi corrigido de ofício.

#### *IV. DISPOSITIVO E TESE*

7. Embargos de declaração não conhecidos, com correção de ofício do erro material. Tese de julgamento: "Nos embargos de declaração opostos por terceiros interessados em habeas corpus, a correção de erro material é admitida de ofício, mesmo diante da discussão sobre a legitimidade para interposição do recurso, desde que o erro seja evidente e não interfira no resultado do julgamento. É possível a correção de ofício do erro material para alinhar o dispositivo à fundamentação, garantindo a coerência da decisão". [...].

Eis seu teor, ora transcrito no que interessa (fls. 941/946):

*Verifica-se do acórdão que, ao reconhecer integralmente a ilicitude das provas ensejando a denegação da ordem, acabou-se, por equívoco, por excluir palavra relevante e pontuar uma exceção, ambas as situações não abarcadas no julgamento do plenário.*

*[...]*

*Pontue-se que a determinação abrangeu serviços da Microsoft utilizados ("Exchange" é um deles). conteúdos de e-mails (não restringiu de qual plataforma da Microsoft), depois é que se pontuou os do sistema "One Drive", registros, acesso e conteúdos ali armazenados. Reprise-se, o magistrado singular não está obrigado a conhecer todos os sistemas ofertados.*

*[...]*

*Outrossim, além do erro material acima retificado, há também o erro contido na autuação dos feitos, o qual reclama correção de ofício, porquanto equivocadamente registrou o sobrenome do paciente [...] como sendo [...], quando o correto, conforme procuração juntada no mov. 51.2 (nº 0026936-36.2022.8.16.0013) [...].*

Na sequência, o recurso ordinário ora em análise impugnou a validação operada, argumentando, em síntese, que

*[n]ão há como se extrair do pedido formulado pela Autoridade Policial, assim como da decisão judicial de primeiro grau que deferiu a interceptação telemática (monitoramento em tempo real dos e-mails dos recorrentes), qualquer autorização para a captura de material telemático (mensagens de e-mail) que não fosse relativo ao período de 15 dias subsequentes à sua implementação (fl. 1014).*

Da moldura fática delimitada pelas instâncias ordinárias e da documentação que instrui o remédio heroico, assiste razão à Defesa.

Conforme o entendimento do Superior Tribunal de Justiça, a *quebra de sigilo de dados estáticos [...] se diferencia das interceptações das comunicações dinâmicas* (AgRg nos EDcl no RHC n. 189.698/SC, relator Ministro Messod Azulay Neto, Quinta Turma, julgado em 17/6/2024, DJe de 20/6/2024).

Com efeito, o fluxo de comunicações pela *internet* e as comunicações privadas já armazenadas são inconfundíveis, como se extrai do art. 7º da Lei n. 12.965/2014, que, em seus incisos II e III, deixa **clara a diferenciação** entre o fluxo de comunicações e as comunicações já armazenadas:

*Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:*

*[...]*

*II - inviolabilidade e sigilo do **fluxo de suas comunicações** pela internet, salvo por ordem judicial, na forma da lei;*

*III - inviolabilidade e sigilo de suas **comunicações privadas armazenadas**, salvo por ordem judicial;*

Acerca do **regramento** envolvendo cada uma das distintas medidas:

RECURSO EM MANDADO DE SEGURANÇA. DIREITO À PRIVACIDADE E À INTIMIDADE. IDENTIFICAÇÃO DE USUÁRIOS EM DETERMINADA LOCALIZAÇÃO GEOGRÁFICA. IMPOSIÇÃO QUE NÃO INDICA PESSOA INDIVIDUALIZADA. AUSÊNCIA DE ILEGALIDADE OU DE VIOLAÇÃO DOS PRINCÍPIOS E GARANTIAS CONSTITUCIONAIS. FUNDAMENTAÇÃO DA MEDIDA. OCORRÊNCIA. PROPORCIONALIDADE. RECURSO EM MANDADO DE SEGURANÇA NÃO PROVIDO.

1. Os direitos à vida privada e à intimidade fazem parte do núcleo de direitos relacionados às liberdades individuais, sendo, portanto, protegidos em diversos países e em praticamente todos os documentos importantes de tutela dos direitos humanos. No Brasil, a Constituição Federal, no art. 5º, X, estabelece que: "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". A ideia de sigilo expressa verdadeiro direito da personalidade, notadamente porque se traduz em garantia constitucional de inviolabilidade dos dados e informações inerentes a pessoa, advindas também de suas relações no âmbito digital.

2. Mesmo com tal característica, o direito ao sigilo não possui, na compreensão da jurisprudência pátria, dimensão absoluta. De fato, embora deva ser preservado na sua essência, este Superior Tribunal de Justiça, assim como a Suprema Corte, entende que é possível afastar sua proteção quando presentes circunstâncias que denotem a existência de interesse público relevante, invariavelmente por meio de decisão proferida por autoridade judicial competente, suficientemente fundamentada, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal, sempre lastreada em indícios que devem ser, em tese, suficientes à configuração de suposta ocorrência de crime sujeito à ação penal pública.

3. Na espécie, a ordem judicial direcionou-se a dados estáticos (registros), relacionados à identificação de usuários em determinada localização geográfica que, de alguma forma, possam ter algum ponto em comum com os fatos objeto de investigação por crimes de homicídio.

4. A determinação do Magistrado de primeiro grau, de quebra de dados informáticos estáticos, relativos a arquivos digitais de registros de conexão ou acesso a aplicações de internet e eventuais dados pessoais a eles vinculados, é absolutamente distinta daquela que ocorre com as interceptações das comunicações, as quais dão acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o seu destinatário. **Há uma distinção conceitual entre a quebra de sigilo de dados armazenados e a interceptação do fluxo de comunicações. Decerto que o art. 5º, X, da CF/88 garante a inviolabilidade da intimidade e da privacidade, inclusive quando os dados informáticos constarem de banco de dados ou de arquivos virtuais mais sensíveis. Entretanto, o acesso a esses dados registrados ou arquivos virtuais não se confunde com a interceptação das comunicações e, por isso mesmo, a amplitude de proteção não pode ser a mesma.**

5. Os dispositivos que se referem às interceptações das comunicações indicados pelos recorrentes não se ajustam ao caso sub examine. **O procedimento de que trata o art. 2º da Lei n. 9.296/1996, cujas**

**rotinas estão previstas na Resolução n. 59/2008 (com alterações ocorridas em 2016) do CNJ, os quais regulamentam o art. 5º, XII, da CF, não se aplica a procedimento que visa a obter dados pessoais estáticos armazenados em seus servidores e sistemas informatizados de um provedor de serviços de internet. A quebra do sigilo de dados, na hipótese, corresponde à obtenção de registros informáticos existentes ou dados já coletados.**

6. Não há como pretender dar uma interpretação extensiva aos referidos dispositivos, de modo a abranger a requisição feita em primeiro grau, porque a ordem é dirigida a um provedor de serviço de conexão ou aplicações de internet, cuja relação é devidamente prevista no Marco Civil da Internet, o qual não impõe, entre os requisitos para a quebra do sigilo, que a ordem judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada por outros meios.

7. Os arts. 22 e 23 do Marco Civil da Internet, que tratam especificamente do procedimento de que cuidam os autos, não exigem a indicação ou qualquer elemento de individualização pessoal na decisão judicial. Assim, **para que o magistrado possa requisitar dados pessoais armazenados por provedor de serviços de internet, mostra-se satisfatória a indicação dos seguintes elementos previstos na lei: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros.** Não é necessário, portanto, que o magistrado fundamente a requisição com indicação da pessoa alvo da investigação, tampouco que justifique a indispensabilidade da medida, ou seja, que a prova da infração não pode ser realizada por outros meios, o que, aliás, seria até, na espécie - se houvesse tal obrigatoriedade legal - plenamente dedutível da complexidade e da dificuldade de identificação da autoria mediata dos crimes investigados.

8. Logo, a quebra do sigilo de dados armazenados, de forma autônoma ou associada a outros dados pessoais e informações, não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas, até porque o objetivo precípua dessa medida, na expressiva maioria dos casos, é justamente de proporcionar a identificação do usuário do serviço ou do terminal utilizado.

9. Conforme dispõe o art. 93, IX, da CF, "todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação". Na espécie, tanto os indícios da prática do crime, como a justificativa quanto à utilização da medida e o período ao qual se referem os registros foram minimamente explicitados pelo Magistrado de primeiro grau.

10. Quanto à proporcionalidade da quebra de dados informáticos, ela é adequada, na medida em que serve como mais um instrumento que pode auxiliar na elucidação dos delitos, cuja investigação se arrasta por dois anos, sem que haja uma conclusão definitiva; é necessária, diante da complexidade do caso e da não evidência de outros meios

não gravosos para se alcançarem os legítimos fins investigativos; e, por fim, é proporcional em sentido estrito, porque a restrição a direitos fundamentais que dela redundam - tendo como finalidade a apuração de crimes dolosos contra a vida, de repercussão internacional - não enseja gravame às pessoas eventualmente afetadas, as quais não terão seu sigilo de dados registrares publicizados, os quais, se não constatada sua conexão com o fato investigado, serão descartados.

11. Logo, a ordem judicial para quebra do sigilo dos registros, delimitada por parâmetros de pesquisa em determinada região e por período de tempo, não se mostra medida desproporcional, porquanto, tendo como norte a apuração de gravíssimos crimes cometidos por agentes públicos contra as vidas de três pessoas - mormente a de quem era alvo da emboscada, pessoa dedicada, em sua atividade parlamentar, à defesa dos direitos de minorias que sofrem com a ação desse segmento podre da estrutura estatal fluminense - não impõe risco desmedido à privacidade e à intimidade dos usuários possivelmente atingidos pela diligência questionada.

12. Recurso em mandado de segurança não provido. (RMS n. 62.143 /RJ, relator Ministro Rogerio Schietti Cruz, Terceira Seção, julgado em 26/8/2020, DJe de 8/9/2020 - grifamos).

AGRAVO REGIMENTAL NO RECURSO ORDINÁRIO EM HABEAS CORPUS. QUEBRA DE SIGILO TELEMÁTICO. NULIDADE. AUSÊNCIA. LEI N. 12.965/2014. NORMA MAIS ESPECÍFICA. DADOS ESTÁTICOS. DECISÕES DEVIDAMENTE FUNDAMENTADAS. OBTENÇÃO DE RIF. COMPARTILHAMENTO DIRETO ENTRE O COAF E MINISTÉRIO PÚBLICO. TEMA 990. BUSCA ESPECULATIVA. NÃO EVIDENCIADA. AGRAVO REGIMENTAL DESPROVIDO.

**1. Inaplicabilidade das disposições da Lei n. 9.296/1996, pois a Lei n. 12.965/2014, por ser mais específica, incide em detrimento daquela à presente hipótese, que diz respeito a dados estáticos, ou seja, a conversas já armazenadas nas contas de e-mail, e não acesso em tempo real. Não havendo interceptação, mas acesso a informações armazenadas, a quebra de sigilo aqui determinada não está abrangida pela lei que disciplina a inviolabilidade das comunicações telefônicas (Lei n. 9.296/1996), incidindo à hipótese a Lei do Marco Civil (Lei n. 12.965/2014), que assegura a inviolabilidade de conversas particulares e o sigilo de comunicações privadas armazenadas, exceto por ordem judicial.**

2. Decisões que deferiram a quebra do sigilo de conteúdos de comunicação armazenados em contas de e-mails que contêm suficiente fundamentação, diante dos fundados indícios de ocorrência de ilícitos - fraudes em licitação, peculato, corrupção, formação de cartel e organização criminosa supostamente praticados por Servidores Públicos da Prefeitura Municipal de Orlândia - SP em conluio com alguns empresariados locais -, com descrição individualizada da suposta conduta criminosa de cada um dos envolvidos.

[...]

4. Ausência de demonstração, no caso, da nefasta prática denominada de pesca predatória (fishing expedition), na medida em que não evidenciada a busca especulativa por provas a serem produzidas em face dos investigados.

5. *Agravo regimental desprovido.* (AgRg no RHC n. 189.011/SP, relator Ministro Ribeiro Dantas, Quinta Turma, julgado em 18/3/2024, DJe de 21/3/2024 - grifamos).

Acerca do estabelecimento de **prazo de duração** para cada medida:

AGRAVO REGIMENTAL NO RECURSO EM HABEAS CORPUS. PROCESSO PENAL. QUEBRA DE SIGILO DE DADOS ARMAZENADOS EM APARELHOS CELULARES. MEDIDA DEVIDAMENTE FUNDAMENTADA. INVESTIGAÇÃO DE CRIMES GRAVES. DECISÃO JUDICIAL AMPARADA EM ELEMENTOS INFORMATIVOS IDÔNEOS. INEXISTÊNCIA DE ILEGALIDADE FLAGRANTE. REEXAME FÁTICO-PROBATÓRIO. IMPOSSIBILIDADE NA VIA ELEITA. AGRAVO REGIMENTAL NÃO PROVIDO.

1. **A jurisprudência desta Corte entende que a decisão judicial que autoriza a quebra de sigilo de dados armazenados, nos termos da Lei n. 12.965/2014, não está sujeita à limitação temporal, diferentemente do que ocorre com a interceptação de comunicações em curso, prevista na Lei n. 9.296/1996.**

2. No caso concreto, a medida de quebra de sigilo de dados armazenados foi devidamente fundamentada em relatório policial que apontou indícios consistentes da prática de tráfico de drogas, porte ilegal de arma de fogo e participação em organização criminosa, com base em denúncias anônimas corroboradas por informante identificado, imagens e dados de inteligência. Demonstrada a vinculação entre os fatos investigados e os aparelhos eletrônicos apreendidos, a medida revelou-se necessária e proporcional, não se tratando de diligência genérica ou especulativa (*fishing expedition*).

3. A revisão das conclusões adotadas pelas instâncias ordinárias quanto à idoneidade da fundamentação da medida judicial demandaria reexame de provas, o que não é cabível na via estreita do *habeas corpus*.

4. *Agravo regimental não provido.* (AgRg no RHC n. 215.014/SC, relator Ministro Reynaldo Soares da Fonseca, Quinta Turma, julgado em 20/5/2025, DJEN de 28/5/2025 - grifamos).

AGRAVO EM RECURSO EM HABEAS CORPUS. OPERAÇÃO PROGRESSO. ORGANIZAÇÃO CRIMINOSA, ASSOCIAÇÃO CRIMINOSA E FALSIDADE IDEOLÓGICA. INTERCEPTAÇÃO TELEFÔNICA. DENÚNCIA ANÔNIMA. ART. 2º DA LEI N. 9.296/1996. REALIZAÇÃO DE DILIGÊNCIAS PRELIMINARES. POSSIBILIDADE. PRECEDENTE. **QUEBRA DE SIGILO DE DADOS TELEMÁTICOS. DADOS ESTÁTICOS. AUSÊNCIA DE LIMITAÇÃO TEMPORAL.** QUEBRA DE SIGILO BANCÁRIO SEM AUTORIZAÇÃO JUDICIAL. NÃO OCORRÊNCIA. PRECEDENTE DO STJ. REQUISICÃO DE DADOS NÃO ABRANGIDOS PELO SIGILO FISCAL. POSSIBILIDADE. PRECEDENTE. NULIDADE. RECEBIMENTO DA DENÚNCIA. DESNECESSIDADE DE FUNDAMENTAÇÃO EXAURIENTE. PRECEDENTE. VIOLAÇÃO DA SÚMULA VINCULANTE 24/STF. RAZÕES EXPRESSAS NO RHC N. 151.007/PR. *Agravo regimental improvido.* (AgRg no RHC n. 200.321/PR, relator Ministro Sebastião Reis Júnior, Sexta Turma, julgado em 26/2/2025, DJEN de 10/3/2025 - grifamos).

Assim, trata-se de **duas hipóteses completamente distintas**, incidentes sobre contextos e objetos diferentes, com graus diversos de afetação do resguardo à intimidade e ao sigilo das comunicações e regência por normativas que não se confundem - inclusive quanto à necessidade de imposição de prazo de duração.

A **interceptação** comporta o monitoramento em tempo real das comunicações (no caso, por *e-mails*), incidindo sobre fluxo dinâmico de dados e encontrando disciplina na Lei n. 9.296/1996 - que estabelece prazo máximo de duração para a medida (15 - quinze - dias, renovável por igual tempo uma vez comprovada a indispensabilidade da prova - art. 5º).

Já a **quebra de sigilo** de dados abrange o acesso retrospectivo, incidindo sobre dados estáticos, já armazenados (e não em fluxo de comunicações). Diante do postulado interpretativo da especialidade, a Lei n. 12.965/2014 encampa os contornos legais da medida, não havendo, conforme a jurisprudência deste Sodalício, imposição legal de limitação temporal para sua duração, embora estabeleça o art. 22, parágrafo único, inciso III da normativa a necessidade de indicação, ao menos, do *período ao qual se referem os registros* para requerimento do fornecimento de registros de conexão ou registro de acesso a aplicações de *internet*.

Quanto a esse ponto, aliás, é elucidativa a *ratio decidendi* trazida no voto da Relatora, Ministra Laurita Vaz, no **RHC n. 99.735/SC** (Sexta Turma, julgado em 27/11/2018, DJe de 12/12/2018), em que, versando a respeito da inviabilidade da utilização de espelhamento via *WhatsApp Web* como meio de prova, salienta justamente as **diferenças entre as hipóteses legais de interceptação e quebra de sigilo**, bem como a **inexistência de uma medida que abarque ambas** (grifamos):

*Em segundo lugar, ao contrário da interceptação telefônica, que tem como objeto a escuta de conversas realizadas apenas depois da autorização judicial (ex nunc), o espelhamento via QR Code viabiliza ao investigador de polícia acesso amplo e irrestrito a toda e qualquer comunicação realizada antes da mencionada autorização, operando efeitos retroativos (ex tunc). Em termos técnico-jurídicos, o espelhamento seria melhor qualificado como um tipo híbrido de obtenção de prova consistente, a um só tempo, em interceptação telefônica (quanto às conversas ex nunc) e em quebra de sigilo de e-mail (quanto às conversas ex tunc). Não há, todavia, ao menos por agora, previsão legal de um tal meio de obtenção de prova híbrido.*

Trata-se, pois, de hipóteses técnica e juridicamente **inconfundíveis**.

Passo, assim, à análise do caso concreto.

Consta, às fls. 24/32, o *pedido de medidas cautelares* formulado pela autoridade policial, assim indicado no campo de identificação do documento (grifamos):

O corpo do documento conta com o capítulo **II - DOS PEDIDOS** (fl. 28), dividido em dois subitens: **DA INTERCEPTAÇÃO TELEMÁTICA** (fls. 28/30) e **DA AÇÃO CONTROLADA** (fls. 30/31). Transcreve-se o teor do primeiro (grifamos):

**DA INTERCEPTAÇÃO TELEMÁTICA**

Assim sendo, pelo que se conclui, os **requisitos exigidos pela Lei n. 9296/96 para o deferimento da interceptação telemática dos investigados** encontram-se presentes, senão vejamos.

Os indícios até o presente momento são contundentes acerca da existência de conduta criminosas e de sua autoria, mormente porque existem indícios verossímeis que evidenciam a gestão de grupo empresarial que está em recuperação judicial por pessoas diversas daquelas que constam em seu contrato social.

A conduta dos investigados se amolda perfeitamente ao tipo legal previsto no artigo 168 da Lei 11.101/05, qual seja a prática de ato fraudulento, durante a recuperação judicial que possa resultar em prejuízo aos credores ou vantagem para si ou para outrem. Ora, se os reais administradores do grupo empresarial estão permitindo que terceiros exerçam a gestão e por sua vez estes terceiros estão exercendo devidamente tais atos, sem sombra de dúvida esta conduta poderá resultar em prejuízo aos credores, que não poderão alcançar os administradores de fato que estão atuando sob o manto da camuflagem.

Destaca-se ainda a **necessidade de utilização da presente técnica de investigação**, uma vez que **as tratativas e respectivas apreciações estão sendo mantidas por e-mails**, o que dificulta a obtenção de elementos de informação por outros meios. Desta feita, resta demonstrado que a **prova não pode ser obtida por outro meio senão pela interceptação telemática**.

Além da necessidade manifesta de utilização da interceptação telemática, **também estão presentes os demais requisitos exigidos pela Lei nº 9.296/96**, quais sejam os indícios razoáveis de autoria e a punição do fato por pena de reclusão, o que se consubstancia pelo conteúdo dos e-mails trocados entre os investigados e pelas manifestações de gestão dos mesmos e pela previsão legal do artigo 168 da Lei 11.101/05 que prevê pena de reclusão de 3 a 6 anos, além de multa.

Há que se destacar que um dos e-mails objeto do presente pedido de interceptação é utilizado pelo patrono do Grupo Imcopa e como advogado há que se respeitar a sua esfera de atuação, porém a Lei 8.906/94 é clara ao disciplinar que é um direito do advogado ter respeitada a inviolabilidade de suas correspondência eletrônica e telemática, salvo quando existirem indícios de autoria e materialidade de crime por parte do advogado, o que se demonstra na presente situação uma vez que o próprio causídico informa ao administrador judicial que os anexos referentes ao edital de venda das plantas do Grupo Imcopa estariam sendo preparados pela R2C Investimentos.

Ora, tal manifestação demonstra o conhecimento da administração do grupo por terceiros e mais ainda, instrumentaliza a gestão do grupo empresarial por pessoas estranhas ao contrato social, o que se traduz em efetiva co-autoria da prática do ato fraudulento em investigação. Desta feita, resta adequado o afastamento do sigilo telemática também do patrono do Grupo Imcopa por se mostrar imprescindível às investigações.

DESTA FEITA, salvo melhor juízo, **presentes os requisitos legais** e com o intuito de dar prosseguimento às investigações, e principalmente diante da imprescindibilidade da medida para colheita de provas que por outro meio não seriam coletadas, vem esta Autoridade Policial **REPRESENTAR para que seja autorizada a INTERCEPTAÇÃO TELEMÁTICA dos e-mails a seguir descritos:**

[...]

A **presente interceptação**, uma vez deferida, deverá ser **atendida pela Microsoft que fornecerá** os dados das contas, por meio de seu portal, detalhes de registro, informações de faturamento e transações de faturamento, acaso existentes, registros dos números de IP (Internet Protocol) no momento do login dos usuários, serviços da Microsoft utilizados, detalhes do registro da conta e do número do IP de acesso quando do registro da conta, **conteúdos de e-mail**, contatos de e-mail, detalhes de registro do OneDrive, logs de IP de acesso ao OneDrive, **arquivos armazenados no One Drive** e registros de transações no OneDrive.

Observa-se, desse modo, que **a medida requerida foi efetivamente a interceptação telemática**, tanto que o substrato legal cujo atendimento se buscou evidenciar foi a **Lei n. 9.296/1996**. O requerimento não faz nenhuma alusão à Lei n. 12.965/2014, regente da modalidade diversa que é a quebra de sigilo de dados.

A manifestação do Ministério Público, à fl. 69, reforça tal circunstância, requerendo complementação de informações para atendimento à Resolução n. 59 do CNJ, que versa, justamente, a respeito da interceptação:

*Meritíssimo(a) Juiz(a):*

I. Trata-se de **pedido de interceptação telemática** a de ação controlada formulado pela autoridade policial, referente aos fatos apurados nos autos de inquérito policial n° 0026936-36.2022.8.16.0013.

II. Preliminarmente, requer seja intimada a d. autoridade policial, a fim de complementar as informações, em conformidade com as normas estatuídas pela **Resolução 59 do Conselho Nacional de Justiça - CNJ**, para que se manifeste a fim de:

a) **especificar o prazo da interceptação telemática;**

c) **indicar a autoridade/agentes policiais responsáveis pela investigação e que terão acesso às informações, com o respectivo meio de contato (e-mail).** (grifamos)

Como cediço, a Resolução n. 59/2008, do CNJ, de acordo com sua ementa,

*[d]isciplina e uniformiza as rotinas visando ao aperfeiçoamento do **procedimento de interceptação de comunicações telefônicas e***

**de sistemas de informática e telemática** nos órgãos jurisdicionais do Poder Judiciário, a que se refere a **Lei nº 9.296**, de 24 de julho de 1996.

A resposta da autoridade policial à diligência consta a fl. 76 (grifamos):

1 - Trata-se de **pedido de interceptação telemática** a de ação controlada formulado por esta Autoridade policial, referente aos fatos apurados nos autos de inquérito policial nº 0026936-36.2022.8.16.0013.

2 - Após a apresentação, o Ministério Público se manifestou no sentido da necessidade de complementação das informações, em especial a respeito do prazo de duração da medida e dos responsáveis por seu acompanhamento.

3 - **No que se refere ao prazo de interceptação**, esta Autoridade Policial esclarece que o prazo da duração, caso a medida seja deferida, deverá ser de **15 (quinze) dias, conforme prevê a Lei 9296/96 sem prejuízo de eventual prorrogação** se as circunstâncias evidenciarem a necessidade, o que será objeto de nova manifestação desta Autoridade Policial. Em relação à Ação Controlada, esta também deverá perdurar pelo mesmo período tendo em vista que o objetivo da mesma é subsidiar o acompanhamento das informações com a possibilidade de intervenção tardia em eventual flagrante.

4 - A **responsabilidade da presente interceptação** será desta Autoridade Policial, Leandro Farnese Teixeira, e-mail del.lfteixeira@pc.pr.gov.br e será implementada por meio do portal de atendimento à autoridades da Microsoft. A implementação ocorre após o deferimento, com o encaminhamento da decisão por meio da plataforma na página de acesso com login desta Autoridade Policial e uma vez analisada a decisão pelo provedor, os dados são liberados para download, providência esta que será efetivada por esta Autoridade Policial diretamente.

O Ministério Público se manifestou quanto ao requerimento de fls. 82 /91, cabendo a transcrição dos fundamentos lançados pelo Parquet a respeito da medida em debate (grifamos):

Trata-se de **representação de interceptação de dados telemáticos** e ação controlada formulada pela autoridade policial da Divisão de Combate à Corrupção - Núcleo de Curitiba, com base no Relatório de Investigação referente ao IP nº 260057/2022 (autos nº 0026936-36.2022.8.16.0013), lavrado pelos agentes da DECCOR - Divisão Estadual de Combate à Corrupção - Núcleo Curitiba.  
[...]

**Da interceptação das comunicações telefônicas e telemática**

A **Lei 9.296/96** regulamentou o inciso XII, parte final, do artigo 5o da Constituição Federal, cujo texto garante, como regra, o sigilo das correspondências e telecomunicações. O inciso constitucional permite, excepcionalmente, a quebra do sigilo, mediante o preenchimento de

dois requisitos: 1) que atenda as hipóteses e a forma prevista em lei; e 2) que a finalidade seja investigação criminal ou produção de prova em processo penal.

O artigo 2º da **Lei n.º 9.296/96** estabelece que a **interceptação de comunicações telefônicas de qualquer natureza** será autorizada nos casos em que estiverem presentes: a) indícios razoáveis da participação dos investigados na prática de infração penal; b) a interceptação se mostrar necessária para a comprovação da participação dos investigados, não havendo outro meio adequado de prova a ser produzido; c) a infração em tese praticada é punida com reclusão.

A partir das informações elencadas pela autoridade policial, verifica-se que estão presentes o *fumus comissi delicti* e o *periculum in mora* necessários para a concessão da medida.

As informações preliminares encaminhadas pela d. autoridade policial e obtidas através de investigações são fidedignas e garantem plausibilidade ao pedido, pois configuram fortes indícios da prática de delitos de fraude a credores e outros correlatos, sendo a medida pleiteada imprescindível para a apuração destes, bem como para a identificação, qualificação e localização das pessoas envolvidas nos crimes.

Considerando que foram executadas as ações possíveis com os recursos disponíveis, verifica-se a imprescindibilidade da autorização de outros meios para obtenção de dados e informações essenciais ao sucesso da investigação e consequente prevenção/coibição aos ilícitos supramencionados.

Oportuno registrar, ainda, que o **deferimento do presente requerimento não encontra obstáculo nas normas estatuídas pela Resolução 59, do Conselho Nacional de Justiça - CNJ**, uma vez que: a) o **usuário que se pretende interceptar** foi devidamente especificado; b) o **prazo de interceptação** é aquele legalmente previsto - 15 (quinze) dias; c) há precisa indicação da autoridade requerente e das autoridades policiais responsáveis pela investigação e que terão acesso às informações.

Registre-se que em um Estado Democrático de Direito a inviolabilidade foi erigida ao status de direito fundamental, justificando a sua violação apenas em circunstâncias excepcionais, legalmente previstas e necessárias à preservação de princípios jurídicos relevantes. Na hipótese, diante das regras legais já mencionadas, e, diante, também, dos princípios jurídicos envolvidos, em um juízo de ponderação entre os interesses em conflito, conclui-se que, no caso concreto, estão presentes os requisitos exigidos pela legislação, justificando-se o deferimento do pedido.

Isto posto, preenchidos os requisitos estabelecidos, o Ministério Público **manifesta-se pelo deferimento do pedido de interceptação de dados telemáticos das contas de e-mail abaixo elencadas**, a ser atendida **pela Microsoft que fornecerá** os dados das contas, por meio de seu portal, detalhes de registro, informações de faturamento e transações de faturamento, acaso existentes, registros dos números de IP (Internet Protocol) no momento do login dos usuários, serviços da Microsoft utilizados, detalhes do registro da conta e do número do IP de acesso quando do registro da conta, **conteúdos de e-mail**, contatos de e-mail, detalhes de registro do OneDrive, logs de IP de acesso ao OneDrive, **arquivos**

**armazenados no One Drive e registros de transações no One Drive, contados da data de implementação da medida até os 15 (quinze) dias seguintes a esta:**  
[...].

A manifestação ministerial se debruça tão somente, no particular, sobre a medida de **interceptação** das comunicações telemáticas, com lastro na **Lei n. 9.296/1996**.

A peça do *Parquet*, ainda, **de forma expressa, circunscreve temporalmente o pedido de interceptação de dados telemáticos, inclusive com o fornecimento de [...] conteúdos de e-mail, contatos de e-mail, detalhes de registro do OneDrive, logs de IP de acesso ao OneDrive, arquivos armazenados no One Drive e registros de transações no One Drive, ao período entre a data de implementação da medida até os 15 (quinze) dias seguintes a esta.**

Evidente, mais uma vez, que se está a tratar de medida **prospectiva**, abrangendo, conforme a terminologia utilizada no precedente desta Sexta Turma, de relatoria da Min. Laurita Vaz, incidência *ex nunc*, mas **não ex tunc**.

Assim, desde o requerimento, a medida postulada pela autoridade policial, que teve concordância do Ministério Público, **não foi** a quebra de sigilo de dados estáticos, mas, sim, a interceptação de dados pelo período **futuro** de 15 (quinze) dias.

A decisão judicial que se seguiu pontuou (fls. 96/103 - grifamos):

1. Trata-se de **representação formulada** por Leandro Farnese Teixeira - Autoridade Policial da Divisão de Combate à Corrupção desta Capital - **pela implementação de interceptação telemática de e-mails** expressamente delineados no requerimento inaugural, isto para a apuração do crime previsto no artigo 168 da Lei nº 11.101/2005 (movimentos 1.1/1.2).

A Autoridade Policial alegou, em síntese, que [...] estariam praticando atos criminosos no bojo da Ação de Recuperação Judicial nº 0000155-53.2013.8.16.0025, em trâmite perante a 1ª Vara de Falências e de Recuperação Judicial deste Foro Central - a qual trata do Grupo IMCOPA -, bem como que **a medida pleiteada é o único meio possível para a coleta de outras provas** da materialidade delitiva, da autoria e **da eventual mobilização dos investigados para prejudicar a investigação**.

Atuando no feito, depois de **informados os períodos para a interceptação** e a ação controlada, a ilustre representante do **Ministério Público se manifestou pelo deferimento da representação** (movimento 16.1 e 20.1). Assim, vieram os autos conclusos.

[...]

Portanto, e de acordo com os documentos e informações que instruem o pedido, verifico a robustez das investigações procedidas, bem como a gravidade dos fatos em apuração, observando que, no caso vertente, prevalece o interesse da sociedade na apuração da verdade (princípio da proporcionalidade).

Nota-se que as medidas investigativas utilizadas até o momento não possuem mais o condão de permitir a evolução da investigação, sendo o **monitoramento das comunicações eletrônicas o único caminho investigativo** que possibilitará novos dados para desbaratar as atividades delituosas encetadas e identificar os autores.

Segundo o disposto no artigo 5º, inciso XII, da Constituição Federal, que vislumbra o rol de direitos e garantias fundamentais de todo cidadão, 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 plena.

Ainda no que pertine à legislação de regência, verifico que os **requisitos para a validade da interceptação** estão elencados no artigo 2º da **Lei nº 9.296/96**.

[...]

O crime que está sendo investigado é de elevada gravidade e apenado com reclusão, conforme determinado pela legislação de regência.

Por outro lado, o acesso a dados, documentos e informações personalíssimas é autorizado em procedimentos investigatórios, consoante já previsto na **Lei nº 9.034/95**, bem como na **Lei nº 9.296/96**, a qual regulamentou o artigo 5º, inciso XII, parte final, da Constituição Federal, conforme, inclusive, entendimento encampado pelo Superior Tribunal de Justiça, nos termos do julgado adiante transcrito.

[...]

Por derradeiro, conclui-se que foram preenchidos todos os requisitos para o deferimento dos pleitos, afigurando-se necessárias as medidas para comprovar os crimes e a participação efetiva das pessoas envolvidas.

4. Em face ao exposto:

4.1. **Autorizo a interceptação telemática pelo prazo de 15 (quinze) dias passível de prorrogação, dos endereços de e-mails abaixo listados, determinando a expedição de ofício à MICROSOFT para que, no prazo de 24 (vinte e quatro) horas, inicie o monitoramento dos e-mails e forneça os dados das contas - por meio de seu portal - detalhes de registro, informações de faturamento e transações de faturamento acaso existentes, registros dos números de IP (Internet Protocol) no momento do login dos usuários, serviços da Microsoft utilizados, detalhes do registro da conta e do número do IP de acesso quando do registro da conta, conteúdos de e-mails, contatos de e-mails, detalhes de registro do One Drive, de IP de acesso ao One Drive, arquivos armazenados no One Drive e registros de transações no One Drive, ficando expressamente vedada a interceptação de endereços eletrônicos não discriminados na presente decisão.**

[...]

4.2. AUTORIZO a utilização de ação controlada, nos moldes da Lei nº 12.850/2013.

4.3. AUTORIZO o Chefe de Secretaria senhor José Carlos Bulgari Júnior a realizar os atos processuais necessários ao trâmite dos presentes autos, pessoalmente ou por servidor por ele indicado.

***O presente feito deverá tramitar em segredo de justiça e observar de forma estrita as disposições estatuídas na Resolução nº 59, do Conselho Nacional de Justiça.***

Verifica-se, portanto, que a decisão que deferiu a medida também o fez (e não poderia ser diferente, dadas as balizas do pedido) tão somente quanto à pleiteada **interceptação telemática**, regida pela **Lei n. 9.296/1996**, expressamente invocada (assim como a Resolução 59 do CNJ) como base normativa para tanto.

Também aqui nenhuma menção se fez à Lei n. 12.965/2014, regente da modalidade diversa que é a quebra de sigilo de dados.

Aliás, não se colhe de nenhum dos documentos (requerimento policial, manifestação do Ministério Público e deferimento da medida) alusão expressa a dados **pretéritos**, tampouco a delimitação ao **período de um ano pretérito à data da decisão atacada** (expressões utilizadas no acórdão).

A **nomenclatura**, o **prazo legal** fixado, a **norma jurídica** subjacente, os limites do **requerimento** e da **concordância** do Ministério Público, enfim, tudo indica que se tratou de pedido e deferimento de medida específica: a **interceptação de dados telemáticos**, a qual, repita-se, é prospectiva, com abrangência *ex nunc* durante prazo determinado, sendo, assim, **inconfundível** com a quebra de sigilo de dados estáticos (retroativa, com abrangência *ex tunc*).

Contudo, conforme se verifica do Ofício 458/23 AMM, a autoridade policial informou ao juízo, em 15/09/2023, que,

*[E]m 04/08/2023, a Microsoft informou que o monitoramento de uma conta espelho não pode ser implementado quando o tipo de conta é "enterprise", em virtude do tratamento de dados.*

*[...]*

*Todavia, em 11/09/2023, a Microsoft entrou em conta reiterando que as contas vinculadas a contratos "enterprise" estão sujeitas a uma série de particularidades técnicas e de compromissos assumidos pela própria Microsoft com o cliente, decorrentes de entendimentos sobre o tratamento de dados.*

*Assim, esta Autoridade Policial consignou que a medida deveria ser cumprida respeitando o sigilo, pedido que foi acatado pela Microsoft, ressaltando que esta só comunicará seus clientes quando houver a baixa do sigilo da medida cautelar.*

*Também, em 12/09/2023 a Microsoft concluiu pelo atendimento da medida Microsoft Law Enforcement Portal, com identificador ED LNS-546520-V6S2C4, o que resultou no **download de aproximadamente 51GB de dados, que já foram extraídos** e que foram encaminhados para análise pelo Setor de Investigação desta Especializada.*

*Ainda, cabe ressaltar que a **Microsoft**, em razão de exigências técnicas, esclareceu que **não poderia cumprir o monitoramento em tempo real das contas de e-mail**, porém tal medida **não gerou prejuízo para a investigação, uma vez que a análise superficial***

**(preliminar) dos dados obtidos evidenciou que os e-mails utilizados nas contas estão disponibilizados nas respectivas pastas.**

*Por fim, informo ainda, que não será necessária a prorrogação de 15 dias da referida interceptação telefônica, uma vez que **os arquivos já foram obtidos e não está ocorrendo monitoramento em tempo real.** Destacando que esta medida cautelar ficará em aberto durante o período necessário para análise, culminando com a apresentação do relatório pelo setor de investigação, ocasião em que esta Autoridade Policial voltará a se manifestar à respeito dos elementos de informação obtidos.*

Assim, ficou demonstrado que **(i) não houve** a interceptação do fluxo de dados/monitoramento em tempo real (interceptação telemática) pela Microsoft e **(ii) foram fornecidos 51GB de dados** pela Microsoft, contendo os e-mails utilizados nas contas (que só podem ser dados estáticos já armazenados, diante do item (i) anterior).

Ou seja: **operou-se, na prática, a quebra de sigilo de dados, e não interceptação de dados telemáticos.**

Ocorre que, diversamente do que concluiu a origem, como visto acima, a medida requerida, que teve concordância do Ministério Público e foi deferida, **não foi** essa, e sim, **tão somente**, a interceptação, a qual, conforme a prova documental, não foi levada a efeito.

Além disso, como apontado pela jurisprudência deste Superior Tribunal, as medidas são **inconfundíveis**, não havendo previsão legal de cautelar híbrida apta a cumprir as duas funções.

Em se tratando de medida estatal que incide sobre garantias do cidadão, não parece razoável que se confira pura e simplesmente fungibilidade entre institutos diversos, com requisitos, fundamentos e efeitos distintos, para que, diante de noticiada impossibilidade técnica, de forma automática, transforme-se a medida prospectiva em retroativa.

Ante o exposto, **dou provimento** ao recurso para **conceder a ordem** de *habeas corpus*, declarando nulos os elementos colhidos a partir da quebra de sigilo telemático dos recorrentes nos autos da Medida Cautelar n. 0016436-71.2023.8.16.0013, determinando, nos termos do art. 157, e parágrafos, do CPP, seu desentranhamento do inquérito, bem como das provas delas derivadas.

É o voto.

CERTIDÃO DE JULGAMENTO  
SEXTA TURMA

Número Registro: 2025/0127658-3

PROCESSO ELETRÔNICO

RHC 214.389 / PR  
MATÉRIA CRIMINAL

Números Origem: 00164367120238160013 00269363620228160013 00341250220258160000  
00722610520248160000 01107631320248160000 01118856120248160000  
1107631320248160000 1118856120248160000  
111885612024816000000341250220258160000 164367120238160013  
269363620228160013 341250220258160000 722610520248160000

PAUTA: 12/08/2025

JULGADO: 12/08/2025  
SEGREGADO DE JUSTIÇA

**Relator**

Exmo. Sr. Ministro **OTÁVIO DE ALMEIDA TOLEDO (DESEMBARGADOR  
CONVOCADO DO TJSP)**

Presidente da Sessão

Exmo. Sr. Ministro SEBASTIÃO REIS JÚNIOR

Subprocurador-Geral da República

Exmo. Sr. Dr. ARTHUR DE BRITO GUEIROS SOUZA

Secretário

Bel. ELISEU AUGUSTO NUNES DE SANTANA

**AUTUAÇÃO**

RECORRENTE : R D G  
RECORRENTE : R M M  
ADVOGADOS : SERGIO ROSENTHAL - SP114806  
JULIANO JOSE BREDAS - PR025717  
ADVOGADA : CARINA QUITO - SP183646  
ADVOGADOS : NICOLE TRAUZYNSKI MUFFONE - PR041301  
ANTONIO GLAUCIUS DE MORAIS - DF012308  
ADRIANO SERGIO NUNES BRETAS - PR038524  
GABRIEL GARCIA SOARES - PR118659  
RECORRIDO : MINISTÉRIO PÚBLICO DO ESTADO DO PARANÁ  
ADVOGADO : JOAO PAULO DE OLIVEIRA BOAVENTURA - DF031680  
INTERES. : T B L  
INTERES. : W C M F  
INTERES. : M D L E R J  
ADVOGADOS : IGOR ARTHUR RAYZEL - PR075656  
OTTO MEDEIROS DE AZEVEDO JUNIOR - DF047761  
IGOR DOS SANTOS JAIME - DF054584  
BENO FRAGA BRANDAO - PR020920  
THIAGO TURBAY FREIRIA - DF057218  
JOAO PAULO DE OLIVEIRA BOAVENTURA - DF031680  
ADVOGADOS : EDUARDA CANDIDO ZAPPONI - DF064353  
LUCAS FISCHER DE MORAES - PR106737  
TRACY JOSEPH REINALDET DOS SANTOS - DF069913  
MATTEUS BERESA DE PAULA MACEDO - DF070111  
IGOR CUSTODIO DE ARAUJO FERREIRA - DF080602

ASSUNTO: DIREITO PENAL - Crimes Previstos na Legislação Extravagante - Crimes Falimentares

**CERTIDÃO**

Certifico que a egrégia SEXTA TURMA, ao apreciar o processo em epígrafe na sessão realizada nesta data, proferiu a seguinte decisão:

Após o voto do Sr. Ministro Relator dando provimento ao recurso para conceder a

**CERTIDÃO DE JULGAMENTO  
SEXTA TURMA**

Número Registro: 2025/0127658-3

**PROCESSO ELETRÔNICO**

**RHC 214.389 / PR**  
MATÉRIA CRIMINAL

ordem, pediu vista antecipada o Sr. Ministro Sebastião Reis Junior. Aguardam os Srs. Ministros Og Fernandes, Rogerio Schietti Cruz e Antonio Saldanha Palheiro.



## SUPERIOR TRIBUNAL DE JUSTIÇA

RECURSO EM HABEAS CORPUS Nº 214389 - PR (2025/0127658-3)

**RELATOR** : **MINISTRO OTÁVIO DE ALMEIDA TOLEDO**  
**(DESEMBARGADOR CONVOCADO DO TJSP)**

**RECORRENTE** : R D G

**RECORRENTE** : R M M

**ADVOGADOS** : SERGIO ROSENTHAL - SP114806  
JULIANO JOSE BREDAS - PR025717  
CARINA QUITO - SP183646  
NICOLE TRAUZYNSKI MUFFONE - PR041301  
ADRIANO SERGIO NUNES BRETAS - PR038524  
GABRIEL GARCIA SOARES - PR118659  
VALESKA TEIXEIRA ZANIN MARTINS - SP153720  
ANTONIO GLAUCIUS DE MORAIS - DF012308

**RECORRIDO** : MINISTÉRIO PÚBLICO DO ESTADO DO PARANÁ

**ADVOGADO** : JOAO PAULO DE OLIVEIRA BOAVENTURA - DF031680

**INTERES.** : T B L

**INTERES.** : W C M F

**INTERES.** : M D L E R J

**ADVOGADOS** : BENO FRAGA BRANDAO - PR020920  
EDUARDA CANDIDO ZAPPONI - DF064353  
IGOR ARTHUR RAYZEL - PR075656  
IGOR CUSTODIO DE ARAUJO FERREIRA - DF080602  
IGOR DOS SANTOS JAIME - DF054584  
JOAO PAULO DE OLIVEIRA BOAVENTURA - DF031680  
MATTEUS BERESA DE PAULA MACEDO - DF070111  
OTTO MEDEIROS DE AZEVEDO JUNIOR - DF047761  
THIAGO TURBAY FREIRIA - DF057218  
TRACY JOSEPH REINALDET DOS SANTOS - DF069913

### VOTO-VISTA

Trata-se de recurso em *habeas corpus* interposto por R D G e R M M contra o acórdão do TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ (*Habeas Corpus* n. 0072261-05.2024.8.16.0000), assim ementado (fl. 731):

*HABEAS CORPUS – CRIMES LEI Nº 11.101/05 – QUEBRA DE SIGILO TELEMÁTICO – LEGALIDADE DA PROVA – OBSERVADOS OS REQUISITOS LEGAIS PARA DEFERIMENTO DA ORDEM – PRAZO PARA ACESSO A E-MAILS – ACESSO DETALHES DO REGISTRO DA CONTA E DO NÚMERO DO IP DE ACESSO QUANDO DO REGISTRO DA CONTA, CONTEÚDOS DE E-MAIL, CONTATOS DE E-MAIL, DETALHES DE REGISTRO DO ONEDRIVE, LOGS DE IP DE ACESSO AO ONEDRIVE, ARQUIVOS ARMAZENADOS NO ONE DRIVE E REGISTROS DE TRANSAÇÕES NO ONEDRIVE – POSTULADO DA PROPORCIONALIDADE – IMPOSSIBILIDADE DE PRODUÇÃO DE PROVAS NA VIA DO – ORDEM DENEGADA.*

Narram os autos que, em razão de notícia-crime na qual foi narrada a ocorrência dos delitos de fraude e abuso na administração de sociedade por ações, associação criminosa (arts. 177, I, e 288 do Código Penal) e indução a erro no processo de recuperação judicial (art. 171 da Lei n. 11.101/2005), foi instaurado o Inquérito Policial n. 0026936- 36.2022.8.16.0013 - 260057/2022, no âmbito da Divisão Estadual de Combate à Corrupção - Núcleo de Curitiba/PR (fl. 347 do apenso 1).

No decorrer da investigação, a autoridade policial representou pela interceptação do sigilo telemático e ação controlada perante a 5ª Vara Criminal da comarca de Curitiba/PR (fls. 24/32), que deferiu o pleito (fls. 93/103 - Medida Cautelar n. 0016436-71.2023.8.16.0013).

Por conseguinte, a defesa pleiteou perante o Juízo de primeiro grau o reconhecimento da ilicitude das provas obtidas por meio da medida cautelar ajuizada, ao argumento de que a decisão não abarcou a quebra de sigilo dos dados previamente armazenados, mas apenas e tão somente a monitoração das comunicações dos alvos pelo prazo de 15 dias após a implementação, mas se indeferiu o pleito (fls. 1.939/1.940)

Consta que os autos da investigação foram redistribuídos à Central de Garantias Especializada de Curitiba/PR e o inquérito policial se encontra suspenso até que os recursos da defesa contra a referida quebra do sigilo sejam julgados (fl. 1.940).

Ainda inconformada, a defesa dos recorrentes impetrou *habeas corpus* na colenda Corte de origem, que denegou a ordem (fls. 731/739).

Aqui, sustentam os recorrentes constrangimento ilegal na obtenção de elementos de informação de forma ilegal pela autoridade policial.

Informam, de início, que, apesar de ter sido deferida a interceptação telemática pelo prazo de 15 dias, a autoridade policial teve *acesso a mensagens antigas*,

*armazenadas nas caixas de e-mails dos investigados, assim como o material telemático armazenado no sistema OneDrive, concernentes ao período de um ano pretérito à data da autorização judicial (fl. 959).*

*Aduzem que não há como se extrair do pedido formulado pela Autoridade Policial, assim como da decisão judicial de primeiro grau que deferiu a interceptação telemática (monitoramento dos e-mails dos recorrentes), qualquer autorização para a captura de material telemático (mensagens de e-mail e/ou dados telemáticos) que não fosse relativo ao período de 15 dias subsequentes à sua implementação (fl. 960).*

*Sustentam que se deve diferenciar a interceptação das comunicações telemáticas da quebra do sigilo telemático, pois é absolutamente inconcebível [...] que uma decisão judicial que autoriza a “interceptação telemática” de comunicações em fluxo por um período de 15 dias futuros seja automaticamente convertida (apenas e tão somente em razão de a MICROSOFT alegar não ter condições técnicas de cumpri-la), pela Autoridade Policial, em uma “quebra de sigilo telemático” referente a período totalmente diverso (fl. 964), até porque não há motivação específica para a quebra do sigilo de e-mails armazenados.*

*Postulam, então, seja dado provimento ao presente recurso para o fim de declarar a nulidade da quebra do sigilo telemático dos recorrentes efetuada ilegalmente pela Autoridade Policial nos autos da medida cautelar de interceptação telemática nº 0016436-71.2023.8.16.0013, instaurada perante a 5ª Vara Criminal de Curitiba, Estado do Paraná, determinando-se, em consequência, o desentranhamento e a inutilização do material ilegalmente juntado aos autos (fl. 970).*

*Admitido o recurso na origem, subiram os autos ao Superior Tribunal de Justiça.*

*A liminar foi indeferida pelo eminente relator, Ministro Otávio de Almeida Toledo (Desembargador convocado do TJSP) – (fls. 1.928/1.931).*

*Prestadas as informações pelas instâncias ordinárias (fls. 1.939/1.941 e 1.947 /1.962), o Ministério Público Federal opinou pelo desprovimento do recurso ordinário (fls. 1.965/1.972).*

*Em sessão de julgamento realizada no dia 12/8/2025, o eminente relator proferiu voto no sentido de dar provimento ao recurso.*

Após, pedi vista antecipada dos autos para verificar, com calma e profundidade, as alegações formuladas pelos recorrentes.

É o relatório.

A questão formulada no presente recurso ordinário cinge-se em verificar se a autorização de interceptação das comunicações telemáticas por prazo determinado, conforme permitido pelo Juízo de primeiro grau, abrangeria o acesso aos dados telemáticos armazenados, relativos a período anterior à autorização judicial.

Confira-se, no que interessa, trecho da decisão de primeiro grau, que autorizou a interceptação do fluxo das comunicações telemáticas dos recorrentes (fls. 96 /103 - grifo nosso):

[...]

1. Trata-se de representação formulada por [...] - Autoridade Policial da Divisão de Combate à Corrupção desta Capital - pela implementação de **interceptação telemática de e-mails expressamente delineados no requerimento inaugural**, isto para a apuração do crime previsto no artigo 168 da Lei nº 11.101/2005 (movimentos 1.1/1.2).

A Autoridade Policial alegou, em síntese, que [...] estariam praticando atos criminosos no bojo da Ação de Recuperação Judicial nº 0000155-53.2013.8.16.0025, em trâmite perante a 1ª Vara de Falências e de Recuperação Judicial deste Foro Central - a qual trata do Grupo IMCOPA -, bem como que a medida pleiteada é o único meio possível para a coleta de outras provas da materialidade delitiva, da autoria e da eventual mobilização dos investigados para prejudicar a investigação.

Atuando no feito, **depois de informados os períodos para a interceptação** e a ação controlada, a ilustre representante do Ministério Público se manifestou pelo deferimento da representação (movimento 16.1 e 20.1).

Assim, vieram os autos conclusos.

2. Verifica-se que a representação policial teve início com a instauração de inquérito após requerimento feito pelo senhor [...], representante legal da [...].

Pelo requerimento, noticiou-se que [...] estariam praticando atos no intuito de encobrir a real administração do [...] no contexto da ação de recuperação judicial para, com isso, obterem vantagens indevidas em prejuízo dos credores.

De acordo com a documentação e o apurado no bojo do inquérito policial instaurado:

[...]

Logo, **há indícios da prática do crime sob apuração, pois a administração do [...] não estaria sendo realizada pela empresa [...], cujos administradores são [...], controladores de fato do grupo em recuperação judicial.**

Portanto, e de acordo com os documentos e informações que instruem o pedido, verifico a robustez das investigações procedidas, bem como a gravidade dos fatos em apuração, observando que, no caso vertente, prevalece o interesse da sociedade na apuração da verdade (princípio da proporcionalidade).

Nota-se que as medidas investigativas utilizadas até o momento não possuem mais o condão de permitir a evolução da investigação, **sendo o monitoramento das comunicações eletrônicas o único caminho investigativo que possibilitará novos dados para desbaratar as atividades delituosas encetadas e identificar os autores.**

Segundo o disposto no artigo 5º, inciso XII, da Constituição Federal, que vislumbra o rol de direitos e garantias fundamentais de todo cidadão, 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 plena.

**Ainda no que pertine à legislação de regência, verifico que os requisitos para a validade da interceptação estão elencados no artigo 2º da Lei nº 9.296/96.**

[...]

O crime que está sendo investigado é de elevada gravidade e apenado com reclusão, conforme determinado pela legislação de regência.

Por outro lado, o acesso a dados, documentos e informações personalíssimas é autorizado em procedimentos investigatórios, consoante já previsto na Lei nº 9.034/95, bem como na Lei nº 9.296/96, a qual regulamentou o artigo 5º, inciso XII, parte final, da Constituição Federal, conforme, inclusive, entendimento encampado pelo Superior Tribunal de Justiça, nos termos do julgado adiante transcrito.

[...]

Por derradeiro, conclui-se que foram preenchidos todos os requisitos para o deferimento dos pleitos, afigurando-se necessárias as medidas para comprovar os crimes e a participação efetiva das pessoas envolvidas.

4. Em face ao exposto:

**4.1. Autorizo a interceptação telemática pelo prazo de 15 (quinze) dias passível de prorrogação, dos endereços de e-mails abaixo listados, determinando a expedição de ofício à MICROSOFT para que, no prazo de 24 (vinte e quatro) horas, inicie o monitoramento dos e-mails e forneça os dados das contas - por meio de seu portal - detalhes de registro, informações de faturamento e transações de faturamento acaso existentes, registros dos números de IP () no momento do login dos usuários, serviços da Microsoft utilizados, detalhes do registro da conta e do número do IP de acesso quando do registro da conta, conteúdos de e-mails, contatos de e-mails, detalhes de registro do , de IP de acesso ao , arquivos armazenados no e registros de transações no , ficando expressamente vedada a interceptação de endereços eletrônicos não discriminados na presente decisão. E-mail - Provedor de hospedagem**

[...]

4.2. AUTORIZO a utilização de ação controlada, nos moldes da Lei nº 12.850/2013.

4.3. AUTORIZO o Chefe de Secretaria senhor [...] a realizar os atos processuais necessários ao trâmite dos presentes autos, pessoalmente ou por servidor por ele indicado.

[...]

Instado sobre a legalidade da medida, o Tribunal de origem afirmou que (fls.

735/738 – grifo nosso):

[...]

No caso o que se verifica é que ambas as plataformas "One Drive" e "Exchange" fazem parte do pacote de serviços "Microsoft 365", contudo da atenta leitura da decisão atacada neste *writ*, apenas a plataforma "One Drive" está contida, tanto na decisão quanto no requerimento da Autoridade Policial.

De fato, o que se verifica é a inexistência de nulidade em relação aos dados fornecidos pela empresa Microsoft referente a detalhes do registro da conta e do número do IP de acesso quando do registro da conta, conteúdos de e-mails, contatos de e-mails, detalhes de registro do OneDrive, logs de IP de acesso ao OneDrive, arquivos armazenados no OneDrive e registros de transações no OneDrive no período de um ano pretérito à data da decisão atacada, porquanto abrangidos pelo teor da decisão judicial proferida, exceto o serviço Exchange, não abarcado pela decisão.

Ao reverso do que apregoa a Defesa, a delimitação temporal exigida pela legislação vigente é imposta ao monitoramento do fluxo de comunicação, uma vez que a decisão atacada, além do monitoramento do fluxo de e-mails, também determinou ao final (e nos termos do requerimento da autoridade policial e manifestação do Ministério Público), o acesso aos arquivos armazenados no “OneDrive”, além dos registros de transações no mesmo dispositivo de armazenamento.

[...]

Observando-se o teor da representação policial e da manifestação ministerial, bem como da decisão questionada, verifica-se expressa menção (e deferimento) de acesso aos arquivos pretéritos armazenados no “OneDrive”. Reitera-se que os arquivos fornecidos datados de momento pretérito não se referem a fluxo de comunicações em curso.

[...]

Reitera-se que a definição de prazo para observância da medida refere-se ao monitoramento do fluxo de comunicação, porquanto para o armazenamento de dados adota-se o critério da razoabilidade e proporcionalidade, os quais, dentro dos limites da decisão atacada, não foram violados no presente caso.

[...]

Outrossim, a alegação de que o parecer técnico anexado pela Defesa concluiu (mov. 38.2) no sentido de que os e-mails pretéritos obtidos pela autoridade policial (de 2022 a 2023) não foram extraídos do sistema “One Drive” e sim, do sistema “Microsoft Exchange”, pelo que constituíram elementos ilícitos, já que não abarcados pela decisão do Juízo, não tem o condão de macular a presente decisão. Além de se referir a documento ao qual o juízo a quo não teve acesso, tratando-se de inovação recursal, reforça a ideia de que se concedeu acesso a registros de e-mails pretéritos, não vinculados ao fluxo de informações, dispensando a delimitação temporal.

[...]

A fim de melhor contextualizar a questão, é importante analisarmos tanto o requerimento formulado pela Autoridade Policial, quanto o parecer do Ministério Público:

Confira-se (fls. 27/30 – grifo nosso):

[...]

Isto posto e apesar da clareza da contextualização dos fatos, mostra-se necessário o prosseguimento das investigações, em especial com **o deferimento de novas medidas voltadas à cabal elucidação das circunstâncias em que tais tratativas restaram engendradas, sendo que nessa perspectiva a interceptação telemática se mostra meio absolutamente necessário, especialmente para a coleta de outras provas acerca da materialidade da prática delitiva, de sua autoria e da eventual mobilização dos investigados para prejudicar o curso da presente investigação.**

#### II- DOS PEDIDOS DA INTERCEPTAÇÃO TELEMÁTICA

Assim sendo, pelo que se conclui, os requisitos exigidos pela Lei n. 9296/96 para o deferimento da interceptação telemática dos investigados encontram-se presentes, senão vejamos.

Os indícios até o presente momento são contundentes acerca da existência de conduta criminosa e de sua autoria, mormente porque existem indícios verossímeis que evidenciam a gestão de grupo empresarial que está em recuperação judicial por pessoas diversas daquelas que constam em seu contrato social.

A conduta dos investigados se amolda perfeitamente ao tipo legal previsto no artigo 168 da Lei 11.101/05, qual seja a prática de ato fraudulento, durante a recuperação judicial que possa resultar em prejuízo aos credores ou vantagem para si ou para outrem.

Ora, se os reais administradores do grupo empresarial estão permitindo que terceiros exerçam a gestão e por sua vez estes terceiros estão exercendo

devidamente tais atos, sem sombra de dúvida esta conduta poderá resultar em prejuízo aos credores, que não poderão alcançar os administradores de fato que estão atuando sob o manto da camuflagem.

**Destaca-se ainda a necessidade de utilização da presente técnica de investigação, uma vez que as tratativas e respectivas apreciações estão sendo mantidas por e-mails, o que dificulta a obtenção de elementos de informação por outros meios. Desta feita, resta demonstrado que a prova não pode ser obtida por outro meio senão pela interceptação telemática.**

Além da necessidade manifesta de utilização da interceptação telemática, também estão presentes os demais requisitos exigidos pela Lei nº 9.296/96, quais sejam os indícios razoáveis de autoria e a punição do fato por pena de reclusão, o que se consubstancia pelo **conteúdo dos e-mails trocados entre os investigados** e pelas manifestações de gestão dos mesmos e pela previsão legal do artigo 168 da Lei 11.101/05 que prevê pena de reclusão de 3 a 6 anos, além de multa.

Há que se destacar que um dos e-mails objeto do presente pedido de interceptação é utilizado pelo patrono do Grupo Imcopa e como advogado há que se respeitar a sua esfera de atuação, porém a Lei 8.906/94 é clara ao disciplinar que é um direito do advogado ter respeitada a inviolabilidade de suas correspondência eletrônica e telemática, salvo quando existirem indícios de autoria e materialidade de crime por parte do advogado, o que se demonstra na presente situação uma vez que o próprio causídico informa ao administrador judicial que os anexos referentes ao edital de venda das plantas do Grupo Imcopa estariam sendo preparados pela R2C Investimentos.

Ora, tal manifestação demonstra o conhecimento da administração do grupo por terceiros e mais ainda, instrumentaliza a gestão do grupo empresarial por pessoas estranhas ao contrato social, o que se traduz em efetiva co-autoria da prática do ato fraudulento em investigação. **Desta feita, resta adequado o afastamento do sigilo telemática também do patrono do Grupo Imcopa por se mostrar imprescindível às investigações.**

DESTA FEITA, salvo melhor juízo, presentes os requisitos legais e com o intuito de dar prosseguimento às investigações, e principalmente diante da imprescindibilidade da medida para colheita de provas que por outro meio não seriam coletadas, vem esta Autoridade Policial REPRESENTAR para que seja autorizada a INTERCEPTAÇÃO TELEMÁTICA dos e-mails a seguir descritos:

[...]

A presente interceptação, uma vez deferida, deverá ser atendida pela Microsoft que **fornecerá os dados das contas, por meio de seu portal, detalhes de registro, informações de faturamento e transações de faturamento, acaso existentes, registros dos números de IP (Internet Protocol) no momento do login dos usuários, serviços da Microsoft utilizados, detalhes do registro da conta e do número do IP de acesso quando do registro da conta, conteúdos de e-mail, contatos de e-mail, detalhes de registro do OneDrive, logs de IP de acesso ao OneDrive, arquivos armazenados no One Drive e registros de transações no OneDrive.**

[...]

O parecer do Ministério Público estadual foi no seguinte sentido (fls. 87/89 - grifo nosso):

[...]

Da interceptação das comunicações telefônicas e telemática.

A Lei 9.296/96 regulamentou o inciso XII, parte final, do artigo 5º da Constituição Federal, cujo texto garante, como regra, o sigilo das correspondências e telecomunicações. O inciso constitucional permite, excepcionalmente, a quebra do sigilo, mediante o preenchimento de dois requisitos: 1) que atenda as hipóteses e a forma prevista em lei; e 2) que a finalidade seja investigação criminal ou produção de prova em processo penal.

O artigo 2º da Lei n.º 9.296/96 estabelece que a interceptação de comunicações telefônicas de qualquer natureza será autorizada nos casos em que estiverem presentes: a) indícios razoáveis da participação dos investigados na prática de infração penal; b) a interceptação se mostrar necessária para a comprovação da participação dos investigados, não havendo outro meio adequado de prova a ser produzido; c) a infração em tese praticada é punida com reclusão. A partir das informações elencadas pela autoridade policial, verifica-se que estão presentes o *fumus comissi delicti* e o *periculum in mora* necessários para a concessão da medida.

**As informações preliminares encaminhadas pela d. autoridade policial e obtidas através de investigações são fidedignas e garantem plausibilidade ao pedido, pois configuram fortes indícios da prática de delitos de fraude a credores e outros correlatos, sendo a medida pleiteada imprescindível para a apuração destes, bem como para a identificação, qualificação e localização das pessoas envolvidas nos crimes.**

Considerando que foram executadas as ações possíveis com os recursos disponíveis, verifica-se a imprescindibilidade da autorização de outros meios para obtenção de dados e informações essenciais ao sucesso da investigação e consequente prevenção/coibição aos ilícitos supramencionados.

Oportuno registrar, ainda, que o deferimento do presente requerimento não encontra obstáculo nas normas estatuídas pela Resolução 59, do Conselho Nacional de Justiça - CNJ, uma vez que: a) o usuário que se pretende interceptar foi devidamente especificado; b) o prazo de interceptação é aquele legalmente previsto - 15 (quinze) dias; c) há precisa indicação da autoridade requerente e das autoridades policiais responsáveis pela investigação e que terão acesso às informações.

Registre-se que em um Estado Democrático de Direito a inviolabilidade foi erigida ao *status* de direito fundamental, justificando a sua violação apenas em circunstâncias excepcionais, legalmente previstas e necessárias à preservação de princípios jurídicos relevantes.

Na hipótese, diante das regras legais já mencionadas, e, diante, também, dos princípios jurídicos envolvidos, em um juízo de ponderação entre os interesses em conflito, conclui-se que, no caso concreto, estão presentes os requisitos exigidos pela legislação, justificando-se o deferimento do pedido.

Isto posto, preenchidos os requisitos estabelecidos, o Ministério Público manifesta-se pelo **deferimento do pedido de interceptação de dados telemáticos das contas de e-mail abaixo elencadas, a ser atendida pela Microsoft que fornecerá os dados das contas, por meio de seu portal, detalhes de registro, informações de faturamento e transações de faturamento, acaso existem, registros dos números de IP (Internet Protocol) no momento do login dos usuários, serviços da Microsoft utilizados, detalhes do registro da conta e do número do IP de acesso quando do registro da conta, conteúdo de e-mail, contatos de e-mail, detalhes de registro do OneDrive, logs de IP de acesso ao OneDrive, arquivos guardados no OneDrive e registros de transações no OneDrive, contados da data de implementação da medida até os 15 (quinze) dias seguintes a esta:**

[...]

Para que não haja prejuízos à investigação, a qual será desenvolvida na sede da Divisão Estadual de Combate à Corrupção - Núcleo Curitiba/PR, requer-se, caso deferido o pedido, a intimação da autoridade policial, na pessoa do Dr. envio de mov. 16.1.

[...]

Do atento exame dos trechos transcritos, verifico que, embora coubesse ao Magistrado singular pormenorizar melhor a forma de efetivação da medida investigativa, a fim de evitar a presente controvérsia, o requerimento da autoridade policial e o parecer do Ministério Público não deixam dúvidas sobre a necessidade de concessão da medida

tanto para monitorar o fluxo das comunicações eletrônicas, como possibilitar o acesso dos dados armazenados, considerados indispensáveis para o êxito das investigações, já que, conforme consta, existem indícios de que as tratativas para a consumação das fraudes contra os credores foram e estão sendo realizadas por e-mails dos investigados.

Estou de acordo com o acórdão hostilizado quando afirma que *a delimitação temporal exigida pela legislação vigente é imposta ao monitoramento do fluxo de comunicação, uma vez que a decisão atacada, além do monitoramento do fluxo de e-mails, também determinou ao final (e nos termos do requerimento da autoridade policial e manifestação do Ministério Público), o acesso aos arquivos armazenados no “OneDrive”, além dos registros de transações no mesmo dispositivo de armazenamento.*

Sustentar que a imposição de prazo para o monitoramento das comunicações telemáticas demonstra que a autorização judicial se limita a tanto é argumento frágil, perto da determinação, constante da mesma decisão, de *fornecimento de conteúdos de e-mail, contatos de e-mail, detalhes de registro do OneDrive, logs de IP de acesso ao OneDrive, arquivos armazenados no One Drive e registros de transações no OneDrive.*

Em face do exposto, peço vênia ao eminente relator e voto no sentido de **negar provimento** ao recurso ordinário.

CERTIDÃO DE JULGAMENTO  
SEXTA TURMA

Número Registro: 2025/0127658-3

PROCESSO ELETRÔNICO

RHC 214.389 / PR  
MATÉRIA CRIMINAL

Números Origem: 00164367120238160013 00269363620228160013 00341250220258160000  
00722610520248160000 01107631320248160000 01118856120248160000  
1107631320248160000 1118856120248160000  
111885612024816000000341250220258160000 164367120238160013  
269363620228160013 341250220258160000 722610520248160000

PAUTA: 12/08/2025

JULGADO: 11/11/2025  
SEGREGADO DE JUSTIÇA

**Relator**

Exmo. Sr. Ministro **OTÁVIO DE ALMEIDA TOLEDO (DESEMBARGADOR CONVOCADO DO TJSP)**

**Relator para Acórdão**

Exmo. Sr. Ministro **SEBASTIÃO REIS JÚNIOR**

**Ministro Impedido**

Exmo. Sr. Ministro : **ROGERIO SCHIETTI CRUZ**

Presidente da Sessão

Exmo. Sr. Ministro **CARLOS PIRES BRANDÃO**

Subprocurador-Geral da República

Exmo. Sr. Dr. **CARLOS FREDERICO SANTOS**

Secretário

Bel. **ELISEU AUGUSTO NUNES DE SANTANA**

**AUTUAÇÃO**

RECORRENTE : R D G  
RECORRENTE : R M M  
ADVOGADOS : SERGIO ROSENTHAL - SP114806  
JULIANO JOSE BREDAS - PR025717  
ADVOGADA : VALESKA TEIXEIRA ZANIN MARTINS - SP153720  
ADVOGADA : CARINA QUITO - SP183646  
ADVOGADOS : NICOLE TRAUZYNSKI MUFFONE - PR041301  
ANTONIO GLAUCIUS DE MORAIS - DF012308  
ADRIANO SERGIO NUNES BRETAS - PR038524  
GABRIEL GARCIA SOARES - PR118659  
RECORRIDO : MINISTÉRIO PÚBLICO DO ESTADO DO PARANÁ  
ADVOGADO : JOAO PAULO DE OLIVEIRA BOAVENTURA - DF031680  
INTERES. : T B L  
INTERES. : W C M F  
INTERES. : M D L E R J  
ADVOGADOS : IGOR ARTHUR RAYZEL - PR075656  
OTTO MEDEIROS DE AZEVEDO JUNIOR - DF047761  
IGOR DOS SANTOS JAIME - DF054584  
BENO FRAGA BRANDAO - PR020920  
THIAGO TURBAY FREIRIA - DF057218  
JOAO PAULO DE OLIVEIRA BOAVENTURA - DF031680  
ADVOGADOS : EDUARDA CANDIDO ZAPPONI - DF064353  
TRACY JOSEPH REINALDET DOS SANTOS - DF069913  
MATTEUS BERESA DE PAULA MACEDO - DF070111  
IGOR CUSTODIO DE ARAUJO FERREIRA - DF080602

ASSUNTO: DIREITO PENAL - Crimes previstos na Legislação Extravagante - Crimes Falimentares

**CERTIDÃO DE JULGAMENTO  
SEXTA TURMA**

Número Registro: 2025/0127658-3

**PROCESSO ELETRÔNICO****RHC 214.389 / PR**  
MATÉRIA CRIMINAL**CERTIDÃO**

Certifico que a egrégia SEXTA TURMA, ao apreciar o processo em epígrafe na sessão realizada nesta data, proferiu a seguinte decisão:

Prosseguindo no julgamento, após o voto vista do Sr. Ministro Sebastião Reis Júnior negando provimento ao agravo regimental, sendo acompanhado pelos Srs. Ministros Joel Ilan Paciornik e Antonio Saldanha Palheiro, a Sexta Turma, por maioria, negou provimento ao agravo regimental, nos termos do voto do Sr. Ministro Sebastião Reis Júnior, que lavrará o acórdão.

Votaram com o Sr. Ministro Sebastião Reis Júnior os Srs. Ministros Antonio Saldanha Palheiro e Joel Ilan Paciornik. Vencido o Sr. Ministro Otávio de Almeida Toledo (Desembargador Convocado do TJSP). Impedido o Sr. Ministro Rogerio Schietti. Afirmou suspeição o Sr. Ministro Og Fernandes. Não participou do julgamento o Sr. Ministro Carlos Pires Brandão.