Poder Judiciário da União
TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS

| | |
|---|---|
| **Órgão** | Câmara Criminal |
| **Processo N.** | AGRAVO REGIMENTAL CRIMINAL 0714619-24.2020.8.07.0000 |
| **AGRAVANTE(S)** | |
| **AGRAVADO(S)** | |
| **Relator** | Desembargador JOÃO TIMÓTEO |
| **Acórdão Nº** | 1276346 |

**EMENTA**

**AGRAVO INTERNO EM MANDADO DE SEGURANÇA. PENAL E PROCESSUAL PENAL. APURAÇÃO DE CRIME DE CONCORRÊNCIA DESLEAL. DECISÃO JUDICIAL. CORREIO ELETRÔNICO E DADOS EM NUVEM. QUEBRA DE SIGILO. LEI Nº 9.296/96. INAPLICABILIDADE. PROVEDOR DE DADOS. OBRIGATORIEDADE DE DISPONIBILIZAÇÃO DAS INFORMAÇÕES EM JUÍZO. LEI Nº 12.965. MARCO CIVIL DA INTERNET. RECURSO DESPROVIDO.**

1. Conforme entendimento do Supremo Tribunal Federal, a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação “de dados” e não dos “dados em si mesmos”.

2. Os dados armazenados em nuvem não evidenciam uma comunicação de dados, mas representam o armazenamento de dados em um provedor de serviços na nuvem (“cloud storage”). Nessa medida, a quebra de sigilo referente a dados armazenados em nuvem não está abrangida pela Lei nº 9.296/96, uma vez que não há interceptação; e sim o conhecimento quando eles já foram armazenados.

3. Por seu lado, o correio eletrônico constitui forma de comunicação mediante correspondência, na qual a mensagem é redigida em computador e transmitida eletronicamente. Ademais, quando a mensagem de *e-mail* chega ao seu destinatário e fica armazenada no provedor, já se aperfeiçou o processo de transmissão da mencionada mensagem.

4. Portanto, mostra-se inviável a aplicação da Lei de Interceptações Telefônicas para a quebra de sigilo de correspondências eletrônicas, porquanto a sua apreciação recai sobre dados em si mesmos, e não sobre fluxo de informações. Ademais, de se observar que o artigo 7º, inciso III, da Lei nº 12.965 (Marco Civil da Internet) excepciona a inviolabilidade e sigilo de comunicações privadas armazenadas diante de ordem judicial.

5. As partes impetrantes/agravantes, na qualidade de provedores responsáveis pela guarda dos referidos dados, possuem o dever legal de fornecê-los em Juízo, nos moldes do artigo 10, § 2º, da Lei nº 12.965/2014.

6. Negado provimento ao agravo interno.

**ACÓRDÃO**

Acordam os Senhores Desembargadores do(a) Câmara Criminal do Tribunal de Justiça do Distrito Federal e dos Territórios, JOÃO TIMÓTEO - Relator, NILSONI DE FREITAS CUSTODIO - 1º Vogal, JESUINO RISSATO - 2º Vogal, WALDIR LEÔNCIO LOPES JÚNIOR - 3º Vogal, JAIR SOARES - 4º Vogal, J. J. COSTA CARVALHO - 5º Vogal, SEBASTIÃO COELHO - 6º Vogal, CARLOS PIRES SOARES NETO - 7º Vogal, DEMÉTRIUS GOMES CAVALCANTI - 8º Vogal, ROBSON BARBOSA DE AZEVEDO - 9º Vogal, GEORGE LOPES - 10º Vogal, ROBERVAL CASEMIRO BELINATI - 11º Vogal e SILVANIO BARBOSA DOS SANTOS - 12º Vogal, sob a Presidência do Senhor Desembargador MARIO MACHADO, em proferir a seguinte decisão: NEGAR PROVIMENTO AO AGRAVO INTERNO. UNÂNIME., de acordo com a ata do julgamento e notas taquigráficas.

Brasília (DF), 19 de Agosto de 2020

**Desembargador JOÃO TIMÓTEO**
Relator

**RELATÓRIO**

Trata-se de mandado de segurança impetrado por G. L. e G. B. I. LTDA. contra decisão (ID 16523795 - Pág. 02/05) proferida pelo Juízo da Vara Criminal e Tribunal do Júri do Guará que, em autos de medida cautelar preparatória de busca e apreensão e produção antecipada de provas, decretou a quebra de sigilo de dados e comunicações telemáticas do usuário de conta de e-mail XXX, incluindo eventuais arquivos armazenados na plataforma Google Drive (nuvem), no período compreendido entre abril de 2018 e maio de 2019

Narra que, no dia 04 de junho de 2019, a ora impetrante G. B. I. LTDA. foi comunicada de decisão determinando a quebra do sigilo telemático de correio eletrônico e de dados em nuvem referente ao usuário XXX.

Assevera que a impetrante G. L. solicitou confirmação ao Juízo de piso quanto à natureza do crime investigado. Destaca que, no dia 05 de fevereiro de 2020, a empresa foi comunicada de decisão do Juízo na origem de que os fatos investigados configurariam, em tese, crime de concorrência desleal, previsto no artigo 195 da Lei nº 9.279/96 e punido com detenção.

Sustenta que a Lei nº 9.296/96 tutela o sigilo das comunicações telemáticas, sendo aplicável a vedação legal de quebra de sigilo para crimes punidos com detenção. Defende que a quebra de dados referentes a serviço de armazenamento em nuvem (*"Google Drive"*) vulnera o princípio da proporcionalidade.

Liminarmente, requer a concessão de efeito suspensivo ao *writ*, para impedir a execução da v. decisão até o julgamento do presente feito. No mérito, pleiteia a concessão da ordem para a anulação da r. decisão, no que tange ao comando para o fornecimento pela Impetrante do conteúdo de *Gmail* e

*Google Drive* referente ao usuário XXX.

Decisão sob esta Relatoria (ID 16650216) indeferindo o efeito suspensivo pleiteado pelo Agravante.

Na sequência, os ora impetrantes, G. L. e G. B. I. LTDA. interpuseram agravo interno contra a decisão monocrática que indeferiu o efeito suspensivo pleiteado.

Em suas razões recursais (ID 5190144), os agravantes reiteram os fundamentos de fato e de direito explicitados na *Ordem do Mandado de Segurança*.

Requerem, ao final, a reconsideração da r. decisão monocrática, para que o presente mandado de segurança seja totalmente conhecido e provido.

Informações prestadas pela autoridade apontada como coatora (ID 16712984).

Manifestação da Procuradoria de Justiça pelo conhecimento e não provimento (ID 17410207).

É o relatório.

**VOTOS**

**O Senhor Desembargador JOÃO TIMÓTEO - Relator**

Presentes os pressupostos legais, conheço do agravo interno.

Em que pesem as respeitáveis alegações constantes do agravo interno, não verifico qualquer fundamento novo apto a modificar a decisão prolatada por esta Relatoria, a seguir transcrita:

> (...) É cediço que o Mandado de Segurança é cabível para proteger direito líquido e certo, não amparado por *habeas corpus*ou *habeas data*, sempre que, ilegalmente ou com abuso de poder, alguém sofrer violação ou houver justo receio de sofrê-la. Ademais, nos termos do artigo 7°, inciso III, da Lei nº 12.016/09, devem ser preenchidos dois pressupostos para a concessão de liminar no *writ of mandamus*, quais sejam, o fundamento relevante da impetração e a possibilidade de ineficácia da decisão final que eventualmente conceda a segurança.
>
> Em análise perfunctória, não se verifica a presença de fundamento relevante da impetração.
>
> Por oportuno, a Constituição Federal estabeleceu, em seu artigo 5º, inciso XII, que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução de processo criminal.

Não obstante a expressa previsão em relação aos direitos fundamentais da privacidade e intimidade, o próprio texto constitucional reconhece não ser absoluto o direito individual em apreço, pois admite a quebra de sigilo para fins de investigação criminal ou instrução processual penal, por ordem judicial.

Com efeito, o "caput" do artigo 1º da Lei nº 9.296/96 prevê a possibilidade de interceptação das comunicações telefônicas, enquanto o parágrafo único do mesmo dispositivo amplia a abrangência da referida norma para os sistemas de informática e telemática, nos seguintes termos:

"Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.

Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática."

Ressalte-se que o fluxo de comunicações em sistemas de informática e telemática somente é abrangido pelas disposições da Lei de Interceptações Telefônicas quando inseridos na modalidade "comunicações telefônicas", o que não é o caso dos autos, em que o Impetrante pretende a manutenção de sigilo de dados telemáticos referentes a correio eletrônico e de dados armazenados em nuvem.

Nesse sentido, são esclarecedores os ensinamentos do jurista Lenio Streck:

"(...) não vislumbro inconstitucionalidade no dispositivo sob comento. O parágrafo único, ao estender a possibilidade de interceptação também ao fluxo de comunicações em sistemas de informática e telemática, apenas especificou que a lei também atingirá toda e qualquer variante de informações que utilizem a modalidade 'comunicações telefônicas'. Ou seja, objetivou a Lei estender a aplicação das hipóteses de interceptação de comunicações telefônicas a qualquer espécie de comunicação, ainda que realizada mediante sistemas de informática, existentes ou que venham a ser criados, desde que tal comunicação utilize a modalidade 'comunicações telefônicas'. (...) (As Interceptações Telefônicas e os Direitos Fundamentais: Constituição, Cidadania, Violência: Lei 9.296/96 e seus reflexos penais e processuais. Porto Alegre: Livraria do Advogado, 1997, p. 42-43)".

Ademais, conforme entendimento do Superior Tribunal de Justiça,"(...) 1. A quebra do sigilo do correio eletrônico somente pode ser decretada, elidindo a proteção ao direito, diante dos requisitos próprios de cautelaridade que a justifiquem idoneamente, desaguando em um quadro de imprescindibilidade da providência. (...)" (HC 315.220/RS, 6ª Turma, Rel. Min. Thereza de Assis Moura, julgamento em 15/09/2015, DJe 09/10/2015).

No caso dos autos, verifica-se que a discussão acerca da imprescindibilidade/proporcionalidade da medida decretada na origem demanda dilação probatória, o que se afigura inviável nessa estreita via processual.

3. Nesses termos, indefiro a liminar. (...)

Conforme se depreende dos autos, no dia 07/05/2019, o Juízo na origem deferiu parcialmente o pleito veiculado na medida cautelar preparatória criminal de busca e apreensão e produção antecipada de provas ajuizada por E. C. S/A, E. E. P. S/A e G. E. C. contra V. D. T. J. B. para "determinar a expedição de mandados de busca e apreensão a serem cumpridos nos endereços vinculados ao Requerido; decretar o afastamento do sigilo de dados e comunicações telemáticas do usuário da conta

de e-mail denominada: XXX e de outras contas de titularidade de V. D. T. J. B., incluindo eventuais arquivos armazenados na plataforma Google Drive (nuvem), no período compreendido entre agosto de 2018 até o dia do efetivo cumprimento da medida" (ID 16712984).

Em 21/05/2019, o Juízo na origem acolheu o pleito das Requerentes para aditar os termos da decisão acima, a fim de que o período do afastamento do sigilo de dados e comunicações seja compreendido entre abril de 2018 até o dia do efetivo cumprimento da medida.

Realizado pedido de esclarecimentos pelas ora impetrantes, G. L. e G. B. I. LTDA., o Juízo de piso prolatou, no dia 04/02/2020, decisão determinando a reiteração dos ofícios, nos seguintes termos (ID 16523795 - Pág. 02/05):

> Trata-se de medida cautelar preparatória de busca e apreensão e produção antecipada de provas ajuizada pelo G. E. C., composto das empresas E. C. S/A e E. E. P. S/A, em face de (...)
>
> Na decisão proferida às fls. 151/154, este Juízo determinou a expedição de mandados de busca e apreensão com vistas à obtenção de registros digitais que comprovem a utilização e/ou acesso indevido a dados de propriedades do G. E. C., inclusive dispositivos de armazenamento eletrônicos (discos rígidos - HDS, notebooks, pen drives, smartphones, CDs e DVDs e demais arquivos eletrônicos) em poder de (...)
>
> No mesmo ato, foi decretado o afastamento do sigilo de dados e comunicações telemáticas do usuário da conta de e-mail denominadaXXXe de outras contas de titularidade de (...), incluindo eventuais arquivos armazenados na plataforma Google Drive (nuvem), no período compreendido entre abril de 2018 até o dia do efetivo cumprimento da medida.
>
> As informações trazidas aos autos nos documentos de fls. 170/179 indicaram que não se logrou êxito no cumprimento dos mandados de busca e apreensão expedidos.
>
> As Requerentes declinaram dois endereços atualizados do Requerido, pugnando pela expedição de novos mandados de busca e apreensão.
>
> O magistrado substituto deste Juízo proferiu decisão à fl. 199/199v., na qual declinou da competência para processar e julgar os presentes autos em favor de uma das Varas Criminais de Brasília.
>
> A Câmara Criminal deste Eg. TJDFT julgou competente para o processamento e julgamento dos autos este Juízo, conforme extrato da decisão proferida à fl. 249.
>
> Na decisão de fls. 238/239, determinou-se a reiteração dos termos do oficio de fl. 180, requisitando-se dados e comunicações telemáticas do usuário da conta de e-mail denominadaXXXe de outras contas de titularidade de (...), incluindo eventuais arquivos armazenados na plataforma Google Drive (nuvem), no período compreendido entre abril de 2018 até o dia do efetivo cumprimento da medida.
>
> No e-mail enviado a este Juízo (fl. 242), a Custodiante de Dados a cargo de G. L. solicitou esclarecimentos a respeito da natureza da investigação levada a efeito nestes autos.
>
> A parte Requerida ingressou nos autos, conforme documentação de fls. 270/276.
>
> No petitório de fls. 273/291, de início, esclareceu que a despeito do absoluto sigilo do presente feito, obteve conhecimento da presente medida cautelar a partir das cópias que

instruem a Queixa-Crime nª 0001428-42.2019.8.07.0014, vinculada à presente medida cautelar, explicando que descobriu a existência da ação em referência por meio do sitio eletrônico "JusBrasil".

A seguir, o Peticionante, sob o entendimento de que não se mostra presente qualquer requisito idôneo a decretar medida tão gravosa em face do Requerido, pugnou pelo imediato arquivamento da presente medida cautelar.

Na petição de fls. 310/316, as Requeridas apresentaram os seguintes pedidos:

a) a manutenção da decisão da quebra de sigilo;

b) o imediato encaminhamento de resposta ao e-mail remetido pelo G. L. para que apresente, no prazo de 05 (cinco) dias, as informações requisitadas anteriormente por meio do oficio nº 643/2019/VCTJGUA/TTJDFT (fl. 180);

c) o imediato cumprimento da medida de busca e apreensão nos seguintes endereços:

(...)

d) a imediata expedição dos respectivos mandados e seu encaminhamento pelo meio mais ágil à d. autoridade policial;

e) que os mandados sejam cumpridos por peritos nomeados pelo juízo e acompanhados pelos assistentes técnicos e pelos advogados das Peticionarias.

É o Relatório. DECIDO.

De início, conquanto as Requeridas tenham questionado o fato de o Requerido ter acessado a queixa-crime nº 0001428-42.2019.8.07,0014, processo este com sigilo decretado nos autos, é certo que na decisão proferida pela magistrada titular da Quinta Vara Criminal de Brasília, em 22/07/2019, quando o feito por ali tramitou, foi decretado o segredo de justiça, contudo autorizou-se o acesso ao teor dos autos pelas partes e seus advogados (vide ID nº 40280341).

Com isso, uma vez que as Requerentes não se insurgiram contra aquela decisão, tenho como regular o acesso aos autos eletrônicos da queixa-crime em referência e aos documentos ali inseridos, por parte dos advogados do Requerido, mormente a considerar a petição de habilitação e as procurações e substabelecimentos (ID nº 52535876 e seguintes).

Feito isso, quanto aos petitórios e documentos acostados pelo Requerido (fls. 273/291, 292/300, e 322/325), de antemão, por se tratarem os presentes autos de medida cautelar preparatória para ajuizamento de eventual queixa-crime, cujas diligências já foram autorizadas inicialmente na decisão de fls. 151/154, esta magistrada não irá se aprofundar na análise do mérito da causa, nestes autos específicos, destacando que a alteração legislativa levada a efeito no artigo 282, § 3º, do Código de Processo Penal Já foi devidamente observada, sendo certo que a parte contrária se manifestou no feito, em mais de uma oportunidade.

**Em atenção aos esclarecimentos solicitados no e-mail de fl. 242, conforme bem consignado pela ilustre Promotora de Justiça, no Parecer de fl. 268, a quebra de sigilo telemático requerida está prevista no artigo 22 da Lei nº 12.965/14 (Lei do Marco Civil da Internet) e deverá ser determinada por ordem judicial a ser cumprida pelo provedor de internet responsável pela guarda dos arquivos digitais vinculados à conta de e-mail do representado.**

No presente caso, este Juízo acolheu o pedido das Requerentes para determinar o afastamento do sigilo de dados e comunicações telemáticas do usuário da conta de e-mail denominada:XXXe de outras contas de titularidade de (...), incluindo eventuais arquivos armazenados na plataforma Google Drive (nuvem), no período compreendido entre abril de 2018 até o dia do efetivo cumprimento da medida.

**Deve ser ressaltado à Custodiante de Dados a cargo de G. L. que não se pretende, na presente medida, a interferência no fluxo de comunicação de terceiros, ou seja, acesso em tempo real, o que só pode acontecer nos termos da Lei nº 9.296/96, mas a determinação judicial se limita a requisitar os dados Já armazenados, salvos após o encerramento da comunicação, os quais não podem ser alcançados por outros meios disponíveis.**

No que se refere ao pedido reiterado das Requerentes, a fim de que sejam expedidos mandados de busca e apreensão domiciliar para cumprimento nos endereços, em tese, vinculados ao Requerido, tenho que não é mais possível o êxito de tais medidas. na atual fase em que se encontra o presente feito.

O entendimento acima se justifica no fato de o Requerido já possuir ciência inequívoca de todos os atos processuais desencadeados nesta medida cautelar sigilosa. conforme alhures anotado.

O próprio advogado do Requerido se manifestou neste sentido e demonstrou, de fato, ter conhecimento do processo, apresentando os petitórios e documentos de fls. 273/291, 292/300, e 322/325. nos quais menciona por diversas vezes as medidas de busca e apreensão pleiteadas pelas Requerentes.

Nos termos do art. 240 do CPP, a busca e apreensão domiciliar poderá ser realizada para a descoberta dos objetos necessários à prova da infração e colheita de quaisquer elementos de convicção, desde que presentes fundadas razoes para o deferimento da medida.

É de sabença que a lei processual penal exige, neste caso, a verificação da necessidade da medida para levantar elementos de prova, baseada em fundadas razões.

Ocorre que o agente cuja medida visa alcançá-lo já tem conhecimento dos tatos e das decisões que foram previamente proferidas nestes autos, além do que constituiu advogado particular que vem acompanhando rotineiramente os andamentos processuais registrados no feito.

Com isso. é pouco provável que (...) ainda mantenha consigo algo que possa eventualmente compromete-lo no bojo de futuro processo-crime.

Diferentemente da quebra de sigilo acima determinada, na busca e apreensão pretendida, o agente poderá mudar o estado das coisas, o que fatalmente frustrará o êxito da medida.

Neste caso, esta magistrada não pode olvidar do alto dispêndio ocasionado com eventual acionamento da máquina estatal, composta de servidores (oficiais de justiça) e equipe de policiais (delegados, agentes), além de peritos e seus assistentes para cumprimento de 02 (duas) diligências, em locais diversos, sabendo-se previamente que a possibilidade de não obtenção de êxito nas medidas é considerável.

Diante das considerações acima:

l- INDEFIRO o pedido das Requerentes para a expedição de novos mandados de busca e apreensão domiciliar para cumprimento nos endereços informados à fl. 316.

II- DETERMINO que sejam reiterados os termos dos ofícios de fls. 180 e 240, instruindo-se os expedientes com cópia desta decisão, com vistas aos esclarecimentos solicitados no e-mail de fl. 242. Consigne-se no documento o pedido de urgência no envio das informações requisitadas. Para o efetivo cumprimento da ordem, encaminhe-se o oficio, também, para o endereço de e-mail de fl. 242, bem como mantenha-se contato com o Escritório de Advocacia que presta serviços à G. L. no fone (...)

III- DETERMINO que os autos prossigam sua tramitação sob segredo de justiça, devendo a Secretaria cuidar para que apenas as partes e seus advogados previamente habilitados tenham acesso ao conteúdo dos atos e documentos acostados ao feito. (...) (Grifo nosso.)

No dia 04 de maio de 2020, o Juízo na origem prolatou nova decisão, a seguir transcrita (ID 16523802 - Pág. 01/06):

(...) 4. Em remate, no que diz respeito à solicitação da empresa G. L., para que seja desobrigada de prestar os dados comunicacionais e privados armazenados na conta indicada pelas Requerentes, sob a alegação de que pretende evitar a violação indevida do sigilo de comunicações, os argumentos sustentados pelas advogadas responsáveis por subscrever o pedido não se sustentam.

De acordo com a inteligência inserta nas explicações prestadas, a pedido da referida empresa, na decisão de fl. 330, a determinação deste Juízo não consiste em interceptação telefônica ou interceptação do fluxo de comunicações em sistemas de informática e telemática, com previsão na Lei nº 9.296/96, conforme a custodiante de dados a cargo de G. L. insiste em se apoiar para deixar de atender às requisições reiteradas constantes dos ofícios de fls. 180 e 240.

Portanto, pela derradeira vez, frise-se que a decisão deste Juízo não foi proferida sob a égide dos ditames da Lei nº 9.296/96, não havendo qualquer ordem de decreto de interceptação telefônica ou de interceptação do fluxo de comunicações em sistemas de informática e telemática.

A autorização judicial para afastamento do sigilo dos dados e comunicações telemáticas do usuário da conta de e-mail denominada:XXX e de outras contas de titularidade de V. D. T. J. B., incluindo eventuais arquivos armazenados na plataforma Google Drive (nuvem), conforme exaustivamente debatido nos autos, foi fundamentada na Lei nº 12.965/14 (Marco Civil da *Internet*), sendo que, de acordo com o laborioso parecer ministerial de fls. 436/437, a referida Lei não estabelece tipo de crime, tampouco período determinado, não cabendo a custodiante de dados a cargo de G. L. fazer análise do mérito, mas apenas atender à requisição judicial, sob pena de incorrer no crime tipificado no artigo 330 do Código Penal.

Ante o exposto, profiro as seguintes decisões abaixo:

I- DEIXO DE ADMITIR os embargos de declaração interpostos às fls. 334/340, tendo em vista a ilegitimidade do embargante.

Nada obstante, não pode esta magistrada olvidar que o fato de a decisão guerreada não modular o período em que deve ser afastado o sigilo telemático do embargante, agregada a circunstância de que, até a presente data, a custodiante de dados a cargo de G. L. não se desincumbiu de atender a requisição judicial, ocasiona, de fato, a omissão indicada, não podendo ser admitido que a medida se estenda por prazo indeterminado, sem que o embargante tenha concorrido para tal elastecimento.

> *In casu*, acolho a sugestão ministerial, por tê-la como razoável, para DETERMINAR que sejam, pela derradeira vez, reiterados os termos dos ofícios de fls. 180, 240 e 332, com cópia dos referidos expedientes e da presente decisão, requisitando-se as informações solicitadas, no prazo improrrogável de 05 (cinco) dias, sob pena de se incorrer nas penas do artigo 330 do Código Penal, bem como na aplicação de multa diária em valor a ser arbitrado por este Juízo.
>
> Deverá a Secretaria acompanhar atentamente o decurso do prazo acima anotado, retornando conclusos os autos, imediatamente, após o seu termo final, em caso de se transcorrer *in albis*o período em referência, a fim de que seja decidida a questão da multa, como também determinados os encaminhamentos sobre eventual incidência no delito de desobediência. (...)

Da detida análise das decisões prolatadas pelo Juízo na origem supramencionadas, verifica-se que grupo empresarial que presta serviços online na área educacional busca apurar eventual crime de concorrência desleal praticado pelo representado ao passar a prestar seus serviços para outra empresa que também presta serviços educacionais no âmbito da internet.

Sustentam as impetrantes/agravantes que a Lei de Interceptações Telefônicas seria aplicável ao caso, de modo que não seria viável a quebra do sigilo referente a dados armazenados em conta de correio eletrônico (Gmail) e de dados em nuvem (Google Drive).

Sem razão, contudo.

Como já mencionado, a Constituição Federal estabeleceu, em seu artigo 5º, inciso XII, que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução de processo criminal.

Não obstante a expressa previsão em relação aos direitos fundamentais da privacidade e intimidade, o próprio texto constitucional reconhece não serem absolutos os direitos individuais em apreço, pois admite a quebra de sigilo para fins de investigação criminal ou instrução processual penal, por ordem judicial.

Na mesma senda, são esclarecedores os ensinamentos de Gilmar Mendes e Paulo Gustavo Gonet, a seguir transcritos:

> A leitura do preceito pode levar à conclusão de que apenas nos casos de comunicações telefônicas seria possível que o Poder Público quebrasse o sigilo e que seria impossível abrir ao seu conhecimento os dados constantes de correspondência postal, telegráfica ou de comunicações telemáticas.
>
> Sabe-se, porém, que a restrição de direitos fundamentais pode ocorrer mesmo sem autorização expressa do constituinte, sempre que se fizer necessária a concretização do princípio da concordância prática entre ditames constitucionais. Não havendo direitos absolutos, também o sigilo de correspondência e o de comunicações telegráficas são passíveis de ser restringidos em casos recomendados pelo princípio da proporcionalidade. Para o STF, ademais, o sigilo garantido pelo art. 5º., XII, da CF refere-se apenas à comunicação de dados, e não aos dados em si mesmos. A apreensão de um computador, para dele se extraírem informações gravadas no *hard disk*, por exemplo, não constitui

> hipótese abrangida pelo âmbito normativo daquela garantia constitucional. (MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional. 10. ed. São Paulo: Saraiva, 2015, pp. 293-294).

Portanto, o ordenamento jurídico brasileiro não admite a utilização abusiva da esfera de proteção constitucional dada à correspondência, comunicações telegráficas, de dados e comunicações telefônicas para a prática de atos ilícitos, de modo que, presentes os requisitos pertinentes, é possível, em caráter excepcional, a decretação de quebra de sigilo dos fluxos de comunicação ou de dados armazenados.

**I – Inaplicabilidade da Lei nº 9.296/96**

**a) Dados armazenados em nuvem**

Conforme entendimento esposado pelo Supremo Tribunal Federal, o inciso XII do artigo 5º da Constituição Federal tutela a comunicação de dados, que não se confunde com os dados em si mesmos.

Com efeito, a comunicação envolve um trânsito/fluxo de dados, os quais podem ficar armazenados em um meio físico (p. ex. pendrives, CDs) ou virtual (p. ex. armazenamento em nuvem).

Desse modo, os dados armazenados em nuvem não evidenciam uma comunicação de dados, mas representam o armazenamento de dados em um provedor de serviços na nuvem (*"cloud storage"*).

Saliente-se que o termo jurídico "interceptar" presente na Lei nº 9.296/06 significa "captar a comunicação telefônica, tomar conhecimento, ter contato com o conteúdo dessa comunicação enquanto ela está acontecendo" (GOMES, Luiz Flávio. Interceptação telefônica: comentários à Lei 9.296/1996. São Paulo: Ed. RT, 2011, p. 24).

Nessa medida, a quebra de sigilo referente a dados armazenados em nuvem não está abrangida pela Lei nº 9.296/96, uma vez que não há interceptação, uma vez que o conhecimento dos dados ocorre quando eles já estão armazenados.

Perfilhando de mesmo entendimento, confira-se a decisão proferida pelo Ministro Luiz Fux no RHC nº 181.877/MG, *ad litteris*:

> (...) **Com efeito, observo que a Lei 9.296/96, a qual "regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal", não se aplica a dados que se encontram armazenados em celular. É que o artigo 5º, XII, da Constituição Federal abrange apenas a comunicação e não os dados já armazenados.** Veja-se a redação do referido dispositivo:"XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal";O parágrafo único do artigo 1º da Lei 9.296/96 delimita o âmbito de aplicação desse diploma normativo:Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz

competente da ação principal, sob segredo de justiça.Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática. **Exsurge da interpretação da norma que o legislador ordinário distinguiu duas situações diferentes: i) o "fluxo de comunicações em sistemas de informática e telemática"; e ii) os dados obtidos como consequência desse diálogo ou outros dados existentes em "sistemas de informática e telemática".** A propósito, o Plenário do Supremo Tribunal Federal já esclareceu o âmbito de abrangência do referido artigo, valendo mencionar, *in verbis*:

"[...] IV - Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a consequente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 3. Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve 'quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial'. 4. A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270). V - Prescrição pela pena concretizada: declaração, de ofício, da prescrição da pretensão punitiva do fato quanto ao delito de frustração de direito assegurado por lei trabalhista (C. Penal, arts. 203; 107, IV; 109, VI; 110, § 2º e 114, II; e Súmula 497 do Supremo Tribunal)." (RE 418.416, Tribunal Pleno, Rel. Min. Sepúlveda Pertence, DJ de 19/12/2006)

No mesmo sentido:

"AGRAVO REGIMENTAL. HABEAS CORPUS SUBSTITUTIVO DE RECURSO ORDINÁRIO. ACESSO A DADOS CADASTRAIS E DE USUÁRIOS. SIGILO DAS COMUNICAÇÕES. AUSÊNCIA DE TERATOLOGIA. 1. Não cabe habeas corpus em substituição ao recurso ordinário constitucional (HC 109.956, Rel. Min. Marco Aurélio). 2. As decisões proferidas pelas instâncias de origem estão alinhadas com a jurisprudência do Supremo Tribunal Federal, no sentido de que "a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos'" (RE 418.416, Rel. Min. Sepúlveda Pertence, Plenário) 3. Ausência de teratologia, ilegalidade flagrante ou abuso de poder que autorize a concessão da ordem de ofício para invalidar a prova. 4. Agravo regimental a que se nega provimento." (HC 124.322-AgR, Primeira Turma, Rel. Min. Roberto Barroso, DJe de 19/12/2016) (...)

(RHC 181.877/MG, Rel. Min. Luiz Fux, julgamento em 03/03/2020, DJe 04/03/2020)

No mesmo sentido, confiram-se precedentes do STF e deste Tribunal:

(...) 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial.

**3. Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve "quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial".**

**4. A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270).**(...)

(RE 418.416/SC, Plenário, Rel. Min. Sepúlveda Pertence, julgamento em 10/05/2006, DJ de 19/12/2006)

RECURSO ORDINÁRIO EM *HABEAS CORPUS*. APURAÇÃO DE CRIME DE FALSIDADE DOCUMENTAL. BUSCA E APREENSÃO. VALIDADE. DILIGÊNCIA REALIZADA EM ÓRGÃO PÚBLICO. ARRECADAÇÃO DE COMPUTADORES SOBRESSALENTES À ORDEM JUDICIAL. ENTREGA VOLUNTÁRIA DAS MÁQUINAS PELA AUTORIDADE RESPONSÁVEL. CLÁUSULA DE RESERVA DE JURISDIÇÃO OBSERVADA. EXAME PERICIAL CONDICIONADO À POSTERIOR AUTORIZAÇÃO JUDICIAL. PRESERVAÇÃO DO DIREITO À INTIMIDADE. ACESSO AOS DADOS REGISTRADOS EM DISPOSITIVO ELETRÔNICO. SUPOSTA VIOLAÇÃO AO SIGILO DE CORRESPONDÊNCIA ELETRÔNICA. INOCORRÊNCIA. INDEFERIMENTO DE DILIGÊNCIAS EM PROCEDIMENTO CRIMINAL. CERCEAMENTO DE DEFESA. NÃO VERIFICAÇÃO. CONTRADITÓRIO E AMPLA DEFESA PRÓPRIOS DA FASE JUDICIAL. RECURSO DESPROVIDO.

(...)

**3. Descabe invocar a garantia constitucional do sigilo das comunicações de dados quando o acesso não alcança a troca de dados, restringindo-se apenas às informações armazenadas nos dispositivos eletrônicos. A orientação jurisprudencial do STF assinala que "A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270)" (RE 418.416, Rel. Min. Sepúlveda Pertence, Tribunal Pleno, DJ 19.12.2006).**

4. Em se tratando de instrumento destinado à formação da *opinio delicti*do órgão acusatório, o procedimento administrativo de investigação criminal não demanda a amplitude das garantias constitucionais da ampla defesa e do contraditório, próprias da fase judicial. Eventual prejuízo advindo do indeferimento de diligências no curso das apurações (nomeação de assistente técnico e formulação de quesitos) é passível de questionamento na ação penal decorrente do respectivo inquérito policial.

5. Recurso ordinário em *habeas corpus* desprovido.

(RHC 132062, Relator(a): Min. MARCO AURÉLIO, Relator(a) p/ Acórdão: Min. EDSON FACHIN, Primeira Turma, julgado em 22/11/2016, PROCESSO ELETRÔNICO DJe-243 DIVULG 23-10-2017 PUBLIC 24-10-2017)

(...) **2. O acesso ao conteúdo de dados, conversas e mensagens armazenadas em aparelhos de telefones celulares não se subordina aos ditames da Lei n. 9.296/96, que**

**disciplina a inviolabilidade das comunicações telefônicas.**

**3. A Lei n. 12.965/2014, Marco Civil da Internet, assegura, no artigo 7º, inciso III, a inviolabilidade de conversas privadas armazenadas, mas também permite, no mesmo dispositivo, a quebra por decisão judicial.**

(...)

5. O acesso aos dados armazenados não se sujeita a período determinado, por sua natureza e também por ausência de previsão legal, sendo certo que o inciso III do artigo 22 da Lei 12.965/2014 não rege a hipótese, pois trata do acesso aos registros de conexão ou de acesso a aplicações de internet.

6. Ordem denegada.

(Acórdão 1200713, 07181739820198070000, Relator: SILVANIO BARBOSA DOS SANTOS, 2ª Turma Criminal, data de julgamento: 12/9/2019, publicado no PJe: 16/9/2019. Pág.: Sem Página Cadastrada) (Grifo nosso.)

Portanto, o acesso a dados armazenados em nuvem não se submete aos ditames da Lei nº 9.296/96, não assistindo razão à irresignação recursal.

**b) Correio eletrônico**

Por seu lado, o correio eletrônico constitui forma de comunicação mediante correspondência, na qual a mensagem é redigida em computador e transmitida eletronicamente.

Na mesma medida, o sigilo epistolar não pode ser utilizado como salvaguarda para a prática de condutas ilícitas.

Confira-se o claro precedente deste e. Tribunal:

*HABEAS CORPUS*. DESENTRANHAMENTO DE DOCUMENTOS. ELEMENTOS INFORMATIVOS DE INQUÉRITO POLICIAL. VIOLAÇÃO AO PRINCÍPIO DO CONTRADITÓRIO. INOCORRÊNCIA. SIGILO DA CORRESPONDÊNCIA. MITIGAÇÃO.

(...)

**4. O sigilo epistolar deve ser mitigado pela aplicação do princípio da proporcionalidade considerando a colisão daquela garantia com a suspeita da prática de infração penal.**

**5. Segundo o Supremo Tribunal Federal, "a cláusula tutelar da inviolabilidade do sigilo epistolar não pode constituir instrumento de salvaguarda de práticas ilícitas" (HC nº 70.814-//SP).**

6. Ordem denegada.

(Acórdão 750346, 20130020292864HBC, Relator: CESAR LABOISSIERE LOYOLA, 2ª Turma Criminal, data de julgamento: 16/1/2014, publicado no DJE: 20/1/2014. Pág.: 188)

Com efeito, a correspondência eletrônica não é passível de ser interceptada, uma vez que isso ocasionaria a intervenção na própria comunicação realizada entre os interlocutores.

Destaque-se que, quando a mensagem de email chega ao seu destinatário e fica armazenada no provedor, já se perfectibilizou o processo de transmissão da mencionada mensagem.

Isso significa dizer que não é cabível a incidência da Lei nº 9.296/96 para a quebra de sigilo de mensagens de correio eletrônico, mas, sim, a incidência dos dispositivos legais aplicáveis à busca e apreensão, nos moldes dos artigos 240 e seguintes do Código de Processo Penal:

> Art. 240. A busca será domiciliar ou pessoal.
>
> § 1º Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para:
>
> (...)
>
> **e) descobrir objetos necessários à prova de infração**ou à defesa do réu;
>
> **f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato;**
>
> (...)
>
> **h) colher qualquer elemento de convicção.**

Nesse sentido, confiram-se os ensinamentos do Professor Geraldo Prado:

> (...) 70. Deste modo, ao realizarmos o processo comunicativo, ao interagirmos, a nossa privacidade corre o risco de ser violada legalmente. Desde que se justifique, mediante o devido processo legal e à consideração pelo juiz da extrema necessidade da medida, a privacidade pode ser afetada. **Isso pode ocorrer, com frequência, quando dois ou mais agentes resolvem pôr em prática, executar, projeto criminoso. Se o fazem, comunicando-se entre si por meio de cartas, estas podem ser apreendidas, uma vez que há justo motivo. É bem verdade que não podem ser interceptadas.**pois o processo comunicativo há de ser preservado à luz da Constituição. Não obstante, repousadas em poder do destinatário, poderão ser arrecadadas, desde que haja ordem judicial neste sentido, emanada em verdadeiro procedimento penal de índole cautelar.
>
> (...)
>
> **72. No exemplo dado, porém, não é difícil perceber que a carta — com ela também o telegrama e os dados contidos em bancos de dados — repousa ao final em poder do destinatário, conferindo exequibilidade à medida destinada a apreendê-la, com relativo grau de segurança.**O mesmo não acontece com a comunicação telefônica,

conforme salientou com extrema lucidez Tercio Sampaio Ferraz Junior, referindo-se à norma constitucional:

"Note-se, antes de mais nada, que dos quatro meios de comunicação ali mencionados — correspondência, telegrafia, dados, telefonia — só o último se caracteriza pela sua instantaneidade".

73. Portanto, se os dados da comunicação desaparecem imediatamente após esta ser concluída, nada existe a apreender que possa ser objeto de uma ação investigativa eficaz, salvo se a própria comunicação for violada. **Como salientou Tercio Ferraz, não são os dados o objeto da proteção constitucional, mas sim a sua comunicação, que poderá excepcionalmente ser afetada, quando de outro modo não for possível apreender a informação.**

**Destaca:**

**"Ora, como vimos, o inciso XII (proteção à comunicação de dados) impede o acesso à própria ação comunicativa, mas não aos dados comunicados"**

(...)

76. Quando os dados informáticos repousarem em bancos de dados, a sua comunicação não poderá ser objeto de interceptação, pois assim estaria sendo violada a Constituição. Porém, interpretada sistemática e teleologicamente, não haverá contraste com a norma de garantia a interceptação determinada à luz do *due process of law*, para fins de instrução criminal ou investigação da mesma natureza, quando se tratar de dados transmissíveis de modo a não repousarem em banco de dados ou forma similar, que permita a apreensão. (PRADO, Geraldo. Limite às Interceptações Telefônicas e a Jurisprudência do Superior Tribunal de Justiça. 2. ed. São Paulo: Editora Lumen Iuris, 2006, pp. 70-73).

Perfilhando de mesmo parecer, é o entendimento do Professor Gustavo Badaró:

A impossibilidade de interceptação do processo comunicativo por e-mail não significa, contudo, um obstáculo intransponível a produção de provas para fins penais. Normalmente, os dados e o conteúdo do e-mail permanecerão arquivados no computador que o enviou e no que recebeu a mensagem, bem como no provedor utilizado. **Dessa forma, do mesmo modo em que se faz com uma carta em papel, será possível a busca e apreensão dos discos rígidos dos computadores ou de qualquer outro suporte em que fique registrada tal correspondência eletrônica, segundo a disciplina legal dos arts. 240 e segs. do CPP.** (BADARÓ, Gustavo Henrique Righi Ivahy. Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia. In: LIMA, José Correa de; CASARA, R. R. Rubens. (Coord.). Temas para uma perspectiva crítica do direito: homenagem ao Professor Geraldo Prado. Rio de Janeiro: Lumen Juris, 2010, pp. 492-493).

Destaque-se, ainda, que a Lei nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil (Marco Civil da Internet), realiza a distinção entre fluxo de comunicações e conversas privadas armazenadas, integrando este último grupo as correspondências eletrônicas:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> 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** (...). (Grifo nosso.)

De se observar que o artigo 7º, inciso III, do Marco Civil da Internet excepciona a inviolabilidade e sigilo de comunicações privadas armazenadas diante de ordem judicial.

Portanto, mostra-se inviável a aplicação da Lei de Interceptações Telefônicas para a quebra de sigilo de correspondências eletrônicas e dados armazenados em nuvem, porquanto a sua apreciação recai sobre dados em si mesmos, e não sobre fluxo de informações.

Igualmente, devem ser observados os requisitos para a decretação de medida cautelar de busca e apreensão, nos moldes do artigo 240 e seguintes do Código de Processo Penal.

*In casu*, verifica-se que os documentos acostados aos autos pelas partes impetrantes são insuficientes para a análise dos requisitos cautelares da medida determinada pelo Juízo na origem e, mesmo que o fosse, tal análise demandaria incursão probatória, o que se afigura inviável nessa estreita via processual.

Vale dizer, o mandado de segurança tutela direito líquido e certo, isto é, aquele passível de ser demonstrado mediante prova pré-constituída.

Assim, não se verifica a existência de direito líquido e certo a ser resguardado no presente processo. Ao contrário, as partes impetrantes, na qualidade de provedores responsáveis pela guarda dos referidos dados, possuem o dever legal de fornecê-los em Juízo, nos moldes do artigo 10, § 2º, da Lei nº 12.965/2014.

Ressalte-se, ainda, que não há óbice que a Defesa, se entender estarem ausentes os pressupostos para a concessão da medida cautelar e em procedimento próprio para tanto, impugne as medidas decretadas pelo Juízo na origem, no exercício legítimo do contraditório e ampla defesa.

Diante do exposto, **nego provimento**ao agravo interno, mantendo incólume a decisão monocrática prolatada pelo Juízo na origem.

É como voto.

**A Senhora Desembargadora NILSONI DE FREITAS CUSTODIO - 1º Vogal**
Com o relator

**O Senhor Desembargador JESUINO RISSATO - 2º Vogal**
Com o relator

**O Senhor Desembargador WALDIR LEÔNCIO LOPES JÚNIOR - 3º Vogal**
Com o relator

**O Senhor Desembargador JAIR SOARES - 4º Vogal**
Com o relator

**O Senhor Desembargador J. J. COSTA CARVALHO - 5º Vogal**

Com o relator

**O Senhor Desembargador SEBASTIÃO COELHO - 6º Vogal**
Com o relator

**O Senhor Desembargador CARLOS PIRES SOARES NETO - 7º Vogal**
Com o relator

**O Senhor Desembargador DEMÉTRIUS GOMES CAVALCANTI - 8º Vogal**
Com o relator

**O Senhor Desembargador ROBSON BARBOSA DE AZEVEDO - 9º Vogal**
Com o relator

**O Senhor Desembargador GEORGE LOPES - 10º Vogal**
Com o relator

**O Senhor Desembargador ROBERVAL CASEMIRO BELINATI - 11º Vogal**
Com o relator

**O Senhor Desembargador SILVANIO BARBOSA DOS SANTOS - 12º Vogal**
Com o relator

**DECISÃO**

NEGAR PROVIMENTO AO AGRAVO INTERNO. UNÂNIME.