

PETIÇÃO 15.693 DISTRITO FEDERAL

RELATOR : MIN. ANDRÉ MENDONÇA
REQTE.(S) : SOB SIGILO
ADV.(A/S) : SOB SIGILO
AUT. POL. : SOB SIGILO

DECISÃO:

1. A Polícia Federal formulou requerimento de manutenção e conservação imediata de dados telemáticos armazenados em nuvem virtual, como medida preparatória para a quebra do sigilo telemático, de contas ativas vinculadas a alguns investigados na “Operação Compliance Zero”.

2. O pedido foi formulado nos seguintes termos:

“E a fim de não tornar ineficaz a futura solicitação de afastamento de sigilo telemático dos investigados na Operação Compliance Zero - integrantes e/ou vinculados ao núcleo de coerção e obtenção de dados sigilosos -, tendo em vista a possibilidade dos investigados ou partícipes deletarem conteúdo armazenado em nuvem, e considerando entendimento do STF exarado na decisão do HC 222.141, no sentido da necessidade de autorização judicial para preservação de dados;

Solicito a Vossa Excelência, com fulcro no disposto no § 2º do art. 13 e no §2º do art. 15, ambos da Lei 12.965/2014 (Marco Civil a Internet), que autorize e expeça Ofício à Apple e Google, a serem encaminhados por esta Polícia Federal, determinando a **preservação imediata de todos os dados e conteúdos telemáticos** existentes em sistemas de informática/armazenamento remoto (nuvem) das contas Apple e Google vinculadas aos IMEIs abaixo relacionados. (e-doc. 1, p. 1; grifos no original).

É o relatório. **Decido.**

3. A análise do elementos trazidos pela autoridade policial revelam que a preservação dos dados citados no requerimento é, de fato, relevante para a efetividade das investigações e para a identificação das medidas que estão sendo adotadas pelos investigados em suas comunicações. Nesse diapasão, os dados são usualmente sincronizados continuamente com as “nuvens” e a sua preservação é de suma importância para a obtenção de informações sobre os fatos que estão sendo apurados nestes autos.

4. O pedido encontra fundamento normativo nos arts. 15 e 22 da Lei nº 12.965/2014 (Marco Civil da Internet), bem como no art. 3º, V, da Lei nº 12.850/2013, assim dispostos:

Lei nº 12.965/2014

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

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Lei nº 12.850/2013

Art. 3º Em qualquer fase da persecução penal, serão permitidos, sem prejuízo de outros já previstos em lei, os seguintes meios de obtenção da prova:

(...)

V - interceptação de comunicações telefônicas e telemáticas, nos termos da legislação específica;

5. Verifica-se que o rol de investigados apresentado pela Polícia Federal refere-se, em sua maioria, àqueles contra os quais foram decretadas medidas constritivas de natureza pessoal no bojo da Pet nº 15.556/DF. Desse modo, os elementos ali já examinados mostram-se aptos a justificar a medida pretendida também neste feito em relação a (i) Luiz Phillipi Machado de Moraes Mourão; (ii) Marilson Roseno da Silva; (iii) Fabiano Campos Zettel; (iv) Ana Claudia Queiroz de Paiva e (v) Daniel Bueno Vorcaro.

6. Com relação a (vi) Daniel Souza Iost, muito embora não se tenha exarado determinação constritiva em seu desfavor, extrai-se da instrução coligida na mesma Pet nº 15.556/DF, notadamente do teor das Informações da Polícia Judiciária nº 1070759/2026 e nº 1020625/2026, que o investigado em questão supostamente realizava acessos ilícitos por via de sistemas internos ao Ministério Público Federal para obtenção de informações sigilosas.

7. No caso dos investigados remanescentes, recorro as informações

trazidas pela Polícia Federal na Pet nº 15.626/DF, na qual apurados indícios de que (vii) David Henrique Alves, (viii) Katherine Venancio Teles e (ix) Victor Lima Sedlmaier comporiam grupo de hackers a serviço de Mourão, razão pela qual ordenou-se, no âmbito daquele processo, a extração de dados de aparelho de celular então apreendido em sua posse.

8. Diante desse contexto, em vista do premente risco de supressão definitiva de dados, cuja obtenção e ciência emergem cruciais para elucidação dos fatos e aprofundamento das investigações, e considerando ainda que o pedido para efetiva quebra do sigilo telemático dos investigados será objeto de deliberação posterior, **DEFIRO o pedido de preservação e conservação de dados formulados pela Polícia Federal**, a fim de que as empresas (i) Apple Computer Brasil Ltda. (Apple Inc.) (lawenforcement@apple.com) e (ii) Google Brasil Internet Ltda. (Google LLC) (juridicobrasil@google.com), nos termos em que respectivamente indicado pela autoridade policial, **procedam, no prazo de 24 horas, à imediata preservação e conservação dos dados vinculados aos IMEIs (International Mobile Equipment Identity) mencionados na solicitação.**

9. Para o cumprimento desta determinação judicial, as duas empresas acima citadas deverão efetuar pesquisas em sistemas próprios, a fim de identificar o ID correspondente à pessoa, **no lapso temporal entre 01/01/2021 até a data da efetivação desta medida em 2026,** utilizando-se os dados fornecidos na tabela de fls. 02 e 03 (e-Doc. 1), e implementar **com a máxima urgência a preservação de todos os dados constantes em nuvem para posterior requisição judicial.**

10. **Determino, ainda, que as empresas Apple Computer Brasil Ltda. (Apple Inc.) e Google Brasil Internet Ltda. (Google LLC), no prazo de 15 dias, informem o cumprimento da determinação de congelamento, com a preservação dos dados a seguir relacionados:**

a) os dados cadastrais completos do usuário, incluindo nome, terminais telefônicos, endereços, e-mails e dados bancários vinculados à conta, além de outras contas ou serviços associados ao usuário e contatos fornecidos para recuperação de conta;

b) *logs* de criação (contendo IP, data, hora e fuso horário) das contas citadas no item “a”;

c) logs de acesso constando endereços de IP, data, hora e fuso horário GMT/UTC, no período de [data de início] até a data de cumprimento desta ordem;

d) dados sobre pagamento, incluindo o número dos cartões de crédito ou de contas bancárias cadastradas.

e) todo o conteúdo das comunicações preservado no período supracitado, incluindo, mensagens na caixa de entrada, de saída, quarentena, lixo, rascunho e quaisquer outras pastas personalizadas pelo cliente, bem como outros arquivos eventualmente armazenados;

f) todos os dados/arquivos armazenados nos aparelhos ou e-mails vinculados;

g) dados/arquivos e todos os demais conteúdos armazenados nos serviços de agenda de compromissos e de agenda de contatos (tais como Apple Agenda, Apple Calendar e similares), de qualquer extensão, data, horário, destinatário, remetente e tamanho;

h) dados/arquivos e todos os demais conteúdos armazenados no “iCloud”, Google Drive ou em qualquer outro repositório de arquivos (iMessage, serviços e sistemas de armazenamento em “nuvem”, de agenda de compromissos, de agenda de contatos, de localização, de calendários, de notas/lembretes, de redes sociais, de mensagens instantâneas – incluindo Whatsapp, Telegram e outros -, fotos e vídeos etc.),

de qualquer extensão, data, horário, destinatário, remetente e tamanho;

i) conteúdo armazenado no aplicativo "Apple Store" ou "Google Play Store", com a identificação de todos os aplicativos instalados nos aparelhos utilizados pelo usuário;

j) histórico de localização (*location history*) do usuário pelo período listado acima;

k) identificação de todos os contatos registrados junto aos aplicativos da plataforma Apple ou Google;

l) identificação de todas as pesquisas vinculadas às contas acima informadas, por meio do navegador Safari ou Google Chrome, no período listado acima;

m) fornecimento de todas as páginas adicionadas como favoritas no navegador Safari ou google Chrome, vinculadas às contas acima informadas.

Da operacionalização da decisão de preservação e conservação dos dados

11. No ofício dirigido à **Apple Computer Brasil Ltda**, em relação aos dados que tiver sob sua guarda dos investigados acima citados, deverá constar a determinação de que referida companhia conserve íntegro: **(i)** o conteúdo armazenado em nuvem; **(ii)** os registros de acesso, IPs e localização; **(iii)** as comunicações eletrônicas; **(iv)** os metadados associados; **(v)** os dados/arquivos e todos os demais conteúdos armazenados no "iCloud" ou qualquer outro repositório de arquivos (iMessage, serviços e sistemas de armazenamento em "nuvem", de agenda de compromissos, de agenda de contatos, de localização, de calendários, de notas/lembretes, de redes sociais, de mensagens instantâneas – incluindo Whatsapp, Telegram e outros -, fotos e vídeos etc.), de qualquer extensão, data, horário, destinatário, remetente e tamanho; **(vi)** o conteúdo armazenado no aplicativo "Apple Store", com a

identificação de todos os aplicativos instalados nos aparelhos utilizados pelo usuário.

12. No ofício dirigido à empresa **Google Brasil Internet Ltda.**, em relação aos dados que tiver sob sua guarda dos investigados acima citados, deverá constar a determinação de que referida companhia conserve íntegro: (a) todo o conteúdo das comunicações de e-mails preservados no período supracitado, incluindo mensagens na caixa de entrada, de saída, quarentena, lixo, rascunho e quaisquer outras pastas personalizadas pelo cliente, bem como outros arquivos eventualmente armazenados; (b) todos os dados/arquivos armazenados nos aparelhos ou e-mails vinculados; (c) dados/arquivos e todos os demais conteúdos armazenados no “Google Drive”, de qualquer extensão, data, horário, destinatário, remetente e tamanho, incluindo e-mails e dados de mensageiros instantâneos; (d) histórico de localização (*location history*) do usuário pelo período listado acima; (e) conteúdo armazenado na aplicação “Google Fotos”, com a indicação dos metadados das imagens e a integralidade de suas funções, tais como identificação de faces da funcionalidade “reconhecimento facial” e endereços de e-mail com quem o mesmo compartilha bibliotecas, referente ao período entre 01/01/2022 até a data de cumprimento da medida; (f) identificação e listagem dos locais salvos e com estrela (*starred locations*), compartilhados e visitados na aplicação “Google Maps”, além de histórico de busca e informações de metadados associados a esses dados, referentes ao período listado acima.

13. Nos termos em que requerido pelo autoridade policial, a **Secretaria Judiciária desta Corte deverá elaborar os ofícios dirigidos às empresas acima mencionadas, os quais serão encaminhados aos respectivos destinatários diretamente pela Polícia Federal.** Além dos ofícios, a autoridade policial deverá **enviar, com máxima urgência, e-mails com cópia desta decisão e da representação inicial (e-Doc. 01) para os emails:** lawenforcement@apple.com (APPLE) e

PET 15693 / DF

juridicobrasil@google.com (GOOGLE).

14. Após a adoção das diligências acima elencadas pela Secretaria Judiciária, dê-se imediata ciência ao MPF.

Intime-se.

Brasília, 18 de março de 2026.

Ministro **ANDRÉ MENDONÇA**
Relator