

A (i)licitude da prova obtida a partir do congelamento do conteúdo da internet

Por Rômulo de Andrade Moreira ¹

Resumen: *En una correcta decisión, la Suprema Corte brasileña anuló todas las pruebas obtenidas del congelamiento del contenido de las cuentas electrónicas de un imputado por supuestas infracciones penales, porque no hubo autorización judicial previa; la singular decisión se tomó en el Habeas Corpus n° 222141.*

Palabras clave: Pruebas - Congelamiento del contenido de las cuentas electrónicas - Autorización judicial previa - Habeas Corpus n° 222141

Em uma correta decisão monocrática, o ministro Ricardo Lewandowski anulou todas as provas obtidas a partir do congelamento do conteúdo de contas eletrônicas de uma acusada por supostas irregularidades no Detran do Paraná, por não ter havido prévia autorização judicial; a decisão singular foi tomada no Habeas Corpus n°. 222141.

No caso concreto, em 22 de novembro de 2019, o Ministério Público do Estado do Paraná solicitou aos provedores Apple e Google a preservação dos dados e IMEIs (identificação internacional de equipamento

móvel) coletados nas contas vinculadas aos sócios de uma determinada empresa, com a finalidade de conseguir elementos de prova para as investigações na “Operação Taxa Alta”, que envolveu o credenciamento de empresas para serviços de registro eletrônico de contratos. O congelamento dizia respeito a informações cadastrais, histórico de localização e pesquisas, conteúdo de e-mails, mensagens e hangouts, fotos e nomes de contatos.

No habeas corpus impetrado junto à Suprema Corte, a defesa de uma das acusadas alegou que a obtenção das provas teria violado o direito à intimidade e à privacidade, e que o conteúdo telemático junto aos provedores de internet teriam sido congelados sem autorização judicial, extrapolando os limites da legislação de proteção geral de dados pessoais, previstos na Lei n°. 12.965/2014, o chamado Marco Civil da Internet.

Anteriormente, o Superior Tribunal de Justiça negou o pedido de suspensão do trâmite da ação penal em curso na 12ª Vara Criminal de Curitiba e a declaração de nulidade das provas obtidas, sob o argumento que a Constituição Federal protegeria somente o sigilo das comunicações em fluxo (troca de dados e mensagens em tempo real, de modo dinâmico), e que o sigilo das comunicações armazenadas, como o depósito registral (dados estáticos), seria tutelado pela previsão constitucional do direito à privacidade.

Discordando do entendimento da Corte Superior, o ministro Ricardo Lewandowski observou que o pedido de quebra do sigilo, no período de 1º. de junho de 2017 até a data do requerimento, foi apresentado pelo Ministério Público à justiça somente em 29 de novembro de 2019, uma semana da

¹ Procurador de Justiça do Ministério Público do Estado da Bahia e professor de Direito Processual Penal da Universidade Salvador – UNIFACS.

implementação da medida de congelamento, deferido em 03 de dezembro de 2019; escreveu o ministro, **in verbis**:

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

Destarte, o congelamento e a consequente perda da disponibilidade dos dados não foram lastreados por nenhuma decisão judicial de quebra de sigilo, como era imperativo à luz da Constituição Federal e do Marco Civil da Internet (Lei nº. 12.965/2014).²

Neste sentido, para o relator, *“caso prevalecesse o entendimento esposado no acórdão combatido, toda e qualquer autoridade policial ou o próprio Ministério Público poderiam requisitar aos provedores da internet, sem a devida autorização judicial, a indisponibilidade de dados telemáticos de qualquer investigado, situação que, a toda evidência, não se concebe. Nesta senda, rememoro as palavras do Ministro Edson Fachin no julgamento da ADPF 403/DF, de sua relatoria, ao enfatizar que a privacidade é o direito de manter o controle sobre a sua própria informação e de determinar a maneira de construir sua própria esfera pública.”*

² Guillermo Beltramone e Ezequiel Zabale definem a internet *“como uma rede de computadores interconectados que agrupa a outras milhares de redes menores, que utilizam um protocolo comum para ‘falar’ entre si. Cada uma dessas redes está gerida pela organização que a controla (organismos públicos e privados, universidades e redes locais privadas.”* (El Derecho en la Era Digital – Derecho Informático de Fin de Siglo. Rosario: Editorial Juris, 1997, p. 11).

E, lembrando reiterada jurisprudência da própria Suprema Corte, o ministro Lewandowski afirmou que a Constituição protege o sigilo das comunicações em fluxo, enquanto o direito constitucional à privacidade tutela o sigilo das comunicações armazenadas. Assim, fez constar do voto, **ipsis litteris**:

“A jurisprudência desta Suprema Corte tem afirmado reiteradamente que o inciso XII do art. 5º da Carta Magna protege o sigilo das comunicações em fluxo (troca de dados e mensagens). Assenta também que o sigilo das comunicações armazenadas, como depósito registral, é tutelado pela previsão constitucional do direito à privacidade, na forma do inciso X do art. 5º, CF (cito, v.g., o HC 91.867/PA, relator Ministro Gilmar Mendes). No campo infraconstitucional, o Marco Civil da Internet (Lei 12.965/2014) traça os princípios aplicáveis em nosso ordenamento, enumerados no art. 3º, tal como o da proteção da privacidade e dos dados pessoais, assegurando, outrossim, a inviolabilidade e sigilo do fluxo de suas comunicações e sigilo de suas comunicações privadas armazenadas, ressalvada ordem judicial de sua quebra (art. 7º da mencionada lei).”

Ademais, segundo ele, o Marco Civil da Internet, ao tratar de forma específica da proteção aos registros, aos dados pessoais e às comunicações privadas, é indubitoso quanto à possibilidade de fornecimento de informações de acesso (registro de conexão e de acesso a aplicações de internet), mediante solicitação do Ministério Público ou das autoridades policiais ou administrativas, sendo, contudo, indispensável a autorização judicial prévia e devidamente fundamentada.³

³ Tratando especificamente do marco jurídico da internet, a autora espanhola, Esther Morón Lerma, afirma que a internet *“caracteriza-se por ser um meio universal de comunicação e busca de informação a muito baixo custo e está composta por um conjunto de redes*

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

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

Em conclusão, o ministro Ricardo Lewandowski anotou “que cabe ao Ministério Público requerer cautelarmente que os registros de conexão sejam guardados por prazo superior a 1 ano, quais sejam, aqueles exclusivos a informações de data e hora de acesso, duração e IP de origem, o que, como afirmado alhures, não se confunde com o conteúdo telemático armazenado dentro dos sistemas autônomos, tais como históricos de pesquisa, todo o conteúdo de e-mail e Imessages, fotos e dados de localização.”

interconectadas, que permitem a comunicação entre milhões de usuários de todo o mundo, gerando um imenso grupo de recursos de informação, em forma de imagens, texto, gráficos e som.” (Internet y Derecho Penal: Hacking e otras Conductas Ilícitas en la Red. Pamplona: Editorial Aranzadi, 1999, p. 137).

A prevalecer entendimento contrário, e ainda na esteira da decisão monocrática, ter-se-ia a possibilidade de “autorização para que houvesse a busca e apreensão prévia de conteúdos e seu congelamento, para posterior formalização da medida por ordem judicial, em prática vedada por qualquer **stantard** que se extraia da ordem constitucional vigente.”

Portanto, em casos como tais, o Ministério Público deve observar a necessária reserva de jurisdição no que toca à ordem de indisponibilidade do conteúdo telemático por parte da sua legítima titular, sob pena de afrontar a Constituição Federal e o Marco Civil da Internet, admitindo-se ao Ministério Público uma “verdadeira medida cautelar, ao ordenar, **sponte propria**, o ‘congelamento’ de todo o conteúdo de comunicações telemáticas da paciente”, retirando “do seu legítimo proprietário o direito de dispor do conteúdo dos seus dados para quaisquer fins, sem que houvesse autorização judicial para tanto.”⁴

Do contrário, teremos uma prova produzida ilicitamente, nos termos do art. 5º, LVI, da Constituição Federal, devendo ser desentranhada do processo, inclusive as subsequentes, dela derivadas, salvo quando não evidenciado o nexo de causalidade entre uma e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras, conforme a doutrina do **fruit of the poisonous** ou **the tainted fruit**⁵ (art. 157, § 1º. do Código de Processo Penal).⁶

⁴ Disponível em: <https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/HC222141.pdf>. Acesso em 15 de dezembro de 2022.

⁵ A respeito do assunto, por todos, confira-se a obra de Luiz Flávio Gomes e Raúl Cervini: *Interceptação Telefônica*, São Paulo: Revista dos tribunais, 1997.

⁶ De se observar, a propósito, haver autores que distinguem as provas ilícitas das chamadas

Sobre a questão da informática e o direito penal argentino, Riquert assevera que “o caráter antijurídico da descoberta de dados está claro quando estes dados estão amparados por preceitos tradicionais que protegem sigilos especiais.” Para este autor, “todas as leis de proteção de dados preveem de maneira especial a proteção dos direitos informativos do cidadão relacionados com os dados que sobre ele são processados: se alguém não tem informação sobre quem obteve informação sobre ele, que tipo de informação e com que meios o fez, não poderá participar na vida pública sem medo.”⁷

Afinal de contas, como já escreveu Cappelletti, “a conformidade da lei com a Constituição é o lastro causal que a torna válida perante todas.”⁸ Devemos interpretar as leis ordinárias em conformidade com a Carta Magna, e não o contrário!

ilegítimas; neste sentido, por exemplo, Ada, Scarance e Magalhães Gomes Filho, esclarecem que “quando a proibição for colocada por uma lei processual, a prova será ilegítima (ou ilegitimamente produzida); quando, pelo contrário, a proibição for de natureza material, a prova será ilicitamente obtida.” (As Nulidades no Processo Penal, São Paulo: Malheiros, 1996, p. 116).

⁷ RIQUERT, Marcelo Alfredo. Informática y Derecho Penal Argentino. Buenos Aires: AD-HOC, 1999, pp. 62 e 65.

⁸ CAPPELLETTI, Mauro. La Giurisdizione Costituzionale delle Libertà, 1955, pp. 136 e 137, **apud** MARQUES, José Frederico. Elementos de Direito Processual Penal, Campinas: Bookseller, 1998, Vol. I, p. 79.