V O T O

O Senhor Ministro Gilmar Mendes (Relator): Na espécie, o paciente foi denunciado por infração ao art. 33 da Lei de Drogas e art. 12 do Estatuto do Desarmamento, após policiais apreenderem seu aparelho celular e, ali, procederem à investigação no aplicativo *WhatsApp* , em que se verificaram trocas de conversas, cujo teor indicaria a traficância.

Em seguida, os agentes policiais ingressaram em seu domicílio, encontrando drogas e arma, o que gerou uma ação penal, com condenação do paciente em primeira instância, mantida pelo TJSP e STJ.

Ao julgar o recurso do paciente, a Quinta Turma do STJ registrou:

> "Em relação à ilicitude da diligência policial, em virtude do ingresso no domicílio do réu sem mandado judicial ou prévia autorização, a insurgência não deve prosseguir, porquanto da leitura do apelo defensivo, constata-se que a Corte estadual não se manifestou quanto ao ponto, impedindo manifestação deste Sodalício, em razão da falta de prequestionamento da matéria, a teor do enunciado sumular n. 282, do Supremo Tribunal Federal [...]
>
> Quanto à prova obtida a partir dos dados dos aparelhos telefônicos apreendidos, o eg. Tribunal de origem ressaltou que não há ilegalidade, uma vez que a necessidade de autorização judicial está restrita à interceptação de comunicação em andamento que não se confunde com o acesso aos dados armazenados no aparelho eletrônico". (eDOC 27, p. 4)

Destarte, o caso em questão trata dos limites da proteção aos dados registrados em aparelho celular através de aplicativos de troca de mensagens, bem como da inviolabilidade de domicílio.

Do sigilo das comunicações telefônicas e de dados e do direito fundamental à intimidade e à vida privada .

Conforme o art. 5º, XII, da CF, é inviolável o sigilo das comunicações telefônicas e de dados, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Por sua vez, a **inviolabilidade da vida privada e da intimidade** é afirmada pelo art. 5º, X, da Constituição Federal. Como leciona Paulo Gonet Branco, o " *sigilo das comunicações é não só um corolário da garantia da livre expressão de pensamento; exprime também aspecto tradicional do direito à privacidade e à intimidade"* (MENDES, Gilmar F.; BRANCO, Paulo G. G. **Curso de Direito Constitucional.** Saraiva, 2013. p. 293).

Tradicionalmente, a doutrina entendia que a inviolabilidade das comunicações não se aplicava aos dados registrados, adotando uma interpretação mais estrita da norma contida no art. 5º, XII, da CF/88.

Partia-se da compreensão que os dados em si não eram objeto de proteção, mas somente as comunicações realizadas.

Nesse sentido, vejam-se as distinções realizadas por Tercio Sampaio Ferraz:

> "O sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade. Isto é feito, no texto, em dois blocos: a Constituição fala em sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas. Note-se, para a caracterização dos blocos, que a conjunção e une correspondência com telegrafia, segue-se uma vírgula e, depois, a conjunção de dados com comunicações telefônicas. Há uma simetria nos dois blocos. Obviamente o que se regula é comunicação por correspondência e telegrafia, comunicação de dados e telefônica. O que fere a liberdade de omitir pensamento é, pois, entrar na comunicação alheia, fazendo com que o que devia ficar entre sujeitos que se comunicam privadamente passe ilegitimamente ao domínio de um terceiro. **Se alguém elabora para si um cadastro sobre certas pessoas, com informações marcadas por avaliações negativas, e o torna público, poderá estar cometendo difamação, mas não quebra sigilo de dados** . **Se estes dados, armazenados eletronicamente, são transmitidos, privadamente, a um parceiro, em relações mercadológicas, para defesa do mercado, também não está havendo quebra de sigilo** . Mas, se alguém entra nesta transmissão como um terceiro que nada tem a ver com a relação comunicativa, ou por ato próprio ou porque uma das partes lhe cede o acesso indevidamente, estará violado o sigilo de dados. A distinção é decisiva: o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação". (FERRAZ, Tercio S. Sigilo de

dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Cadernos de Direito Constitucional e Ciência Política,** n. 1, 1992).

Essa orientação foi incorporada pela jurisprudência do Supremo Tribunal Federal.

No julgamento do **HC 91.867/PA** (Segunda Turma, de minha relatoria, DJe 20.9.2012), destaquei a diferença entre *comunicação telefônica* e *registros telefônicos* , os quais receberiam proteção jurídica distinta.

Naquela oportunidade, defendi a impossibilidade de interpretar-se a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral, porquanto a proteção constitucional seria da comunicação, e não dos dados.

Creio, contudo, que a **modificação das circunstâncias fáticas e jurídicas** , a promulgação de **leis posteriores** e o significativo **desenvolvimento das tecnologias da comunicação, do tráfego de dados e dos aparelhos *smart phones*** leva, nos dias atuais, à solução distinta.

Ou seja, penso que se está diante de típico caso de **mutação constitucional** .

Questiona-se se o acesso a informações e dados contidos nos celulares se encontra ou não expressamente abrangido pela cláusula do inciso XII do art. 5º.

Contudo, ainda que se conclua pela não inclusão na referida cláusula, entendo que tais dados e informações encontram-se abrangidos pela proteção à intimidade e à privacidade, constante do inciso X do mesmo artigo.

Tratando sobre o direito à intimidade, José Adércio Leite Sampaio defende que:

> "Em geral, define-se o direito à intimidade como uma espécie de editoria das informações pessoais ou como um genérico 'direito a ser deixado em paz'. Ele é mais do que isso e mais bem se apresenta como um direito à liberdade, marcado por um conteúdo mais determinado ou determinável, conjugado a um complexo de princípios constitucionais, que nada mais são do que suas manifestações concretas. [...] **Afirmar que o ser humano é livre exige, não como seu**

> **pressuposto, mas como consectário, reconhecer seu domínio ou controle sobre os inputs e outputs de informação** . Esse sentido natural da liberdade se traduz, no mundo jurídico, na liberdade 'informacional' próxima ao que o Tribunal Constitucional Federal alemão chamou de *Informationelle Selbsstbestimmung*, ou autodeterminação em matéria de informação, que conjuga o aspecto negativo de não impedimento ao positivo, de controle". (In: CANOTILHO, J. J. Gomes; MENDES, Gilmar; SARLET, Ingo; STRECK, Lênio Luiz. **Comentários à Constituição do Brasil** , p. 292-293).

No âmbito infraconstitucional, as normas do art. 3º, II, III; 7º, I, II, III, VII; 10 e 11 da Lei 12.965/2014 – o marco civil da internet – estabelecem diversas proteções à privacidade, aos dados pessoais, à vida privada, ao fluxo de comunicações e às comunicações privadas dos usuários da internet.

A norma do art. 7º, III, da referida lei é elucidativa ao prever a inviolabilidade e sigilo das **comunicações privadas armazenadas (dados armazenados)** , *"salvo por ordem judicial"*.

Percebe-se, portanto, que a legislação infraconstitucional avançou para possibilitar a proteção dos dados armazenados em comunicações privadas, os quais só podem ser acessados mediante prévia decisão judicial – matéria submetida à reserva de jurisdição.

Entendo que o avanço normativo nesse importante tema da proteção do direito à intimidade e à vida privada deve ser considerado na interpretação do alcance das normas do art. 5º, X e XII, CF.

Tão importante quanto a alteração do contexto jurídico é a impactante transformação das circunstâncias fáticas, que trazem novas luzes ao tema.

Nesse sentido, houve um incrível desenvolvimento dos mecanismos de comunicação e armazenamento de dados pessoais em *smartphones* e telefones celulares na última década.

Nos dias atuais, esses aparelhos são capazes de registrar as mais variadas informações sobre seus usuários, como a sua precisa localização por sistema GPS ou estações de rádio base, as chamadas realizadas e recebidas, os registros da agenda telefônica, os dados bancários dos

usuários, informações armazenadas em nuvem, os *sites* e endereços eletrônicos acessados, lista de *e-mail* , mensagens por aplicativos de telefone, fotos e vídeos pessoais, entre outros.

Além disso, a conexão de todos esses aparelhos à rede mundial de computadores faz com que estejamos todos integralmente conectados, o tempo todo, fornecendo dados e informações para órgãos públicos e privados.

Conforme noticiado pelos meios de comunicação, os celulares são a principal forma de acesso dos brasileiros e cidadãos do país à *internet*. Esse motivo, por si só, já seria suficiente para concluir pela incidência das normas acima descritas no que toca à proteção dos dados, fluxos de dados e demais informações contidas nesses dispositivos.

Considerando essa nova realidade e defendendo a necessidade de decisão judicial para acesso aos dados contidos em aparelhos telefônicos, assenta-se na doutrina que:

> " **Do direito fundamental à privacidade protegido constitucionalmente extrai-se como princípio básico, que quanto mais grave for a intervenção, maiores devem ser os requisitos para a intervenção nesse direito e mais específica deve ser a lei que prevê tal interferência** Essa regra, deduzida do princípio da proporcionalidade, está presente também no inciso XII, do art. 5° da Constituição Federal, que exige a reserva legal qualificada para a intervenção na garantia da inviolabilidade do sigilo das comunicações telegráficas, de dados e das comunicações telefônicas, ao prescrever o requisito 'da ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal'.
>
> **Se o STF no RE 418.416/SC já entendeu que a garantia da inviolabilidade de sigilo do art. 5°, XII, referia-se à comunicação de dados e não aos dados em si, é porque certamente o cenário dos riscos ao cidadão era bastante diverso tendo em vista as tecnologias então existentes** . Afinal, usualmente os dados sofrem maior risco de interceptação durante o processo de comunicação – isto é, no tráfego – e não enquanto eles estão armazenados. Ocorre que com o advento da internet e dos aparelhos pessoais conectados em rede, a constelação de riscos alterou-se radicalmente e os programas espiões são o maior exemplo do risco de acesso clandestino e de manipulação dos dados armazenados em sistemas pessoais, que na vida moderna, guardam praticamente todas as informações a respeito de seu usuário. Nesse

> contexto, a efetividade da garantia constitucional da inviolabilidade do sigilo pressupõe que ela alcance também os dados armazenados em sistemas informáticos pessoais – tais como computadores, *smartphones* e agendas eletrônicas – cujo acesso passa a ser possível por meio desses programas e que podem acarretar riscos gravíssimos de monitoramento e vigilância ao cidadão sem que ele tome sequer conhecimento a respeito". (MENDES, Laura Schertel. **Uso de softwares espiões pela polícia: prática legal?** Disponível em: <//www.jota.info/opiniao-e-analise/artigos/uso-de-softwares-espioes-pela-policia-pratica-legal-04062015>. Acesso em 4.6.2015).

Os casos citados no referido artigo são paradigmáticos. Há, nos dias atuais, a possibilidade de inserção de *softwares* espiões em aparelhos celulares. A partir do telefone, pode-se verificar se determinada pessoa esteve ou não em determinado local, qual o percurso que ela percorreu e que *sites* acessou no caminho.

Câmeras de reconhecimento facial integradas à internet possibilitam o reconhecimento instantâneo de suspeitos. Algorítimos podem ser usados para prever e evitar crimes.

Esses avanços tecnológicos são importantes e devem ser utilizados para a segurança pública dos cidadãos e a elucidação de delitos . Contudo, **deve-se ter cautela, limites e controles para não transformar o Estado policial em um Estado espião e onipresente** , conforme descrito por George Orwell em seu livro "1984".

Importante ressaltar que o próprio STJ assentou, nos autos do RHC 89.981, a necessidade de autorização judicial para acesso a dados constantes do aplicativo *WhatsApp* , em acórdão publicado em 5.12.2017, de cujo teor extraio o seguinte trecho:

> "Contudo, embora a situação retratada nos autos não esteja protegida pela Lei n. 9.296/1996 nem pela Lei n. 12.965/2014, haja vista não se tratar de quebra sigilo telefônico por meio de interceptação ou de acesso a mensagens de texto armazenadas, ou seja, embora não se trate violação da garantia de inviolabilidade das comunicações, prevista no art. 5º, inciso XII, da Constituição Federal, houve sim violação dos dados armazenados no celular de um dos acusados. **De fato, deveria a autoridade policial, após a apreensão do telefone, ter requerido judicialmente a quebra do sigilo dos dados armazenados,**

haja vista garantia, igualmente constitucional, à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, prevista no art. 5º, inciso X, da Constituição Federal .

Assim, a análise dos dados armazenados nas conversas de *Whatsapp* , revela manifesta violação da garantia constitucional à intimidade e à vida privada, razão pela qual se revela imprescindível a autorização judicial devidamente motivada, o que nem sequer foi requerido ".

Destaque-se que essas recentes resignificações do direito à privacidade e à intimidade também têm sido objeto de intenso debate em outros países.

Em 2018, por exemplo, o Tribunal Constitucional alemão declarou a inconstitucionalidade da lei de proteção da Constituição do Estado de Nordrhein-Westfalen (NRW-VSG), que permitia à polícia daquela unidade da federação a realização de buscas ou investigações secretas e remotas em computadores de pessoas suspeitas de cometer ilícitos criminais, autorizando, ainda, o monitoramento de todas as atividades de suspeitos na internet. (MENKE, Fabiano. I *n:* MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, Inovação e Tecnologia,** p. 215-216).

Nesse julgamento, a Corte construiu o conceito do denominado direito fundamental da garantia da confidencialidade e integridade dos sistemas técnico-informacionais (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*).

Ou seja, decidiu a Corte alemã que os dados pessoais dos indivíduos não podem ser acessados de forma indiscriminada, devendo existir sistemas, procedimentos e instrumentos de controle contra esses acessos indevidos.

A Europa também possui uma avançada legislação sobre a proteção de dados (*General Data Protection Regulation* – GDPR) , recentemente aprovada, que dispõe sobre o livre consentimento no compartilhamento de dados e informações pessoais, a privacidade dos usuários e até mesmo a portabilidade das informações fornecidas.

Embora voltada para as relações entre os usuários da internet e as grandes empresas de comunicação, a legislação em questão evidencia a importância da proteção aos dados nos dias atuais.

Portanto, **entendo ser possível o acesso aos dados contidos em aparelhos celulares,** uma vez que não há uma norma absoluta de proibição da visualização do seu conteúdo, conforme se poderia extrair a partir de uma interpretação literal da norma contida no art. 5º, XII, da Constituição da República.

Não obstante, a proteção à intimidade e à vida privada contida no art. 5º, X, da CF/88, e a exigência da observância ao princípio da proporcionalidade nas intervenções estatais nesses direitos, impõem a revisão de meu posicionamento anterior, **para que o acesso seja condicionado à prévia decisão judicial.**

As normas do art. 3º, II, III; 7º, I, II, III, VII; 10 e 11 da Lei 12.965/2014 e as significativas alterações no contexto fático subjacente evidenciam se tratar de verdadeiro caso de **mutação constitucional** na interpretação do âmbito de proteção dos direitos estabelecidos no art. 5º, X e XII, da CF.

Da inviolabilidade de domicílio

Em relação à inviolabilidade de domicílio, o art. 5º, XI, da Constituição da República estabelece o seguinte:

> "XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial"

Interpretando a referida norma, o professor Paulo Gustavo Gonet Branco defende que *"o domicílio delimita um espaço físico em que o indivíduo desfruta da privacidade, em suas variadas expressões. Ali, não deve sofrer intromissão por terceiros, e deverá gozar da tranquilidade da vida íntima"* (MENDES, Gilmar Ferreira; BRANCO Paulo Gustavo Gonet. **Curso de Direito Constitucional.** p. 289).

O STF já declarou, em inúmeros precedentes, a ilicitude de provas obtidas com a violação a esse direito fundamental. No MS-MC, **o Ministro Celso de Mello** ressaltou que a garantia do art. 5º, XI, da CF/88 abrange: a) qualquer compartimento habitado; b) qualquer aposento ocupado de habitação coletiva; c) qualquer compartimento privado onde alguém exerce profissão ou atividade.

O conceito de domicílio abrange todo lugar privativo, ocupado por alguém, com direito próprio e de maneira exclusiva, mesmo sem caráter definitivo ou habitual, tratando-se de noção mais ampla do que aquela vigente no direito civil (MENDES, Gilmar Ferreira; BRANCO Paulo Gustavo Gonet. **Curso de Direito Constitucional.** p. 290).

No julgamento da AP 307-3, Rel. Min. Ilmar Galvão, DJ 13.10.1995, o STF declarou inclusive a ilicitude de prova apreendida em escritório particular, por entender que se estava sob a tutela da inviolabilidade de domicílio.

Desta feita, a violação à referida norma deve acarretar a nulidade dos elementos de prova eventualmente colhidos.

Do caso concreto

No presente *writ,* a ilegalidade verificada, segundo a defesa, decorre do fato de que, **após a abordagem do paciente, os policiais, ao apreenderem seu aparelho de celular, procederam à análise das conversas registradas no aplicativo *WhatsApp* .**

Dessa análise, verificaram que haveria traficância e, a partir daí, dirigiram-se à residência do paciente, onde apreenderam drogas e arma.

Foram apreendidos uma porção grande e três porções pequenas de maconha (74,70 gramas), um revólver calibre 38 com 5 projéteis intactos, 13 projéteis intactos, 5 *eppendorf* de cocaína, além de R$ 3.779,00 em moeda corrente.

Segundo a impetração, os policiais militares receberam denúncia anônima de tráfico de drogas, tendo se dirigido até o local de residência do paciente.

Lá, encontraram o réu sentado na calçada e procederam, de imediato, a busca em seu celular, oportunidade em que encontraram mensagens com informações suspeitas.

A partir daí, ingressaram no imóvel do paciente, oportunidade na qual se depararam com as drogas e a arma. O paciente alega que não autorizou o acesso ao seu aparelho celular e à sua residência. Defende, ainda, que seria usuário de drogas e que as substâncias entorpecentes seriam para consumo.

Em primeira instância, a juíza sentenciante, embora tenha reconhecido a **ilicitude do acesso às mensagens de *Whatsapp* do paciente,** afastou a nulidade das provas decorrentes pela ausência de prejuízo às investigações e existência de fontes independentes.

No mérito, absolveu o paciente da acusação de tráfico, reconhecendo a sua condição de usuário - art. 28 da Lei 11.343/2006. **Por conta do crime de posse ilegal de arma de fogo de uso permitido, o requerente foi condenado à pena mínima de 1 ano de detenção e 10 dias-multa, que foi convertida na prestação de serviços à comunidade.**

Contudo, o TJSP deu provimento ao recurso do Ministério Público para condenar o paciente às penas do art. 33, *caput* , da Lei de Tóxicos, fixada em 5 (cinco) anos de reclusão. O Tribunal aplicou **o redutor do §4º do art. 33 da Lei 11.343/2006** no percentual de um terço, fixando a pena em 3 (três) anos e 4 (quatro) de reclusão.

Determinou, ainda, a inclusão do paciente no regime fechado, **com base apenas no art. 2º, §1º, da Lei 8.072/1990.** Para tanto, a Corte deduziu que a decisão do STF que declarou a inconstitucionalidade da norma ocorreu de modo incidental, sem caráter vinculante.

O STJ deu provimento ao recurso especial para determinar a aplicação, no grau máximo, do redutor do §4º do art. 33 da Lei de Drogas e fixar o regime inicial aberto. Contudo, não analisou a questão da violação ao domicílio em virtude da não apreciação pelo TJSP e decidiu que a necessidade de autorização judicial **se restringe apenas às comunicações, mas não aos dados já registrados** .

Penso, contudo, que o caso merece solução distinta. **A nulidade das provas obtidas em virtude do acesso indevido ao telefone e à residência do paciente** foram deduzidas em primeira instância, tendo sido **reconhecidas na sentença de primeiro grau que, não obstante, constatou a suposta existência de provas autônomas** (eDOC 6).

Foi igualmente objeto de apreciação no julgamento da apelação, tendo sido afastada pelo Tribunal, conforme demonstra o trecho do voto do Desembargador Relator, abaixo transcrito:

> "[...] **a mera consulta aos apontamentos - dados constantes de aparelhos telefônicos ou qualquer outro objeto que realiza armazenamento de memória eletrônica não se confunde com a quebra**

> **do sigilo das comunicações de dados, cuja violação encontra obstáculo na Lei Fundamental** . E no caso em tela, a autoridade policial apenas consultou o teor das mensagens registradas no aplicativo **Whatsapp** do aparelho celular do réu, **cuja posse lhe era legítima.** Nesse sentido, o E. Superior Tribunal de Justiça [...]"

Pelo que se observa do acórdão proferido pelo TJSP, não restam dúvidas sobre o acesso imediato ao celular do paciente, sem prévia autorização judicial. A questão discutida nos autos não se refere ao revolvimento de matéria fático-probatória incapaz de ser apreciada em sede de *habeas corpus* , mas sim à própria qualificação jurídica dos fatos.

A transcrição da **sentença de primeiro grau** não deixa dúvidas quanto a essas circunstâncias (eDOC 6):

> "O réu, ouvido em Juízo, negou o delito de tráfico de entorpecentes, dizendo que as drogas encontradas eram para o seu consumo pessoal. Confessou a propriedade da arma. Contou que, no dia dos fatos, estava em frente de sua residência e os policiais o abordaram. **Em revista pessoal e em seu carro, nada foi encontrado. Indagado, ele disse que não tinha nada em casa. Os policiais pegaram seu celular e ingressaram em sua residência sem sua permissão. Como já estava dentro da casa, o réu mostrou onde estavam as drogas, a arma e o dinheiro.**
>
> [...] **A testemunha DAVID SERRADO DA SILVA JÚNIOR, policial militar, declarou em Juízo que recebeu denúncia de populares de que o réu comercializava drogas e possuía arma de fogo em sua residência.** No local dos fatos, com o réu nada foi encontrado. Indagado, ele nada respondeu. **Foi solicitada autorização ao réu para ver seu celular, com o intuito de verificar o IMEI** , pois atualmente há um procedimento para ver se o celular é roubado. **Seu colega de farda visualizou pedido possível de compra de drogas nas mensagens do celular** . Também foi autorizada a entrada dos policiais na residência [...]
>
> **Informalmente, o réu disse que comprou a arma por R$ 500,00 de uma pessoa de Ourinhos para defesa pessoal e, quanto à droga, o réu disse que vendia e que o dinheiro era proveniente da venda de droga** [...]"

Desta feita, uma vez que a apreensão das drogas e da arma, que ensejou a condenação do paciente, somente ocorreu após o acesso indevido a seu celular e o ingresso desautorizado em sua residência, concluo pela **ilicitude das provas que deram origem à apuração e de todo o processo penal, com base no art. 5º, X, XI e LVI, da CF/88 e nos fundamentos acima transcritos** .

Destaque-se que a **permissão de acesso direto a aparelhos telefônicos** , por autoridades policiais, pode servir de estímulo para que pressões indevidas sejam exercidas sobre os acusados para o fornecimento de senhas de acesso e informações confidenciais.

Não é incomum ouvir relatos de investigados que forneceram " **voluntariamente** " senhas de acesso a celulares ou prestaram depoimentos " **informalmente"** no momento da prisão e, posteriormente, na fase judicial do processo, afirmaram que, em realidade, foram pressionados a isso.

É exatamente o que ocorre no caso. Os policiais alegam que o paciente franqueou voluntariamente o acesso a seu celular e a sua residência. O paciente nega. Os agentes afirmam que o réu confessou, em "depoimento informal", o tráfico de drogas. O postulante se contrapõe a essa afirmação.

Nesse sentido, o acesso direto a aparelhos telefônicos e a residência de suspeitos, sem autorização judicial, fora das hipóteses de flagrante e com o não estabelecimento de procedimentos bem delimitados que garantam a observância dos direitos fundamentais dos indivíduos também conflita com o direito fundamental à não autoincriminação (art. 5º, LVII, da CF/88).

É por isso que essas medidas devem ser submetidas à prévia decisão judicial, enquanto garantia procedimental *in concreto* através da qual sejam analisados e registrados, especificamente, os fundamentos que possam afastar os direitos fundamentais envolvidos.

Ou seja, a existência de prévia decisão judicial é capaz de demonstrar a necessidade, adequação e proporcionalidade da pretensão dos órgãos de segurança de acesso aos dados, informações e residência dos suspeitos. Permite, ainda, o controle desses fundamentos.

A transcrição, assinatura e registro formal do depoimento dos investigados, com a declaração de ciência de seus direitos constitucionais, impede que investigações sejam realizadas e condenações sustentadas com base em confissões informais prestadas durante o ato de prisão e sob fortes suspeitas de violação de direitos.

Nesse sentido, entendo que o STF poderia caminhar para a criação de uma fórmula de garantia dos direitos das pessoas investigadas cuja inobservância leve à nulidade dos atos de investigação e coleta de provas, mesmo que durante o inquérito policial – tal como ocorreu no relevante precedente estabelecido pela Suprema Corte dos Estados Unidos em 1966, no julgamento do caso *Miranda v. Arizona* (384 U.S. 436).

Nesse precedente, a Suprema Corte dos Estados Unidos decidiu que a acusação **não poderia se utilizar de declarações obtidas por agentes policiais após a apreensão ou detenção de acusados, sem a demonstração da utilização de procedimentos que evidenciassem a proteção contra a autoincriminação** prevista na Quinta Emenda à Constituição dos Estados Unidos.

Registrou-se, como *ratio decidendi* , que a incomunicabilidade existente nos interrogatórios policiais nos Estados Unidos constituiria um **ambiente intimidatório que diminuiria o direito à não incriminação** . **E que o fato de o indivíduo sob investigação responder a algumas perguntas durante o interrogatório não significaria que ele abriu mão desse direito, que pode ser invocado posteriormente.**

Outro relevante precedente estabelecido pela Suprema Corte dos Estados Unidos, e que pode servir de norte à consolidação de uma jurisprudência brasileira que favoreça os direitos em análise, ocorreu no julgamento do caso *Mapp v. Ohio* 367 U.S. 643, de 1961, no qual se decidiu que **toda prova obtida a partir de uma busca e apreensão em violação à Constituição não seria judicialmente admitida.**

É o que ocorre no caso em análise, no qual todas as provas foram obtidas a partir do acesso indevido às comunicações de *Whatsapp* e à residência do paciente.

Por esses motivos, **concedo a ordem para declarar a nulidade das provas obtidas mediante o acesso indevido ao aplicativo *WhatsApp* e à residência do paciente e, constatada a derivação de todas as demais provas , declaro nulo o processo, determinando o trancamento da ação e a absolvição do paciente.**

É como voto.