EXCELENTÍSSIMO SENHOR MINISTRO RELATOR DO ARE nº 1.042.075/RJ–RG.

ARE 1.042.075/RJ-RG
RECORRENTE: MINISTÉRIO PÚBLICO DO ESTADO DO RIO DE JANEIRO
RECORRIDO: GUILHERME CARVALHO FARIAS
(DEFENSORIA PÚBLICA DO ESTADO DO RIO DE JANEIRO)
RELATOR: MINISTRO DIAS TOFFOLI

MEMORIAIS

1. Trata-se de caso em que a autoria de crime de roubo circunstanciado (CP, art. 157, §2º, I e II) veio a ser descoberta após acesso a *dados* armazenados em telefone celular (de tipo *smartphone*) que o agente deixou cair no local dos fatos. De posse do aparelho celular, a vítima o entregou à polícia que, *sem autorização judicial*, logrou desbloquear/acessar os dados gravados na memória do aparelho e, com isso, identificar o agente da conduta delitiva. Condenado em primeira instância e absolvido em grau de apelação pelo reconhecimento de ilicitude da prova assim obtida, o Recurso Especial acusatório veio a ser inadmitido, assim como o Extraordinário; interpondo-se o presente ARE, afetado por Repercussão Geral.

2. A questão de fundo, em síntese, diz respeito ao alcance do art. 5º, incisos X e XII da Constituição da República, bem como da Lei 9.296/96 que regulamenta este último. Também outros dispositivos constitucionais e legais auxiliam o intérprete no enfrentamento do tema, como o art. 5º, inciso IV e a Lei nº 12.965/14. Em outros termos, trata-se de saber se é lícita a "perícia" realizada em celular (*smartphone*) encontrado no local do crime por autoridade policial sem autorização judicial.

3. É certo que o tema já fora visitado pela **2ª Turma do STF** ao julgar (em 24.04.2012) o **HC 91.867/PA** – relatoria do Min. GILMAR MENDES. Derivado de **caso concreto ocorrido em 2004**, foi considerado lícito o acesso ao histórico de ligações telefônicas armazenado no aparelho celular (de propriedade de um dos acusados) apreendido pela polícia *no momento do flagrante*, o que tornou possível chegar a coautor de crime de homicídio. Contudo, importa ressalvar que, **à época (2004), os**

aparelhos de telefonia celular não eram, como hoje, microcomputadores multiuso de bolso (*smartphones*) que soem armazenar "a vida inteira" de seus portadores e não apenas agenda telefônica e algumas poucas mensagens de texto (SMS).

4. Em decisões calcadas em fatos mais recentes, o **STJ** também enfrentara o tema. No **RHC nº 51.531/RO**, de relatoria do Min. NEFI CORDEIRO, **a 6ª Turma declarou a nulidade das provas obtidas sem autorização judicial**, i.e., após a apreensão do aparelho pela polícia por ocasião da prisão em flagrante (ocorrida em 18.03.2014). Considerou ilícita tanto a devassa dos dados como das conversas de *whatsapp*, determinando o seu desentranhamento dos autos.

5. No **RHC nº 51.531/RO**, releva salientar as contribuições lançadas pelo Min. ROGÉRIO SCHIETTI em seu **voto-vista**, onde, aludindo ao HC julgado pela 2ª Turma do STF (HC 91.867/PA), observa no voto do Min. GILMAR MENDES expressa referência ao fato de que as "autoridades policiais não tiveram, em nenhum momento, acesso às conversas mantidas entre os pacientes e o executor do crime..." para distinguir entre dois tipos de dados protegidos: os *dados gravados no aparelho* e os *dados contidos nos aplicativos de comunicação* instantânea (Whatsapp, Telegram etc...).

6. Prossegue, então, o Min. SCHIETTI: "Por isso, **o precedente do HC n. 91.867/PA não é mais adequado para analisar a vulnerabilidade da intimidade dos cidadãos na hipótese da apreensão de um aparelho de telefonia celular em uma prisão em flagrante.**" (grifo no original). Salienta o Ministro SCHIETTI que o caso se assemelha ao julgado pela Suprema Corte dos EUA (*Riley* vs. *California*), no qual se decidira que o acesso ao smartphone do suspeito viola o seu direito à privacidade porque, agora, a tecnologia permite "que um indivíduo transporte essas informações em sua mão [e isso] não torna a informação menos digna de proteção". Embora reconheça que o tema é novo e "sujeito a oscilações", acompanhara o relator no **RHC 51.131/RO**, reconhece que "o acesso aos dados do celular e às conversas de *whatsapp* sem ordem judicial constituem devassa e, portanto, violação à intimidade do agente", para declarar a "nulidade das

provas obtidas pelo exame do celular do paciente sem autorização judicial, cujo produto deve ser desentranhado dos autos".

7. Ainda no **RHC 51.131/RO**, também a Min. MARIA THEREZA DE ASSIS MOURA manifestou-se em voto-vista e também aludiu ao precedente da 2ª Turma do STF para pontuar que o inciso XII do art. 5º protege a *comunicação de dados,* mas não *os dados em sim mesmos*. Todavia, prossegue a Ministra: "Isso não significa, por outro lado, que os dados armazenados em um aparelho de telefone celular estejam desprovidos de qualquer proteção constitucional. Pelo contrário. Nos tempos que correm, os chamados *smartphones,* dotados de elevada capacidade de armazenamento e amplas funcionalidades, contém invariavelmente uma elevada quantidade de dados pertinentes à esfera íntima de privacidade do seu titular." A proteção constitucional a que se referira a Ministra está insculpida no inciso X do art. 5º da Constituição da República.

8. Anote-se que a Ministra também se refere a julgados internacionais no enfrentamento da matéria. A Suprema Corte do Canadá "ao decidir R. vs. Fearon (2014 SCC 77, [2014] S.C.RR. 621) entendeu, por maioria de 4 votos a 3, pela legitimidade do acesso pela polícia aos dados armazenados em aparelho celular, sem a necessidade de prévia ordem judicial, quando realizado tal acesso na sequência de uma prisão em flagrante." **A hipótese é distinta da versada neste ARE, aqui a [questionável] prisão em flagrante se dera *após e em decorrência* do acesso aos dados**. Além disso, no caso *Kevin Fearon*, a excepcionalidade de tal tipo de acesso é sublinhada e **deve vir acompanhada de registros que possibilitem o seu controle ulterior**, o que inocorreu *in casu*. Vejamos: "Na minha opinião, dado que estamos lidando aqui com uma pesquisa extraordinária que não requer nem um mandado, nem argumentos razoáveis e prováveis, a obrigação de manter um registro cuidadoso do que é pesquisado deve ser imposta como uma questão de imperativo constitucional. O registro deve geralmente incluir os aplicativos pesquisados, a extensão do serarca, o tempo da busca,

seu purismo e sua duração."[1]. **Nada disso foi feito, no contexto dos fatos tratados pelo presente ARE. O modo de acesso aos dados é extraído das declarações prestadas por uma testemunha (Policial Civil MAYKE[2]) motivo pelo qual o mesmo deve ser improvido mantendo-se a ilicitude da prova tal como obtida.**

9. O segundo precedente internacional invocado é extraído do Tribunal Constitucional da Espanha, pontuando a Ministra MARIA THEREZA que o pretório espanhol "ressaltou que o caso era de uma ´ingerência leve´ na intimidade, pois somente a agenda telefônica foi examinada, de modo que, à luz do princípio da proporcionalidade, a medida deveria ser admitida como válida. Consignou-se que a situação seria diversa se o exame houvesse sido aprofundado para outras funções do aparelho, quando então estaria em jogo uma invasão mais substancial da privacidade, a demandar um parâmetro ´especialmente rigoroso´ de verificação de observância ao princípio da proporcionalidade." Registre-se que o caso concreto deste ARE aponta para a devassa de *arquivos de imagem* e também de *registros de chamadas* (vide item 12 infra – conf. nota de rodapé nº 2), **a denotar não apenas uma "ingerência leve" *in casu,* como no citado julgado espanhol, até porque envolveu o levantamento de dados de terceira pessoa (suposta namorada do suspeito)**.

10. O voto da Ministra ainda faz referência a dispositivos da Lei 9.472/97 (art. 3º, V) e da Lei 12.695/14 (art. 7º, III) e pontua a distinção entre o acesso a dados de um *smartphone* e aqueles julgados tanto no HC 91.867 do STF quanto pelo Tribunal Constitucional espanhol. Conclui que, "a depender do caso concreto, caso a demora na obtenção de um mandado judicial pudesse trazer prejuízos concretos à investigação ou especialmente à vítima do delito, mostre-se possível admitir a validade da prova colhida

[1] No original: "*In my view, given that we are dealing here with an extraordinary search oiwer that requires neither a warrant nor reasonable anda probable grounds, the obligation to keep a careful record of what is searched should be imposed as a matter os constitucional imperative. The record should generally nclude the applications searched, the extent of the serarch, the time of the search, its purose and its duration.*"

[2] Transcrição parcial de suas declarações consta do acórdão absolutório proferido pela Sexta Câmara Criminal do Tribunal de Justiça do Estado do Rio de Janeiro.

através do acesso imediato aos dados do aparelho celular. Imagine-se, por exemplo, um caso de extorsão mediante sequestro, em que a polícia encontre aparelhos celulares em um cativeiro recém-abandonado: o acesso *incontinenti* aos dados ali mantidos pode ser decisivo para a libertação do sequestrado."

11. Dos aportes jurisprudenciais que reputamos pertinentes destacar, **percebe-se uma aproximação da questão jurídica a partir de *distinções* relacionadas ao caso concreto**, o qual deve ser sempre levado em conta em suas minúcias e circunstâncias e ineditismo. Assim, procura-se distinguir **(i)** entre *dados* e *comunicação de dados* [como no HC 91.867/PA]; ou **(ii)** entre os aparelhos de telefone antigos e os modernos *smartphones* [voto-vista do Min. SCHIETTI no RHC 51.131 e caso *Riley* – Suprema Corte dos EUA]; ainda **(iii)** uma distinção relacionada à urgência no acesso aos dados [voto-vista da Min. MARIA THEREZA no RHC 51.131 e caso *Riley* – Suprema Corte dos EUA]; e outra **(iv)** se se trata de objeto apreendido num situação de flagrante ou não [conforme decisão da Suprema Corte canadense], cabendo questionar-se neste caso se seria imprescindível mandado específico para acesso aos dados do objeto apreendido.

12. Assim, no caso deste ARE 1.042.075, tem-se, a partir das distinções acima delineadas: que a polícia acessou (i) ***dados*** **de um** (ii) ***smartphone*** (iii) **sem que houvesse urgência justificável e** (iv) **fora de uma situação flagrancial.** Em que pese ter sido lavrado auto de prisão em flagrante em desfavor do acusado, está claro que só se chegou ao mesmo a partir da *devassa* em seu telefone celular (fortuitamente abandonado na cena do crime)[3] que envolvera, inclusive, os dados de terceira pessoa.

13. O *cotejo entre as circunstâncias concretas e a análise jurisprudencial aponta para ilicitude da prova obtida mediante acesso ao celular do acusado*,

[3] Neste sentido, confira-se o seguinte trecho da sentença condenatória (reformada em grau de apelação): "*Que no celular fornecido pela vítima tinham fotos do acusado e, além disso, pelo registro de ligações conseguiram o telefone fixo da namorada do acusado, e que assim, por uma consulta, conseguiu o nome dessa jovem e descobre então que esta havia visitado um indivíduo na cadeia. Que imprimiu a foto desse indivíduo e a vítima o reconheceu sendo o autor do fato.*" (e-DOC. 3 VOL. p. 32)

sendo certo que o único elemento de convicção capaz de refrear essa conclusão a partir dos precedentes citados é a caracterização do achado policial no telefone do agravado como *dado* e não como *dado comunicado* nos termos da distinção inaugurada por ocasião do julgamento do HC 91.867/PA pela 2ª Turma do STF, cuja decisão, não se olvide, não serve de paradigma ao presente caso, como destacaram os votos-vista (no RHC 51.131/RO) da Ministra MARIA THEREZA DE ASSIS MOURA e do Ministro ROGÉRIO SCHIETTI, insistimos.

14. Neste escorço jurisprudencial, pedimos vênia para colacionar, ainda, o acórdão proferido pela Quinta Câmara Criminal do TJRJ (HC nº 0046727-85.2018.8.19.0000) analisando situação na qual "agentes da lei apreenderam telefones celulares, utilizando-se de mensagens de Whatsapp sem autorização judicial", assim ementado no ponto de interesse:

> ***HABEAS CORPUS*. ASSOCIAÇÃO PARA O TRÁFICO ENVOLVENDO ADOLESCENTE (ARTIGO 33 C.C. ARTI-GO 40, VI DA LEI 11343/06). RELAXAMENTO DA PRISÃO DEFERIDA EM SEDE DE LIMINAR. CONSOLIDAÇÃO. VIOLAÇÃO DE DOMICÍLIO. NÃO CONFIGURAÇÃO. TRANCAMENTO DA AÇÃO PENAL. IMPOSSIBILIDADE. APREENSÃO DE APARELHOS CELULARES. VIOLAÇÃO DO SIGILO DE DADOS. NECESSIDADE DE AUTORIZAÇÃO. AUSÊNCIA. CONCESSÃO PARCIAL DA ORDEM.**
>
> Inicialmente, bom consignar que em sede de Plantão Judiciário, foi deferida, parcialmente, a liminar, com o relaxamento da prisão dos pacientes e imposição das medidas cautelares de comparecimento mensal em juízo até o dia 10 de cada mês para informar e justificar atividades, bem como a todos os atos para os quais forem intimados e, ainda, proibição de mudar de endereço sem comunicar ao Juízo de origem e de ausentar-se do Estado por mais de 08 dias sem prévia autorização judicial, conforme decisão já transcrita às fls. 100/103 e, diante de seu acerto, será mantida.
>
> Ultrapassadas tais considerações, a Defensoria Pública sustenta, neste remédio heroico, a ocorrência de violação de domicílio na empreitada policial, bem como afirma que os agentes da lei apreenderam telefones

celulares, utilizando-se de mensagens de WathsApp sem autorização judicial, evidenciando-se, assim, a ilicitude das provas angariadas, pleiteando, em decorrência da ilicitude, além do relaxamento da custódia cautelar dos pacientes (o que foi concedido em sede de liminar), o trancamento da ação penal e, subsidiariamente, a exclusão das mensagens obtidas por meio ilícito. [...]

PEDIDO SUBSIDIÁRIO DE DESENTRANHAMENTO DA PROVA OBTIDA SEM AUTORIZAÇÃO (MENSAGENS DO WHATSAPP). Noutro giro, assiste razão à Defesa ao pretender a exclusão e o desentranhamento da prova obtida mediante violação do sigilo de dados e comunicações telefônicas, diante da violação ao disposto no artigo 5º, incisos X e XII, da Constituição Federal, cujo texto consagra, dentre outras garantias fundamentais, a inviolabilidade da intimidade, o sigilo das comunicações telegráficas, de dados e das comunicações telefônicas, excepcionando-se, neste último caso, tal premissa, somente, por ordem judicial e nas hipóteses e forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Cabe ressaltar, também, que a Lei nº 12.965/14, estabelece os princípios, garantias e deveres para o uso da Internet no Brasil. E prevê, em seu artigo 7º, inciso III, dentre os direitos assegurados aos usuários da rede mundial, "a inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial".

In casu, segundo a denúncia, em revista pessoal dos pacientes e dos dois adolescentes, foram encontrados cinco aparelhos celulares contendo mensagens sobre tráfico de drogas e alertas sobre a localização dos agentes da lei. Noutras palavras, o acesso aos dados armazenados no aparelho celular dos pacientes ocorreu sem sua autorização e ao arrepio da garantia constitucional ínsita no artigo 5º, inciso X, da Constituição da Repú-blica, de forma a justificar a declaração de nulidade da prova obtida durante a diligência policial, o que, por consequência, determina-se o seu desentranha-mento, como requerido pela Defensoria Pública. Precedentes do Superior Tribunal de Justiça e desta Câmara de Justiça.

> Destaque-se, também, que na decisão que concedeu, parcialmente, a liminar, relaxando a prisão dos pacientes, contém o registro de que **"Não foi delineada, portanto, especificamente em relação aos ora pacientes, situação flagrancial prévia à apreensão dos aparelhos de telefonia celular e mesmo que assim não fosse, a violação aos sigilo de dados e à intimidade não estaria autorizada, já que os direitos fundamentais em comento encontram-se recobertos por cláusula de reserva de jurisdição, estabelecida no artigo 5º, XII, da Constituição da República".** [...] (HC nº 0046727-85.2018.8.19.0000, Quinta Câmara Criminal do TJRJ, Rel. Des. Denise Vaccari Machado Paes, Julg. 25.10.18. Public. 31.10.2018) – negritos no original; sublinhados nossos.

15. Portanto e ademais, na esteira da jurisprudência colacionada enquanto paradigmática no caminho de se enfrentar adequadamente o tormentoso tema, releva trazer à baila outro *recente* julgado da Suprema Corte estadunidense. Referimo-nos ao caso *Carpenter v. Estados Unidos (nº 16-402. Discutido em 29.11.2017 e decidido em 22.06.2018).* Neste, o FBI obteve das companhias de telefonia celular, os registros das torres de celular do acusado (Timothy Ivory Carpenter). Os dados foram obtidos *diretamente* pelos investigadores com amparo no *Stored Communication Act* e permitiram concluir que o telefone de T. Carpenter esteve conectado a torres localizadas próximas aos locais e no horário dos roubos investigados. A defesa de Carpenter sustentara ofensa à Quarta Emenda[4], sendo certo que, antes do caso chegar à Suprema Corte, instâncias inferiores haviam entendido que a obtenção dos registros não feria o mencionado dispositivo porque o usuário do serviço de telefonia compartilhava voluntariamente os dados de sua localização com as operadoras de celular "*como um meio de estabelecer comunicação*".

[4] Emenda IV (Ratificada em 15 de Dezembro de 1791): O direito do povo à inviolabilidade de pessoas, casas, documentos e propriedade pessoal contra buscas e apreensões não razoáveis não deve ser violado, e não devem ser emitidos mandatos a não ser com causa provável apoiada por juramento ou declaração e descrevendo especificamente o local da busca e as pessoas ou coisas a serem apreendidas. (No original: "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searchs and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particular describing the place to be searched, and the persons or things to be seized.*")

15. Trata-se de situação diversa do emblemático caso *Riley.* Neste, a Corte reconhecera a *imensa capacidade de armazenamento de telefones celulares modernos ao sustentar que os policiais devem, em regra, obter um mandado judicial antes de vasculhar o conteúdo de um telefone.* De acordo com a Suprema Corte dos EUA, embora a regra geral permita a busca incidente à prisão por atingir um equilíbrio adequado no contexto de objetos físicos – situação agasalhada pelo inciso II, do art. 6º e pelo art. 244 do nosso CPP –, nenhuma de suas justificativas tem muita força em relação à vasta quantidade informações sensíveis contidas num telefone celular.

16. No caso *Carpenter,* a partir do entendimento histórico "do que foi considerado uma busca e apreensão desarrazoada quando a Quarta Emenda foi adotada" (*Carrol v. United States*, 267 U.S. 132, 149 - 1925), a Corte pontuou que a Quarta Emenda busca assegurar "as privacidades da vida" contra o "poder arbitrário" (*Boyd v. Unites States*, 116 U.S. 616,630 – 1886) e que um dos objetivos centrais dos Fundadores era "colocar obstáculos no caminho da vigilância policial demasiadamente ostensiva" (*United States v. Di Re*, 332 U.S. 581, 595 – 1948). Tudo para concluir que tais vetores devem ser observados na aplicação da Quarta Emenda em relação às inovações das ferramentas de vigilância, a fim de "assegurar a preservação desse grau de privacidade contra o Governo que existia quando a Quarta Emenda foi adotada" (*Kyllo v. United States*, 355 U.S. 27,34 – 2001), rejeitando uma interpretação mecânica do dispositivo.

17. Assim, no caso *Carpenter* a Suprema Corte dos EUA se distanciará da "*doutrina da terceira parte*" (quando o proprietário das informações a compartilha voluntariamente com terceiros – equiparados a testemunhas). Por esta doutrina, não há uma expectativa razoável de privacidade, "mesmo se a informação é revelada [a terceiros] pressupondo que será utilizada apenas para um propósito limitado" (*United States v. Miller*, 425 U.S. 435, 443 – 1976), no caso um banco (instituição financeira), cujos registros foram acessados diretamente pela investigação sem uma ordem

judicial. No caso *Miller*, entendeu-se que não houve ofensa à Quarta Emenda porque os dados já haviam sido compartilhados com o banco.

18. Já no caso *Smith*, igualmente entendeu-se não violar a Quarta Emenda o compartilhamento de dados com uma companhia telefônica (e não com um banco): com o auxílio de um dispositivo eletrônico ("*pen register*") acoplado a um telefone fixo, o Governo obtinha os registros de ligações efetuadas pelo investigado. Segundo a Corte, nestas circunstâncias, a expectativa de privacidade do chamador "não é aquela que a sociedade está preparada para reconhecer como razoável" até porque se sabe que as companhias telefônicas utilizam esses números "para uma variedade de fins comerciais legítimos", de modo que considerou que o réu "assumiu o risco" de que os registros da empresa pudessem ser "cedidos à polícia" (*Smith v. United States*, 442 U.S., 743 e 745).

19. Com os registros relativos a um s*martphone* é diferente. Dados de localização no espaço e no tempo registrados nas torres geridas pelas operadoras de telefonia celular imprescindem de autorização judicial para serem acessados pelo Estado. Eis o que restou decidido no caso *Carpenter*. O telefone celular é quase uma "característica da anatomia humana" (*Riley,* 573 U.S.) porque "os indivíduos carregam compulsivamente seus celulares consigo o tempo todo", de modo que o aparelho "segue fielmente seu dono para além das vias públicas e adentram residências particulares, consultórios médicos, sedes de partidos políticos, e outros locais potencialmente reveladores", logo "quando o Governo rastreia a localização de um telefone celular, atinge um nível de vigilância quase perfeito, como se tivesse colocado uma tornozeleira eletrônica no tornozelo do usuário de telefone celular"[5].

19. Este pequeno panorama do entendimento da Suprema Corte estadunidense, revela que **a inovação tecnológica que nos trouxe até os hodiernos**

[5] Anote-se que o modelo de *smartphone* da empresa Apple se chama IPhone, em tradução livre: "Eu-telefone", a proporcionar uma espécie de *self* do proprietário incorporado no aparelho.

hábitos sócio-comportamentais relacionados ao uso de *smartphones* estão a demandar interpretação adequada às garantias fundamentais insculpidas nos incisos XII e X do art. 5º da Constituição da República, pena de superdimensionar a vigilância do Estado em detrimento do direito à intimidade e à privacidade do indivíduo, mesmo em se tratando de *dados* compartilhados com terceiros (caso *Carpenter,* quando a Corte exige o mandado judicial; não basta a requisição direta, ainda que amparada no *Stored Communications Act*) e registrados no aparelho (não apagados). Por isso, reitere-se: **o precedente do HC 91.867/PA é anacrônico aqui** (assemelha-se ao caso *Smith*, quando o acesso se dera ao número de telefone discado num aparelho "grampeado" pela "*pen register*", permitindo acessar o histórico de registros de chamadas), embora *in casu* também tenha havido acesso ao registro de chamadas do celular do acusado. Trata-se, neste ARE, de dupla violação, em síntese.

20. Por isso também, é preciso que a jurisprudência do STF esteja atenta às peculiaridades de acesso a dados armazenados em *smartphones*. No contexto fático que culminou com a impetração do HC 91.867/PA, a polícia acessara o histórico de chamadas armazenado no aparelho para se chegar a um *dado não comunicado* (número de telefone de terceiro, identificado como coautor dos fatos) porque simplesmente gravado na memória do telefone (histórico de chamadas). Foi o que permitiu a *analogia* com um registro impresso ou escrito (uma caderneta), uma anotação em papel, um bilhete ou uma carta[6]. Sobre essa *analogia*, releva anotar o comentário de TÉRCIO SAMPAIO FERRAZ JR. às ponderações formuladas por JULIANO MARANHÃO em palestra reduzida a escrito e transformada em artigo, *in verbis*:

[6] Trata-se do seguinte trecho do voto do Min. Relator, GILMAR MENDES: "ad argumentandum*, abstraindo-se do meio material em que o dado estava registrado, o aparelho celular, indago: e se o número estivesse em um pedaço de papel no bolso da camisa usada pelo réu no dia do crime, seria ilícito o acesso pela autoridade policial? E se o número estivesse anotado nas antigas agendas de papel ou eu um caderno que estava junto com o réu no momento da prisão? Ademais, impende lembrar que a CF excepcionou a inviolabilidade domiciliar na hipótese de flagrante delito. A própria liberdade sofre restrição no flagrante delito. Um aparelho celular receberia proteção diversa?*"

> "Eu reconheço que a dificuldade, que na minha época não me parecia tão difícil assim, está em você lidar com a comunicação telemática, vamos chamar assim, em termos de separar o *fluxo* do *resultado*. Eu reconheço, é muito difícil fazer isso tecnicamente falando. Agora, na cabeça de quem estudou direito dentro do outro mundo, as soluções acabam sendo deste jeito, só que elas acabam, por assim dizer, saindo um pouco pela tangente, porque você não consegue, diferentemente de outras situações lidar com essa separação de uma maneira clara.
>
> O exemplo da armazenagem poderia dar uma certa força à analogia: *aquilo que você armazena é, para assim dizer, o resultado da comunicação*; o *fluxo* é diferente dessa armazenagem. Só que essa armazenagem, ao contrário do mundo físico, não é algo que está ali e que é diferente do próprio fluxo, esse é o problema. Ou seja, a ideia de original e cópia, nesse mundo, não funciona mais desse jeito, você não tem mais o autêntico e depois a cópia, a cópia em termos informáticos é absolutamente inseparável do 'original', o que talvez nos dê essa medida de dificuldade entre você separar o fluxo da própria armazenagem. Quer dizer, no fundo é a mesma coisa e só com um artifício, na hora de tomar a decisão, é que você olha para o celular e diz 'é como se fosse um caderninho de notas'. Não é um caderninho de notas, é completamente diferente."[7]

21. No caso destes autos, além da fotografia do acusado, fora acessada *também* o histórico de chamadas do celular. Sequer se pode ter certeza do local, no smartphone, de onde os dados foram encontrados. No álbum de fotografias (onde seria considerado "mero" *dado*)? Numa conversa de aplicativo (onde estaria inserido num fluxo ou resultado desse fluxo comunicacional)? – o que se sabe por conta das declarações prestadas por uma das testemunhas atuantes nas diligências que precederam o *questionável flagrante* lavrado em desfavor do acusado como dito no itens 10 e 12 (conf. notas de rodapé 2 e 3) – a envolver terceira pessoa na celeuma

[7] "O que é dado não comunicado?" in ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (eds.) Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. I. São Paulo, InternetLab, 2018; pp. 53 e 54. (grifamos)

jurídica, o que não passou despercebido pela arguta reflexão do professor SAMPAIO JR., que prossegue no parágrafo imediatamente após ao citado acima:

> "Por enquanto a gente trata desse jeito, só que quando você trata desse jeito, você acaba interferindo em inviolabilidades que antes você conseguia separar. No seu caderninho de notas provavelmente você não teria a possibilidade de cometer uma incursão na vida de terceiros como aconteceu em tornar pública uma delação premiada desse jeito. Ela não está mais em um registro policial, papel etc. ela está em outro registro e ali a dificuldade está em como é que você protege as diferentes individualidades?"[8]

22. E **não há mesmo qualquer laudo ou registro policial capaz de permitir o controle, mesmo *a posteriori*, da devassa realizada no *smartphone* como determinado pela Suprema Corte canadense (caso *Kevin*) nas situações que a urgência e a dinâmica do caso concreto venha a exigir pronto e imediato acesso aos dados**. *In casu,* além de se dar sem qualquer urgência justificável, a devassa acabou alcançando terceira pessoa (identificada como namorada do acusado) quando era perfeitamente possível a obtenção de prévia autorização judicial, respeitando-se a cláusula de reserva de jurisdição (CR, art. 5º, inciso XII, *in fine*) e, em última análise, a garantia constitucional.

23. O que não se pode admitir, *concessa maxima venia*, é a conclusão – adotada pelo relator no julgamento do HC nº 91.867/PA, apoiada na *teoria da descoberta inevitável* –, de que o acesso *direto* aos dados contidos no *smartphone* do agravado estaria agasalhado pelo disposto no §2º do art. 157 do Código de Processo Penal porque, cedo (violando o direito constitucional) ou tarde (obtendo mandado judicial) chegariam o agravado do mesmo jeito. Isto não é verdade. *In casu*, o cotejo da fotografia [apresentada à vítima em *show up*[9]] com o acesso a ligações efetuadas para

[8] *Idem*; p. 54.

[9] Prática que, aliás, contraria a literatura científica referente ao tema do reconhecimento de pessoas. Vejamos: "No reconhecimento por show-up, somente um suspeito é apresentado à pessoa para que faça o reconhecimento. Muitas vezes, esse tipo de procedimento é utilizado quando a polícia tem praticamente certeza que a pessoa é culpada ou quando o suspeito for conhecido da testemunha. O show up também costuma ser utilizado quando o suspeito é preso

terceira pessoa é que *determinou* a linha de investigação. Esta não seria trilhada não fosse a violação da privacidade (CR, art. 5º, X) do agravado.

24. Não havia risco à integridade física dos policiais ou da vítima. A devassa nos dados, além disso, permitiu a lavratura de um auto de prisão em flagrante ao arrepio das hipóteses dos incisos do art. 302 do Código de Processo Penal. Aqui, o seguinte trecho da decisão da Suprema Corte dos EUA no caso *Riley* é ilustrativo: "O fato de que a tecnologia agora permite que um indivíduo carregue essa informação em sua mão não torna a informação menos digna da proteção pela qual os Fundadores lutaram. Nossa resposta para a pergunta sobre o que a polícia deve fazer antes de procurar um telefone celular apreendido durante uma detenção é simples - obtenha um mandado."[10] No presente, sequer houve detenção prévia.

25. Evidente que situações de risco iminente, de urgência, constituem exceções à regra, como já ventilamos no presente arrazoado ao colacionar o voto-vista da Ministra MARIA THEREZA DE ASSIS MOURA no HC 51.531/RO, preocupação que também não escapou da Suprema Corte norte-americana no caso *Riley*: "Tais exigências podem incluir a necessidade de impedir a destruição iminente de provas em casos individuais, perseguir um suspeito em fuga, ajudar pessoas que estão gravemente feridas ou são ameaçadas de ferimentos iminentes."[11]

---

logo em flagrante. Mesmo nestas condições, o suspeito deve ser apresentado à testemunha/vítima fora de um contexto sugestivo que seria, por exemplo, aparecer dentro de uma viatura, ou estar algemado com policiais ao lado (IDETIFYING THE CULPRIT, 2014). Já os especialistas (LINDSAY et al., 2007) são unânimes em não recomendar a técnica de show-up, em função do potencial bastante grande de erro de reconhecimento (LAWSON; DYSART; 2014)." *in* Avanços Científicos em Psicologia do Testemunho Aplicados ao Reconhecimento Pessoal e aos Depoimentos Forenses. Disponível em: http://pensando.mj.gov.br/wp-content/uploads/2016/02/PoD_59_Lilian_web-1.pdf

[10] No original: "*The fact thar technology now allows an individual to carry such information in his hand doen not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple - get a warrant.*"

[11] No original: "*Such exigencies could include the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, an to assist persons who are seriously injures or are threatened with imminente injury.*"

26. No caso concreto, porém, deu-se justamente o oposto. Nenhum risco havia. Sequer se poderia falar da existência de um "suspeito" antes da violação aos dados armazenados no aparelho telefônico. A suspeita surge justamente da violação à cláusula pétrea (seja ela a do art. 5º, inciso X; seja a do inciso XII). Portanto, não se trata *in casu* de uma devassa *no contexto de uma detenção (prisão-captura)*, muito pelo contrário. Mas, ainda que se tratasse disso, a autorização legal para a busca e apreensão do aparelho (CPP, art. 244) não faz prescindível a ordem judicial para acessar os dados armazenados nele contidos.

27. Afetado o julgamento pela Repercussão Geral, impende prospectar os impactos que de uma eventual decisão afastando a reserva de jurisdição para acesso/devassa ao conteúdo armazenado em *smartphones* no Brasil.

28. Para que se depreenda da sensível discussão no que toca aos impactos dessa autorização jurisprudencial para a devasse de *smartphones*, é válido mencionar trecho do voto do Min. GILMAR MENDES quando do início do julgamento do RE nº 635.659/SP – RG, também afetado por Repercussão geral e no qual se debate a constitucionalidade do art. 28 da Lei de Drogas. *In verbis*:

> "...por volta de **80% das condenações decorreram de prisões em flagrante**, na maioria das vezes realizadas pela polícia em abordagem de **suspeitos na rua (82% dos casos)**, geralmente **sozinhos (cerca de 60%)** e com **pequena quantidade de droga (inferiores a 100g)**.
>
> Outro dado interessante é que, em apenas 1,8% dos casos da amostra, houve menção ao envolvimento do acusado com organizações criminosas.
>
> A pesquisa constatou, também, uma **considerável presença de jovens e adolescentes nas ocorrências**. A maioria dos apreendidos (75,6%) é composta por jovens na **faixa etária entre 18 e 29 anos**.

> Verificou-se, ainda, que 62,1% das pessoas presas responderam que exerciam alguma atividade remunerada – formal ou informal. Revela a pesquisa, também, que **57% das pessoas não tinham nenhum registro em sua folha de antecedentes**.
>
> O **padrão de abordagem** é quase sempre o mesmo: **atitude suspeita, busca pessoal, pequena quantidade de droga e alguma quantia em dinheiro**. Daí pra frente, o sistema repressivo passa a funcionar de acordo com o que o policial relatar no auto de flagrante, já que a sua palavra será, na maioria das vezes, a única prova contra o acusado. Não se está aqui a afirmar que a palavra de policiais não mereça crédito. **O que se critica é deixar exclusivamente com a autoridade policial**, diante da ausência de critérios objetivos de distinção entre usuário e traficante, a definição de quem será levado ao sistema de Justiça como traficante, dependendo dos elementos que o policial levar em consideração na abordagem de cada suspeito."[12] (grifos nossos)

29. A Pesquisa "***Tráfico e Sentenças Judiciais – uma análise das justificativas na aplicação da lei de drogas na região metropolitana do Rio de Janeiro***" realizada pela Defensoria Pública do Estado do RJ em parceria com a SENAD, **revela achados semelhantes**, a saber: **82,13% dos processos têm início a partir da prisão em flagrante**; em 26,33% dos casos – e esse é o dado que destoa da pesquisa referida no voto acima citado – houve condenação por associação ao tráfico, sendo certo que tais condenações foram, em 40,92% dos casos fundamentadas na presunção de que, dado o local dos fatos (referidos como **"favela", "morro" ou "comunidade"** nas sentenças), seria inviável o comércio de drogas sem estar associado a facções criminosas.; em **quase metade dos casos (49,72%) fora apreendida até 100g de maconha**. Apenas **6,1% dos casos tiveram início a partir de investigações**, de inteligência policial.

[12] Íntegra do voto disponível em: https://www.conjur.com.br/dl/re-posse-drogas-pra-consumo-voto-gilmar.pdf A Pesquisa mencionada pelo Min. GILMAR MENDES é a seguinte: Tráfico e Constituição: um estudo sobre a atuação da justiça criminal do Rio de Janeiro e de Brasília no crime de tráfico de drogas. Revista Jurídica, Brasília, v. 11, n. 94, 1-29, jun/set 2009, publicação quadrimestral da Presidência da República.

30. Em síntese, as duas pesquisas revelam que **uma maioria de jovens primários, desarmados e portando pequena quantidade de drogas constitui o perfil dos *presos em flagrante* por tráfico – o crime que, de acordo com o último INFOPEN mais prende no Brasil**. E são esses os brasileiros e brasileiras sujeitos ao "padrão de abordagem" identificado pelo Ministro GILMAR MENDES: "atitude suspeita, busca pessoal, pequena quantidade de droga e alguma quantia em dinheiro...".

31. **Neste caldo de real funcionamento e operacionalidade prática da polícia, é temerário autorizar a possibilidade de acesso aos dados armazenados em *smartphones* sem ordem judicial expressa específica e balizada.** No contexto de uma abordagem seguida da captura por posse de drogas por tráfico, por exemplo, é certo que se permite a busca pessoal e apreensão de eventual aparelho telefônico localizado com o suspeito (CPP, art. 6º, II e III e art. 244). Mas não se pode autorizar a polícia, de antemão, a acessar o aparelho *sponte propria* como fizera no caso concreto.

32. Esta foi, alías, no ponto (limites ao acesso), o entendimento adotado pelo próprio Ministro GILMAR MENDES ao julgar, mais recentemente (j. 16.02.2018; DJe 19.02.2018), o RE 1.048.340/RN. No caso, o acesso estava autorizado judicialmente, todavia, o MPF postulara acessar "*qualquer outro dado que porventura exista nos referidos aparelhos e que sejam de interesse da investigação*". Acerca do que pertine a este ARE, releva colacionar as palavras do Ministro MENDES:

> "A regra é a inviolabilidade do sigilo. O afastamento, por revelar exceção, não admite potencialização. A interpretação há de ser estrita. Surge inconcebível que o Ministério Público Federal almeje obter do Judiciário uma carta branca para vasculhar todo e qualquer dado do investigado, sem especificar quais e porquê."

33. Ora, o MPF postulou devidamente o acesso e o Judiciário o negou. Como se daria esse controle no acesso, "a quente" (no calor dos acontecimentos), realizado

pela autoridade policial sem que, sequer a autoridade judicial tome conhecimento do que se passa? Impossível. **A ausência de limites é justamente a potencialização da violação, pela polícia.**

34. O caso concreto analisado no julgamento do **HC 99.735/SC** dá a exata dimensão da potencialização desse arbítrio a partir da falta de limites temporais e fáticos (fatos investigados) proporcionada pela inovação tecnológica. Isto se dera num caso em que houve autorização judicial (!), ulteriormente reformada pela Sexta Turma do STJ à unanimidade. Daí porque é necessário rigoroso controle judicial do acesso a tais dados. Veja-se a ementa (grifamos):

> RECURSO ORDINÁRIO EM *HABEAS CORPUS*. PENAL E PROCESSO PENAL. TRÁFICO DE DROGAS E ASSOCIAÇÃO AO TRÁFICO. **AUTORIZAÇÃO JUDICIAL DE ESPELHAMENTO, VIA *WHATSAPP WEB*, DAS CONVERSAS REALIZADAS PELO INVESTIGADO COM TERCEIROS. ANALOGIA COM O INSTITUTO DA INTERCEPTAÇÃO TELEFÔNICA. IMPOSSIBILIDADE.** PRESENÇA DE **DISPARIDADES RELEVANTES.** ILEGALIDADE DA MEDIDA. **RECONHECIMENTO DA NULIDADE DA DECISÃO JUDICIAL E DOS ATOS E PROVAS DEPENDENTES. PRESENÇA DE OUTRAS ILEGALIDADES.** LIMITAÇÃO AO DIREITO DE PRIVACIDADE DETERMINADA SEM INDÍCIOS RAZOÁVEIS DE AUTORIA E MATERIALIDADE. DETERMINAÇÃO ANTERIOR DE ARQUIVAMENTO DO INQUÉRITO POLICIAL. FIXAÇÃO DIRETA DE PRAZO DE 60 (SESSENTA) DIAS, COM PRORROGAÇÃO POR IGUAL PERÍODO. **CONSTRANGIMENTO ILEGAL EVIDENCIADO.** RECURSO PROVIDO.
>
> 1. Hipótese em que, após coleta de dados do aplicativo *WhatsApp*, realizada pela Autoridade Policial mediante apreensão judicialmente autorizada de celular e subsequente espelhamento das mensagens recebidas e enviadas, os Recorrentes tiveram decretadas contra si prisão preventiva, em razão da suposta prática dos crimes previstos nos arts. 33 e 35 da Lei n.º 11.343/2006.

2. O espelhamento das mensagens do *WhatsApp* ocorre em sítio eletrônico disponibilizado pela própria empresa, denominado *WhatsApp Web*. Na referida plataforma, é gerado um tipo específico de código de barras, conhecido como Código QR (*Quick Response*), o qual só pode ser lido pelo celular do usuário que pretende usufruir do serviço. Daí a necessidade de apreensão, ainda que por breve período de tempo, do aparelho telefônico que se pretende monitorar.

3. **Para além de permitir o acesso ilimitado a todas as conversas passadas, presentes e futuras**, a ferramenta *WhatsApp Web* foi desenvolvida com o objetivo de possibilitar ao usuário a realização de todos os atos de comunicação a que teria acesso no próprio celular. O emparelhamento entre celular e computador autoriza o usuário, se por algum motivo assim desejar, a conversar dentro do aplicativo do celular e, simultaneamente, no navegador da *internet*, ocasião em que as conversas são automaticamente atualizadas na plataforma que não esteja sendo utilizada.

4. Tanto no aplicativo, quanto no navegador, **é possível, com total liberdade, o envio de novas mensagens e a exclusão de mensagens antigas (registradas antes do emparelhamento) ou recentes (registradas após), tenham elas sido enviadas pelo usuário, tenham elas sido recebidas de algum contato.** Eventual exclusão de mensagem enviada (na opção "Apagar somente para Mim") ou de mensagem recebida (em qualquer caso) não deixa absolutamente nenhum vestígio, seja no aplicativo, seja no computador emparelhado, e, por conseguinte, não pode jamais ser recuperada para efeitos de prova em processo penal, tendo em vista que a própria empresa disponibilizadora do serviço, em razão da tecnologia de encriptação ponta-a-ponta, não armazena em nenhum servidor o conteúdo das conversas dos usuários.

5. Cumpre assinalar, portanto, que o caso dos autos difere da situação, com legalidade amplamente reconhecida pelo Superior Tribunal de Justiça, em que, a exemplo de conversas mantidas por *e-mail*, ocorre autorização judicial para a obtenção, sem espelhamento, de conversas já

registradas no aplicativo *WhatsApp*, com o propósito de periciar seu conteúdo.

6. **É impossível, tal como sugerido no acórdão impugnado, proceder a uma analogia entre o instituto da interceptação telefônica (art. 1.º, da Lei n.º 9.296/1996) e a medida que foi tomada no presente caso.**

7. Primeiro: ao contrário da interceptação telefônica, no âmbito da qual o investigador de polícia atua como mero observador de conversas empreendidas por terceiros, **no espelhamento via *WhatsApp Web* o investigador de polícia tem a concreta possibilidade de atuar como participante tanto das conversas que vêm a ser realizadas quanto das conversas que já estão registradas no aparelho celular, haja vista ter o poder, conferido pela própria plataforma *online*, de interagir nos diálogos mediante envio de novas mensagens a qualquer contato presente no celular e exclusão, com total liberdade, e sem deixar vestígios, de qualquer mensagem passada, presente ou, se for o caso, futura**.

8. **O fato de eventual exclusão de mensagens enviadas (na modalidade "Apagar para mim") ou recebidas (em qualquer caso) não deixar absolutamente nenhum vestígio** nem para o usuário nem para o destinatário, e o fato de tais mensagens excluídas, em razão da criptografia *end-to-end*, não ficarem armazenadas em nenhum servidor, **constituem fundamentos suficientes para a conclusão de que a admissão de tal meio de obtenção de prova implicaria indevida presunção absoluta da legitimidade dos atos dos investigadores**, dado que exigir contraposição idônea por parte do investigado seria equivalente a demandar-lhe produção de prova diabólica.

9. Segundo: ao contrário da interceptação telefônica, que tem como objeto a escuta de conversas realizadas apenas depois da autorização judicial (*ex nunc*), **o espelhamento via Código QR viabiliza ao investigador de polícia acesso amplo e irrestrito a toda e qualquer comunicação realizada antes da mencionada autorização, operando efeitos retroativos (*ex tunc*)**.

10. Terceiro: ao contrário da interceptação telefônica, que é operacionalizada sem a necessidade simultânea de busca pessoal ou

> domiciliar para apreensão de aparelho telefônico, **o espelhamento via Código QR depende da abordagem do indíviduo ou do vasculhamento de sua residência, com apreensão de seu aparelho telefônico por breve período de tempo e posterior devolução desacompanhada de qualquer menção, por parte da Autoridade Policial, à realização da medida constritiva, ou mesmo, porventura** – embora não haja nos autos notícia de que isso tenha ocorrido no caso concreto –, **acompanhada de afirmação falsa de que nada foi feito**.
>
> 11. Hipótese concreta dos autos que revela, ainda, outras três ilegalidades: (a) sem que se apontasse nenhum fato novo na decisão, a medida foi autorizada quatro meses após ter sido determinado o arquivamento dos autos; (b) ausência de indícios razoáveis da autoria ou participação em infração penal a respaldar a limitação do direito de privacidade; e (c) ilegalidade na fixação direta do prazo de 60 (sessenta) dias, com prorrogação por igual período.
>
> 12. Recurso provido, a fim de **declarar a nulidade da decisão judicial que autorizou o espelhamento do *WhatsApp* via Código QR, bem como das provas e dos atos que dela diretamente dependam ou sejam consequência**, ressalvadas eventuais fontes independentes, revogando, por conseguinte, a prisão preventiva dos Recorrentes, se por outro motivo não estiverem presos. (RHC 99.735/SC, Sexta Turma, Rel. Min. Laurita Vaz, unânime, julg. em 12.12.2018)

35. Os fundamentos lançados na decisão são relevantes para o julgamento deste ARE na medida em deixam ver as amplas possibilidades de arbítrio, mesmo quando o acesso é autorizado judicialmente. Admitindo-se a devassa, tudo poderia ter sido feito clandestinamente pela autoridade policial ou seus agentes "com apreensão de seu aparelho telefônico por breve período de tempo e posterior devolução desacompanhada de qualquer menção, por parte da Autoridade Policial, à realização da medida constritiva, ou mesmo, [...], acompanhada de afirmação falsa de que nada foi feito." O STF não dará um passo nesse sentido.

36. Como critério jurisprudencial de razoabilidade – ante o **feixe internacional**, **constitucional** de **direitos e garantias fundamentais**, bem como considerada a **legislação aplicável** (Lei 12.965/14, art. 7º, III) à salvaguarda da inviolabilidade e sigilo do fluxo de comunicações e de comunicações privada armazenadas (ou simplesmente, dados armazenados) – **é inadmissível que se autorize à polícia o acesso direto aos dados armanezados num *smartphone*.** Isto acabaria por **vulnerar e rebaixar o direito à privacidade e ao sigilo de comunicações entre os usuários desses modernos aparelhos sem os quais já não se pode estar completamente integrado à sociedade contemporânea.**

37. **As garantias em jogo neste julgamento, *ad argumentandum,* assumem particular relevância ante ao objetivo fundamental da República insculpido no art. 3º, III da Constituição**. Referimo-nos ao **mandamento constitucional relacionado à redução das formas e modos de marginalização**. Com efeito, aqueles identificados como **alvo preferencial da malha criminal (a juventude negra, pobre, desescolarizada e periférica** – potenciais assistidos da Defensoria Pública) **restariam ainda mais vulneráveis à violência de Estado, caso venham a ser hipertrofiadas as possibilidades de acesso aos dados armazenados em seus smartphones,** o que colaboraria para aprofundar a seletividade e o arbítrio intrínsecos à realidade do policiamento ostensivo no Brasil. Um exemplo dessa situação citamos no item 14 supra.

38. **Some-se a isso, o fato de que a autorização da devassa desse tipo não teria qualquer limite quanto aos aplicativos passíveis de acesso, tampouco limites temporais relacionados às conversações armazenadas.** Essa realidade torna imperiosa a salvaguarda da "reserva de jurisdição" quando ao acesso aos dados. Somente a partir do ***rigoroso controle jurisdicional prévio*** seria possível, por exemplo, obervar-se os princípios elencados pela *United Nations Global Pulse* sobre

ética e proteção de dados[13], assim sintetizados: (i) uso legal, legítimo e justificável; (ii) finalidade específica, limitada e compatível; (iii) mitigação de riscos e danos; (iv) uso responsável de dados sensíveis; (v) segurança; (vi) retenção e minimização dos dados; (vii) qualidade dos dados; (viii) transparência e prestação de contas; (ix) colaboração de terceiros.

39. No mesmo diapasão, a novel Lei nº 13.709/18 (Marco Civil da Internet), com início de vigência previsto para o mês de agosto de 2020, embora não se aplique ao tratamento de dados pessoais realizados para fins exclusivos de atividades de investigação e repressão penais (art. 4º), disciplina a sua proteção a partir dos seguintes fundamentos (art. 2º): respeito à privacidade, liberdade de expressão, inviolabidade da intimidade, da honra e da imagem, dentre outros. E não só: o tratamento de dados deve respeitar a boa-fé e princípios de necessidade ("limitação ao mínimo necessário para a realização das finalidades"), transparência, segurança, prevenção ("prevenir a ocorrência de danos"), não discriminação ("impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos"), responsabilização e prestação de contas.

40. Com isso, **o tema assume relevância ainda maior**. Na medida em que a salvaguarda constitucional precisa ser preservada pelo seu maior guardião (CP, art. 102), **espera-se que Supremo Tribunal Federal não autorize o acesso pela autoridade policial (ou seus agentes) sob nenhuma hipótese**, *salvo em excepcionalíssimas situações reservadas à análise de casos concretos*, com a necessária confecção de termo pormenorizado, a fim de dar transparência a todos os acessos realizados, requisitos sem os quais o controle das partes sobre as diligências investigatórias restaria absolutamente impossível. É o que se pode extrair das decisões internacionais (EUA, Canada e Espanha) aqui colacionadas.

[13] NAÇÕES UNIDAS. Data Privacy, Ethics and Protection: Guidance note on big data for the 2030 agenda. Genebra: Nações Unidas, 2017. Disponível em: <https://undg.org/wp-content/uploads/2017/11/UNDG_BigData_final_web.pdf>. Acesso em: 28 jan. 2019.

41. Diversos outros aspectos relacionados ao tema são abordados e aprofundados no **parecer anexado, elaborado pelo IDDD, pelo Article 19 e pelo IDDH**, destacando-se o enfrentamento do tema sob a perspectiva do direito à intimidade, à inviolabilidade das comunicações e da proteção de dados a partir: **(i)** do que dispõem **Tratados Internacionais**, como a Declaração Universal dos Direitos Humanos, o Pacto Internacional sobre Direitos Civis e Políticos, a Carta Africana dos Direitos Humanos e dos Direitos dos povos, a Declaração Americana dos Direitos e Deveres do Homem, a Convenção Americana de Direitos Humanos e a Convenção Europeia sobre Direitos Humanos, dentre outros documentos internacionais; **(ii)** da **Constituição da República** e da **legislação brasileira**; **(iii)** do cenário de **violações e abusos por parte de autoridades policiais** no Brasil; **(iv)** de comentários ao caso *Riley v. California*, dentre outros relevantíssimos aportes para o justo e adequado enfrentamento do tema. Por estes motivos, pedimos vênia para anexá-lo à presente manifestação em memoriais.

40. Pelo exposto, e pelo mais que certamente virá à tona em razão dos abalizados votos a serem proferidos pelos Ministros deste Supremo Tribunal Federal, **pugna e espera a Defensoria Pública do Estado do Rio de Janeiro que o Agravo venha a ser improvido** com a manutenção da absolvição do agravado, reconhecendo-se a ilicitude da prova tal como obtida nestes autos.

Termos em que pede deferimento. Brasília, 2 de maio de 2018.

Pedro Paulo Lourival Carriello
Defensor Público 820.959-5
Representação nos Tribunais Superiores

Emanuel Queiroz Rangel
Defensor Público 852.722-8
Coordenação de Defesa Criminal

Ricardo André de Souza
Defensor Público 877.375-6
Subcoordenador de Defesa Criminal

Daniel Lozoya C. Lopes
Defensor Público 949.550-8
NUDEDH

PEDRO PAULO LOURIVAL CARRIELLO:8209595

Assinado de forma digital por PEDRO PAULO LOURIVAL CARRIELLO:8209595
DN: c=BR, o=ICP-Brasil, ou=Autoridade Certificadora da Justica - AC-JUS, ou=Cert-JUS Poder Publico - A3, ou=Defensoria_Publica_do_Estado_do_Rio_de_Janeiro-DPRJ, ou=DEFENSOR PUBLICO, cn=PEDRO PAULO LOURIVAL CARRIELLO:8209595
Dados: 2019.05.02 18:24:58 -03'00'