O CELULAR DE UM HOMEM E O SEU CASTELO: PRIVACIDADE E SMARTPHONES NA INVESTIGAÇÃO CRIMINAL

THE CELLPHONE OF A MAN IS HIS CASTLE: PRIVACY AND SMARTPHONES IN THE CRIMINAL INVESTIGATION

Luís Renato Vedovato
Leandro Zedes

RESUMO

O artigo aborda a evolução do tratamento jurídico do acesso a dados armazenados em smartphones apreendidos com pessoas presas, à luz da Constituição brasileira, bem como das leis 9296/96 e 12965/14. Utilizando o método jurisprudencial comparativo, analisa a jurisprudência, tomando por paradigma o caso Riley vs. California, da Suprema Corte dos Estados Unidos, e o HC 91867/PA, do Supremo Tribunal Federal do Brasil. Busca responder se é necessário mandado judicial para acesso aos dados armazenados em celulares apreendidos, concluindo de modo afirmativo.

Palavras-chave: Direito Constitucional. Sigilo de dados. Smartphones.

ABSTRACT

The article discusses the evolution of the juridical treatment of the access to data stored in smartphones seized with arrested people, in light of the brazilian Constitution, as well of the 9296/96 and 12965/14 federal laws. Using the jurisprudential comparative method, analyses the decisions, after the SCOTUS case Riley vs. California, and the HC 91867/PA, of the Federal Supreme Court of Brazil. Aims to answer if is necessary warrant to the access to stored data in seized cell phones, concluding affirmatively.

Keywords: Constitutional law. Data secrecy. Smartphones.

INTRODUÇÃO

A Constituição da República Federativa do Brasil assegura como direitos invioláveis do indivíduo, em seu artigo 5º, inciso X, "a intimidade, a vida privada, a honra e a imagem das pessoas"; em outro inciso do mesmo artigo (XII), determina ser "inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

Esse conjunto normativo incide decisivamente sobre as investigações criminais, já que a comunicação é elemento central de qualquer empreitada criminosa de vulto. Preenchidos certos requisitos legais, é lícito aos investigadores recorrer à interceptação telefônica, que nada mais é do que um meio de obter informação em fluxo (comunicação em andamento), visando preservá-la, para elucidar a prática de crimes.

Todavia, dados[1] não são de interesse apenas para a investigação criminal. Na verdade, a questão do acesso, interpretação e tratamento de dados é hoje central para nossa economia e sociedade. Nesta linha, Manuel Castells classifica como *informacional* a atual economia, "porque a produtividade e a competitividade de unidades ou agentes nessa economia (sejam empresas, regiões ou nações) dependem basicamente de sua capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos"[2].

Cada vez menos provas de um crime são físicas. Em um mundo dia a dia mais virtual, as facilidades de comunicação proporcionadas pela disseminação da internet e dos celulares conhecidos como *smartphones*[3] criam a necessidade de adaptação dos paradigmas investigativos. Entretanto, não se pode descurar dos direitos fundamentais dos investigados. O presente artigo procura contribuir com a análise do conflito entre necessidades da investigação e direito de privacidade / sigilo das comunicações. Em especial, busca analisar a evolução do entendimento jurisprudencial a respeito, a partir de julgados considerados representativos. A questão central é a necessidade ou não de mandado judicial para acesso aos dados armazenados nos celulares

apreendidos, com olhos nas mudanças tecnológicas e sociais e seus efeitos na própria percepção de privacidade nos últimos anos, e se tal quadro está sendo absorvida pelas cortes do Brasil e dos EUA. A resposta é essencial para uma persecução penal efetiva e que observe os direitos individuais dos investigados.

Uma das premissas deste artigo é o proveito no uso do direito comparado como forma de abordagem do fenômeno jurídico. A interação das pessoas, dos bens e sistemas jurídicos na sociedade global vem continuamente desafiando as fronteiras. Isso torna importante conhecer as leis e decisões judiciais de outros países, como forma de enriquecer o debate. Como ensina Barroso[4], "A globalização do direito é uma característica essencial do mundo moderno, que promove, no seu atual estágio, a confluência entre Direito Constitucional, Direito Internacional e Direitos Humanos".

O ANTES E O DEPOIS DA LEI 9296/96.

O texto clássico sobre intimidade no cenário norte-americano, *The Right to Privacy*[5], expressava preocupação com o surgimento de tecnologias como fotografias instantâneas, origem de agravos cada vez maiores ao direito de ficar sozinho[6] e a consequente necessidade de evolução de tal prerrogativa individual. Como em 1890, nossos tempos vêm exigindo ajustes nos limites e na compreensão da privacidade, sob pena de cercear o desenvolvimento da personalidade de cada um e ofender a dignidade humana, transformando a todos nós em objeto da curiosidade alheia.

Em trabalho científico de 1993[7], referenciado ainda nos dias atuais, Tércio Sampaio Ferraz Junior considera ser a privacidade "o direito de o indivíduo excluir do conhecimento de terceiros aquilo que só a ele é pertinente e que diz respeito ao seu modo de ser exclusivo no âmbito de sua vida privada". A tese central de Ferraz Junior é a de que, no inciso XII[8] do artigo 5º, a Constituição pretendeu proteger a comunicação de dados, e não os dados em si:

> 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 telefonia. 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[9]. (*Grifos* do original)

Ao longo da década de 1990, vale lembrar que o Supremo Tribunal Federal (STF) sequer admitia a interceptação telefônica, mesmo que com ordem judicial:

> O art. 5º, XII, da Constituição, que prevê, excepcionalmente, a violação do sigilo das comunicações telefônicas para fins de investigação criminal ou instrução processual penal, não é autoaplicável: exige lei que estabeleça as hipóteses e a forma que permitam a autorização judicial. Precedentes. Enquanto a referida lei não for editada pelo Congresso Nacional, é considerada prova ilícita a obtida mediante quebra do sigilo das comunicações telefônicas, mesmo quando haja ordem judicial (CF, art. 5º, LVI). O art. 57, II, a, do Código Brasileiro de Telecomunicações não foi recepcionado pela atual Constituição[10], a qual exige *numerus clausus* para a definição das hipóteses e formas pelas quais é legítima a violação do sigilo das comunicações telefônicas. A garantia que a Constituição dá, até que a lei o defina, não distingue o telefone público do particular, ainda que instalado em interior de presídio, pois o bem jurídico protegido é a privacidade das pessoas, prerrogativa dogmática de todos os cidadãos. (HC 72.588, rel. min. Maurício Corrêa, j. 12-6-1996, P, DJ de 4-8-2000)[11]

Assim, em um momento inicial, sequer se falava em uso lícito da interceptação telefônica ou telemática no direito brasileiro, o que se reflete inclusive na nomenclatura utilizada no voto do relator no HC 72.588: "grampo" ou "grampeamento". Mas já se podia entrever a decisiva influência da visão de Ferraz Junior nos debates do MS 21729[12], especificamente no voto do Ministro Sepúlveda Pertence:

> "Da minha leitura, no inciso XII da Lei Fundamental, o que se protege, e de modo absoluto, até em relação ao Poder Judiciário, é a comunicação "de dados", e não os "dados", o que tornaria impossível qualquer investigação administrativa, fosse qual fosse".

Após a edição da Lei 9292/96, o STF passou a admitir a interceptação, enfrentando mais diretamente o inciso XII e conformando sua aplicação. E neste labor, continuou a adotar a interpretação de Ferraz Junior:

> Primeiramente, sobreleva destacar que não se confundem comunicação telefônica e os registros telefônicos, recebendo, inclusive, proteção jurídica distinta. E, como já enfatizei em outras oportunidades, entendo que não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação 'de dados' e não os 'dados'. O tema foi objeto de percuciente análise em estudo singular desenvolvido por Tércio Sampaio Ferraz[13].

É válido observar que também a Lei 9296/96 adotou a distinção em análise: o parágrafo único do seu artigo 1º estende a disciplina legal "à interceptação *do fluxo de comunicações* em sistemas de informática e telemática". Mesmo na doutrina o ponto repercutiu, como se vê no excerto do comentário de Lênio Luiz Streck ao inciso XII do artigo 5º:

> Não se pode, todavia, confundir dados estáticos – que, aliás, sequer estão protegidos pelo dispositivo constitucional sob comento (veja-se que a Constituição alude à "comunicação de dados") – com dados em tráfego (excepcionalmente violáveis): há que se distinguir "bancos de dados" do seu "conteúdo", qual seja, os dados em si – cujo conteúdo se relaciona a crimes – transmitidos, via informática, de um banco ou uma empresa para outra (empresa ou pessoa)[14].

O que se pretende vincar é o seguinte: no contexto dos anos 1990 e até há pouco tempo, o inciso X[15] do art. 5º (intimidade e vida privada) não estava em posição central na discussão. A ênfase hermenêutica se dava nos limites e possibilidades do art. 5º, inciso XII. A despeito da previsão da interceptação telefônica como técnica de investigação, a telefonia no Brasil engatinhava em um mercado estatizado e precário. Os primeiros

celulares começaram a ser vendidos no país na década de 1990, mas a tecnologia era cara, falha e limitada.

A interceptação era extensivamente utilizada, com permissão de *acesso à base física onde armazenados os dados sem maiores questionamentos*, pela adoção da distinção entre comunicação de dados e dados estáticos. A questão não era analisada sob o prisma da violação da intimidade: os celulares armazenavam, quando muito, algumas fotos, a agenda de contatos e registros de ligações efetuadas e recebidas. Não havia maior interesse naqueles aparelhos.

Quando efetuada uma prisão e apreendido um celular, considerava-se normal e lícito o acesso a seu conteúdo. É oportuno lembrar que o longevo Código de Processo Penal brasileiro prevê, em seu artigo 244[16], a possibilidade da busca incidente à prisão, silenciando acerca da análise posterior dos elementos apreendidos.

Tudo refletia uma realidade em que sequer existiam aparelhos pessoais multifuncionais. Não é mais este o ambiente em que se movem os operadores.

O NOVO CENÁRIO: A LEI 12965/2014.

Em 1998, o governo federal começa a privatizar o setor de telefonia, havendo expansão da oferta do serviço. Com a evolução tecnológica, hoje, um celular, aparelho portátil e de uso altamente disseminado[17], possui capacidade de processamento e armazenamento muitas vezes superior a computadores de mesa de 1990. Para se ter uma ideia, um smartphone contemporâneo é um computador muitas vezes superior ao que equipava a nave Apolo 11, com a qual o homem chegou à Lua[18].

Da mesma forma, os últimos anos testemunharam alterações comportamentais profundas em nossa sociedade. Todos estamos sempre conectados; as chamadas redes sociais tornaram-se praticamente onipresentes e lograram alcançar certo desapego de seus clientes no que diz com a privacidade[19]. É raro quem não tenha seu smartphone (por vezes mais de um), e simplesmente neste ato de portar estes aparelhos várias informações se tornam disponíveis:

> (...) embora o Facebook saiba muito a seu respeito, ele se parece mais com um 'colega de trabalho': por mais que vocês passem muito tempo juntos, há limites claros nesse relacionamento. O Facebook só sabe o que você faz no Facebook. Há muitos lugares com alcance muito maior. Se você tem um iPhone, a Apple pode ter seus contatos, agenda, fotos, mensagens, todas as músicas que escuta, os lugares aonde vai e até quantos passos levou para chegar lá, haja vista que celulares têm um pequeno giroscópio. Não tem um iPhone? Então troque 'Apple' por Google, Samsung ou Verizon[20].

Mariana Giorgetti Valente, ao abordar a importância dos smartphones para a investigação criminal em operações de grande porte, aduz:

> Nessas operações, as 'informações digitais' assumiram um papel central. Afinal, a vida conectada deixa muitos rastros: você já parou para pensar em quantas informações estão armazenadas só nos telefones celulares? São agendas de contatos, arquivos de textos, fotografias tiradas diariamente, anotações, caixas de e-mails, históricos de mensagens instantâneas, históricos de navegação na Internet, informações de GPS sobre cada lugar que visitamos e que caminho fizemos. Resumindo: nossos smartphones se tornaram verdadeiros "baús do tesouro" para investigadores[21].

Tais aspectos culturais e comportamentais se somaram à tendência das empresas de tecnologia, após o episódio Edward Snowden[22], de incrementar o uso de criptografia[23] em seus produtos. No limite, isso inviabiliza (ou dificulta severamente) a interceptação de dados, tornando necessário a obtenção física do aparelho celular para ter acesso[24].

O quadro levou à edição do Marco Civil da Internet (Lei 12965/2014), que estipulou um conjunto normativo que exige cautelas especiais dos atores da persecução penal quando do manejo de um smartphone:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
>
> II - proteção da privacidade;
>
> III - *proteção dos dados pessoais*, na forma da lei;
>
> (...)
>
> Art. 5º Para os efeitos desta Lei, considera-se:
>
> (...)

> II - terminal: o computador *ou qualquer dispositivo que se conecte à internet;*
>
> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - *inviolabilidade da intimidade e da vida privada,* sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II - *inviolabilidade e sigilo do fluxo de suas comunicações* pela internet, salvo por ordem judicial, na forma da lei;
>
> III - *inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;* (Original sem *grifo*)

Percebe-se da leitura dos dispositivos selecionados que o Marco Civil[25] distinguiu expressamente dados e comunicação de dados (neste último caso chegando a falar em fluxo de comunicações e comunicações armazenadas), a todos atribuindo sigilo. Ou seja, impôs sigilo (também) aos dados estáticos[26], uma novidade em relação ao já analisado quadro anterior. Desrespeitar o sigilo gera a nulidade da prova obtida e sua necessária exclusão dos autos (exclusionary rule), conforme exposto por Rosa e Heil (2015).

Com estes subsídios, será apresentada a questão do acesso a dados armazenados em smartphones através da comparação entre a decisão adotada pela Suprema Corte dos Estados Unidos (doravante SCOTUS) em Riley vs. California (573 U.S.) e a adotada no Habeas Corpus 91867/PA[27] pelo STF, além de precedentes oriundos do Superior Tribunal de Justiça (STJ).

O PRECEDENTE RILEY VS. CALIFORNIA, DA SCOTUS.

Em Riley vs California, a SCOTUS traz inicialmente um quadro fático[28] bastante preciso. David Leon Riley foi parado pela polícia para uma averiguação por violação de leis de trânsito (estava dirigindo veículo com registro vencido). Durante a revista pessoal (Riley estava com a habilitação também vencida) e no veículo, os policiais encontraram duas armas ocultas e carregadas, o que levou à prisão de Riley. Um celular tipo smartphone[29] foi apreendido no bolso do detido, e acessado no local por um dos policiais que o abordou, que

verificou o uso de termos ligados a uma gangue de rua local (Bloods). Após a prisão (cerca de duas horas depois), e já na delegacia de polícia, o celular foi entregue a um detetive especializado em gangues, que analisou fotos e vídeos armazenados no celular, e que ligavam Riley a um tiroteio ocorrido poucas semanas antes, o que acabou levando à sua condenação. Riley impugnou a validade das provas obtidas em seu celular, argumento rechaçado nas instâncias ordinárias, com base no precedente Chimel vs. California (395 U.S. 752), de 1969.

A *Chimel Rule*, como é conhecida, estipula que os policiais que estejam prendendo alguém em sua casa não podem revistar todo o local sem um mandado judicial; mas podem revistar a área imediatamente ao alcance do detido, para garantir a segurança dos policiais e se prevenir contra o risco de fuga do preso ou destruição de provas. Assim, e até o caso Riley, um celular, caso estivesse ao alcance[30] do detido no momento da prisão, poderia ser objeto de buscas e análise policial.

Em Riley, a SCOTUS negou a aplicação da *Chimel Rule* à hipótese. Firmou-se a orientação de que a polícia, em princípio, não pode empreender buscas em informações digitais armazenadas em celulares apreendidos de um indivíduo detido antes de obter mandado judicial para acesso ao conteúdo do telefone. Proceder de maneira diversa viola o texto da Quarta Emenda à Constituição dos Estados Unidos:

> O direito dos cidadãos de estarem seguros em suas pessoas, casas, documentos e bens, contra buscas e apreensões desarrazoadas, não será violado, e não serão concedidos mandados, senão com base em causa provável, com base em juramento ou afirmação, e descrevendo particularmente o lugar a ser objeto de buscas, e as pessoas ou coisas a serem apreendidas[31].

No sistema norte-americano, uma busca sem mandado somente é válida se o caso se enquadrar em uma exceção específica à exigência de mandado constante da Quarta Emenda à Constituição (citou-se como exemplo o caso Kentucky v. King, 563 U.S.[32]), ou se for restrita à área sob influência imediata do detido, onde está justificada pelo interesse na segurança dos policiais e para prevenção de destruição de provas (exatamente o caso Chimel vs. California, 395 U.S. 752, já mencionado).

A SCOTUS não considerou, em Riley vs. California, que a situação autorizasse uma busca sem mandado. Avaliou-se que dados digitais armazenados em celulares não podem ser usados como arma contra um policial ou para a fuga do detido, em regra. Sob outra ótica, e diante do argumento de que celulares, mesmo quando fisicamente seguros, estão vulneráveis ao apagamento remoto de seus dados ou encriptação, a SCOTUS decidiu que não ficou claro como o acesso aos dados no momento da prisão evitaria tais riscos, bem como que as forças policiais possuem meios de evitar a perda de provas (como desligar o celular, o que previne apagamento remoto, ou usar envelopes de Faraday[33]).

Durante a fundamentação, entendeu-se que inspecionar os bolsos de um detido lhe causa uma intrusão leve na privacidade[34], mas este raciocínio só é válido para itens físicos. A privacidade é atingida mais significativamente quando dados digitais estão envolvidos, pelas diferenças substanciais quantitativas e qualitativas de celulares modernos, com grande capacidade de armazenamento. A análise conjunta do conteúdo de um celular (fotos, vídeos, textos) revela muito mais do que um registro isolado, até pelo alcance temporal das informações armazenadas, que pode atingir muitos anos. Isso gera uma expectativa de privacidade que a SCOTUS entendeu por bem tutelar. Como elemento adicional, aduziu-se que anos atrás era ocasional um policial apreender um item fortemente pessoal como um diário, mas hoje mais do que 90% dos americanos adultos que possuem celulares mantém neles um registro digital de praticamente todo aspecto de suas vidas.

A SCOTUS reconheceu que o precedente teria algum impacto na habilidade das forças de manutenção da lei de combater o crime. Declarando que "a privacidade vem com um preço", a Corte firmou que não estava dizendo que as informações do celular são imunes a buscas; apenas que um mandado judicial é geralmente necessário antes de fazê-lo, em respeito à Quarta Emenda e devido ao fato de que mandados judiciais podem ser obtidos rapidamente. Ademais, buscas sem mandado continuam sendo possíveis se impostas pelas circunstâncias[35]. As provas foram consideradas ilícitas e excluídas dos autos (*exclusionary rule*), anulando a condenação de Riley.

O caso Riley deixou algumas lacunas: como aponta Danielsen[36], a SCOTUS não ofereceu qualquer orientação sobre o que caracterizaria causa provável para obtenção de mandado para análise de um smartphone, ou as exigências para preenchimento de um requerimento de mandado, como por exemplo uma discriminação mais específica do quê se pretende encontrar nos arquivos armazenados. Mandados que permitam acesso a "todo e qualquer" arquivo que constitua prova de crime parecem incidir em violação à Quarta Emenda, que veda mandados genéricos. Entretanto, a quantidade de dados e programas que um celular geralmente contém oferecem evidentes dificuldades para indicações mais precisas por parte das agências de manutenção da lei.

Segundo Whitebread e Slobogin (2015, p. 163-165), Riley vs. California funciona, assim, como uma exceção à regra da busca incidental quando da prisão de alguém, que pode ser realizada na pessoa presa e naquilo que estiver ao seu alcance (Armspan rule).

O HABEAS CORPUS 91867/PA NO SUPREMO TRIBUNAL FEDERAL

A questão do acesso a dados contidos em celulares ainda não foi analisada pelo STF após a edição do Marco Civil da Internet e o julgamento da SCOTUS. O precedente disponível e escolhido para confronto data de 2004: o Habeas Corpus 91867/PA[37], um caso de homicídio triplamente qualificado e formação de quadrilha. Em novembro de 2004, no começo da noite e em plena praça pública, um pistoleiro de aluguel (Francisco Leite da Silva) efetuou vários disparos de arma de fogo na cabeça da vítima. O crime foi encomendado por membros de uma família poderosa e temida no local (Ulianópolis/PA). Francisco foi preso em flagrante, e dois policiais, no momento da prisão, checaram os registros das últimas chamadas efetuadas e recebidas nos dois celulares apreendidos (não há detalhes sobre a natureza dos aparelhos), que incluíam números de celulares que depois se descobriu pertencerem aos mandantes, um dos quais impugnou a obtenção dos dados, alegando violação ao sigilo das conversas telefônicas.

O acórdão faz expressa referência, novamente, aos ensinamentos de Ferraz Junior:

> Primeiramente, sobreleva destacar que não se confundem comunicação telefônica e os registros telefônicos, recebendo, inclusive, proteção jurídica distinta. (...) não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação 'de dados' e não os 'dados'[38].

O julgado não põe ênfase na questão constitucional envolvida. A partir da vedação de admissão da prova ilícita (artigo 5º, LVI), cita uma série de outras normas constitucionais regradoras do processo[39], inclusive e incidentemente o artigo 5º, inciso X. Mas os argumentos utilizados pelo relator foram predominantemente de natureza infraconstitucional processual penal, com referências à natureza inquisitorial do inquérito policial, ao dever da autoridade policial de recolher provas (Código de Processo Penal – CPP, artigo 6º[40]) e todo material de interesse da investigação.

O tratamento dado ao celular buscou analogias com outros objetos materiais (pedaço de papel, agenda, caderno). Não se identificou potencial violação da privacidade no acesso levado a efeito pela polícia, como se vê do seguinte trecho:

> Saliento que o exame do objeto — aparelho celular — indicou apenas o número de um telefone. Esse dado, número de telefone, por si só, conecta-se com algum valor constitucionalmente protegido? Penso que não. É que o dado, como no caso, mera combinação numérica, de per si nada significa, apenas um número de telefone. (…) Ad argumentandum, abstraindo-se do meio material em que o dado estava registrado (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 em um caderno que estava junto com o réu no momento da prisão? (…) A obviedade que resulta da resposta a essas indagações, denota que, não raras vezes, na construção argumentativa desvia-se o foco da tutela constitucional. A proteção jurídica à intimidade, à vida privada, não me parece que tenha o alcance pretendido pelo impetrante. [41]

Enfatizou-se (inclusive graficamente, pelo uso de negrito[42]) que se cuidava de prisão em flagrante, o que autoriza, constitucionalmente (artigo 5º, inciso XI) até mesmo a entrada em domicílio, indiciando que o acesso a celular não haveria de receber proteção diversa[43].

No final do voto do relator, fez-se ainda referência à mitigação da teoria dos frutos da árvore venenosa, especificamente à descoberta inevitável, já que o fato de terem sido apreendidos telefones celulares fatalmente levaria (na visão do relator) à quebra de seu sigilo e obtenção dos mesmos dados ora impugnados. O julgado foi unânime e não houve registro de votos com outras nuances ou fundamentos[44].

COMPARAÇÃO ENTRE AS DECISÕES DAS CORTES SUPREMAS

O primeiro ponto a ser realçado é que existem diferenças sensíveis entre a forma de julgamento na SCOTUS e no STF. O quadro fático é melhor delineado na corte americana, logo no início do julgado, de forma a demonstrar qual a situação abrangida pelo precedente – uma exigência do sistema da *common law*. Para verificação semelhante no julgado brasileiro, é necessário recorrer a numerosos pontos do acórdão – as referências fáticas são feitas na medida da necessidade do relator durante a argumentação.

A SCOTUS, agindo como verdadeira corte constitucional, privilegiou a análise do tema sob o prisma do direito à intimidade, entendendo necessária a intervenção judicial para o acesso aos dados, em uma perspectiva nitidamente evolutiva da jurisprudência desde a *Chimel Rule*. Já o STF não delimitou nitidamente seu fundamento constitucional, recorrendo mais enfaticamente a dispositivo infraconstitucional para decidir (CPP 6º), afastando a incidência do art. 5º, XII na espécie e pincelando aspectos do tratamento constitucional da prova ilícita.

O tratamento dado pela SCOTUS tende a repercutir entre nós, como se demonstrará a seguir, deslocando o eixo interpretativo do inciso XII do artigo 5º para o inciso X. Com efeito, os requerimentos defensivos (e mesmo os julgados) antes do precedente Riley primavam

por manejar teses em torno de ofensa ao art. 5º, XII, buscando aplicar o regramento da interceptação telefônica, ainda que por analogia, a qualquer acesso aos dados telefônicos, mesmo os estáticos. Esta postura se devia, presumivelmente, à ausência, no marco normativo brasileiro, de regramento a respeito do sigilo de dados estáticos, o que mudou desde o Marco Civil da Internet.

O julgado norte-americano, em um ambiente de difusão cada vez mais rápida de informação e teses jurídicas, argumentou que não se cuida efetivamente de interceptação de comunicação. O advento do Marco Civil da Internet deu azo a discussões sobre suas disposições, com distinção da doutrina a respeito de dados dinâmicos e estáticos, bem como a exigência, agora legal, de autorização judicial para acesso a ambos.

Firmado que os dados armazenados em um celular são dados estáticos, sua tutela constitucional parece centrar-se em outro dispositivo – especificamente no inciso X (tutela da intimidade e vida privada), na linha do decidido em Riley vs. California. E esta forma de pensar se deve, também, pelos desenvolvimentos do tema em território nacional, como se passa a demonstrar.

INFLUENCIA DE RILEY VS. CALIFORNIA EM JULGADOS BRASILEIROS

Luís Roberto Barroso registra o "crescente diálogo constitucional envolvendo citação mútua, conferências de intercâmbio acadêmico e organização de fóruns públicos" entre tribunais constitucionais e cortes supremas de todo o mundo, bem como o papel de modelo que cortes como a Suprema Corte dos Estados Unidos[45] e o Tribunal Constitucional Federal da Alemanha têm desempenhado para várias democracias[46].

Essa influência já pode ser sentida no que diz com a busca e apreensão de aparelhos celulares. O precedente ora analisado da SCOTUS já inspirou[47] ao menos um julgado do Superior Tribunal de Justiça[48] brasileiro, recomendando sua leitura pelos operadores locais.

Em voto-vista no Recurso em Habeas Corpus 51.531-RO[49], o Min. Schietti Cruz afastou a orientação do STF alegando que, quando

do julgamento do HC 91867/PA, os celulares não tinham acesso à internet de banda larga. Com a tecnologia atual, o acesso dos policiais é necessariamente mais intrusivo, já que os celulares dispõem de arquivos gravados que dão acesso a vários aspectos da vida do indivíduo: "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". O Min. Schietti Cruz fez expressa referência ao precedente Riley vs. California, abonando suas conclusões. E afasta a relevância da prisão em flagrante no tratamento da questão, ponto enfatizado, como visto, quando da decisão do HC 91867 no STF. Já o voto do relator cita o Marco Civil da Internet como fundamento, especificamente seu art. 7º, III, indiciando a absorção das alterações do marco legal interno nas decisões.

Orientação no mesmo sentido pode ser extraída do Recurso em Habeas Corpus 67379/RN[50], relator o Ministro Ribeiro Dantas, onde se consignou, com apoio na disciplina do Marco Civil da Internet, que

> Embora seja despicienda ordem judicial para a apreensão dos celulares, pois os réus encontravam-se em situação de flagrância, as mensagens armazenadas no aparelho estão protegidas pelo sigilo telefônico (...). Em verdade, deveria a autoridade policial, após a apreensão do telefone, ter requerido judicialmente a quebra do sigilo dos dados nele armazenados, de modo a proteger tanto o direito individual à intimidade quanto o direito difuso à segurança pública.

Embora possa ser criticada a fundamentação do último precedente, na medida em que o sigilo telefônico não é o fundamento aplicável à espécie[51], temos precedentes de ambas as Turmas da 3ª Seção do STJ, firmados em 2016, assentarando a necessidade de mandado judicial para acesso às informações armazenadas em celulares apreendidos quando de flagrante, mesmo em situações de crime permanente (ambos os precedentes cuidavam de tráfico de drogas).

A solução foi outra em caso em que existia mandado de busca e apreensão, ainda que inespecífico. A situação foi enfrentada, ainda que como *obiter dicta*, em ao menos um precedente do STJ, onde se admitiu a licitude da prova obtida mediante acesso ao conteúdo de mensagens

arquivadas no aparelho celular, desde que apreendido com amparo em mandado judicial:

> PROCESSUAL PENAL. OPERAÇÃO "LAVA-JATO". MANDADO DE BUSCA E APREENSÃO. APREENSÃO DE APARELHOS DE TELEFONE CELULAR. LEI 9296/96. OFENSA AO ART. 5º, XII, DA CONSTITUIÇÃO FEDERAL. INOCORRÊNCIA. DECISÃO FUNDAMENTADA QUE NÃO SE SUBORDINA AOS DITAMES DA LEI 9296/96. ACESSO AO CONTEÚDO DE MENSAGENS ARQUIVADAS NO APARELHO. POSSIBILIDADE. LICITUDE DA PROVA. RECURSO DESPROVIDO. I - A obtenção do conteúdo de conversas e mensagens armazenadas em aparelho de telefone celular ou smartphones não se subordina aos ditames da Lei 9296/96. II - *O acesso ao conteúdo armazenado em telefone celular ou smartphone, quando determinada judicialmente a busca e apreensão destes aparelhos, não ofende o art. 5º, inciso XII, da Constituição da República,* porquanto o sigilo a que se refere o aludido preceito constitucional é em relação à interceptação telefônica ou telemática propriamente dita, ou seja, é da comunicação de dados, e não dos dados em si mesmos. III - Não há nulidade quando a decisão que determina a busca e apreensão está suficientemente fundamentada, como ocorre na espécie. IV - *Na pressuposição da ordem de apreensão de aparelho celular ou smartphone está o acesso aos dados que neles estejam armazenados, sob pena de a busca e apreensão resultar em medida írrita, dado que o aparelho desprovido de conteúdo simplesmente não ostenta virtualidade de ser utilizado como prova criminal.* V - Hipótese em que, demais disso, a decisão judicial expressamente determinou o acesso aos dados armazenados nos aparelhos eventualmente apreendidos, robustecendo o alvitre quanto à licitude da prova. Recurso desprovido. (RHC 75.800/PR, Rel. Ministro FELIX FISCHER, QUINTA TURMA, julgado em 15/09/2016, DJe 26/09/2016)

No corpo do voto condutor (que cita o MS 21729 do STF e a doutrina do Professor Tércio Ferraz), fica claro que, no caso concreto, o magistrado autorizou expressamente o acesso aos dados constantes dos celulares apreendidos[52]. Mas a leitura do precedente guarda interesse para nossa análise, senão vejamos.

O recorrente citou o RHC 51531 em abono de sua tese, mas o Min. Felix Fischer bem distinguiu as situações, posto que no RHC 51531 não havia autorização judicial para acesso. E disse mais: invocando o HC 91867/PA, aduziu, com amparo em doutrina anglo-saxã, que qualquer

iniciativa de *overruling* da orientação do STF sobre a matéria haveria de partir do próprio STF[53]. E lançou o seguinte trecho:

> Na pressuposição do comando de apreensão de aparelho celular ou smartphone está o acesso aos dados que neles estejam armazenados, sob pena de a busca e apreensão resultar em medida írrita, dado que o aparelho desprovido de conteúdo simplesmente não ostenta virtualidade de ser utilizado como prova criminal. Dessarte, se se procedeu à busca e apreensão da base física de aparelhos de telefone celular, como, aliás*, expressamente autorizado na decisão judicial que determinou a busca e apreensão, - ante a relevância para as investigações -, a fortiori,* não há óbice para se adentrar ao seu conteúdo – repise-se, já armazenado -, porquanto necessário ao deslinde do feito*. Não está configurada, pois, qualquer ilicitude na diligência empreendida.*

RESPEITO AOS DIREITOS INDIVIDUAIS NA INVESTIGAÇÃO CRIMINAL

Os julgados da SCOTUS e do STJ parecem tutelar de forma mais efetiva o direito à intimidade das pessoas, uma preocupação na ordem do dia em todo o mundo. Em linha de princípio, a autorização judicial é exigível, tanto em respeito à principiologia constitucional, quanto pela mudança infraconstitucional (Marco Civil da Internet). Com a prisão em flagrante e a apreensão dos objetos em posse da pessoa detida, cuidados simples como desligar o celular já previnem riscos de apagamento remoto e resguardam as provas eventualmente armazenadas no dispositivo. Se a prisão decorre de mandado, houve investigação prévia, na qual será possível verificar o interesse concreto na quebra do sigilo dos dados estáticos e pedir fundamentadamente a medida ao juízo competente.

Como aliás consta expressamente da decisão em Riley, a obtenção de um mandado judicial não é medida de especial dificuldade. Acresce-se que a imensa maioria das situações do cotidiano forense não apresenta urgência que justifique a exposição da intimidade do preso. Em geral o interesse na medida se dá para reforçar os elementos já existentes do crime e para investigar a existência de outros envolvidos. Nos dois casos,

a investigação pode esperar. Como já se disse, a justiça penal não se faz a qualquer preço.

Ainda que o respeito aos direitos individuais do detido não sensibilizasse os órgãos de persecução penal, o que não se coaduna com o Estado de Direito, vale destacar que não adequar o procedimento à tendência jurisprudencial aqui examinada redundará em trabalho em vão, ou seja, investigações que serão anuladas posteriormente, como exposto por Garcia (2017). É que precedentes de ambas as Turmas do STJ anularam provas assim obtidas (*exclusionary rule*). Não parece prudente dar azo a nulidades que se pode evitar. Apreendido o celular, deve-se acautelar o aparelho e representar pela quebra do sigilo, apontando as razões pelas quais se acredita haver interesse para a investigação na medida, como percebido por Sá (2017, p. 597-598).

Em termos mais mediatos, julga-se que a leitura dos precedentes listados demonstra a importância de ser enfrentada a questão do agravo à intimidade do detido, o direito difuso à segurança pública e a ponderação de tais princípios nos processos em curso. Este foi o eixo da decisão da SCOTUS, invocada no STJ, e parece ser a tendência, até pela pacificação em torno da distinção entre dados estáticos e em fluxo, que já vem de algumas décadas e é citada amplamente nos tribunais. Desenvolver argumentação analítica a respeito se torna curial para a persecução penal não se frustrar nas instâncias superiores e ser conduzida com respeito aos direitos individuais.

É certo que a SCOTUS e o voto da Ministra Maria Thereza de Assis Moura no RHC 51531 assinalaram que, em certas circunstâncias, a exigência de mandado / decisão judicial pode ser relativizada[54]. A SCOTUS apontou, dentre considerações de menor alcance prático (como a possibilidade dos policiais analisarem o celular para se certificarem de que não é uma arma[55]), que uma busca nos dados do celular pode prevenir os policiais no local de que eventuais comparsas do detido foram chamados para a cena do crime (o que se enquadra em duas das exceções decorrentes da *Chimel Rule*: buscas voltadas a impedir a fuga do detido e garantir a segurança dos policiais responsáveis pela prisão[56]). Admitiu-se ainda a possibilidade de evitar, no caso concreto, a destruição de provas, a busca de um suspeito em fuga, ou para ajudar pessoas

feridas ou ameaçadas de dano iminente. A análise da situação concreta pode revelar particularidades que legitimem o acesso imediato[57], mas é preciso dizer que se cuidam de casos excepcionais.[58].

Em suma, o acesso a dados armazenados em celulares exige dos operadores da persecução penal especial atenção, por se tratar de uma questão nova, com regulação ainda incipiente e cuja importância só tende a aumentar, pela penetração dos celulares na vida da população e sua inegável utilidade na comunicação, aspecto chave em empreitadas criminosas. Aguarda-se nova orientação do STF, aperfeiçoando a tutela à intimidade, diante das radicais mudanças sociais e tecnológicas desde seu posicionamento anterior na temática.

CONCLUSÕES

a) A Constituição brasileira possui dispositivos que visam tutelar a intimidade do indivíduo, inclusive em processos e procedimentos criminais. Desde a promulgação da Constituição de 1988 até meados da década de 2010, a proteção foi entendida como incidente apenas sobre os dados em fluxo ou dinâmicos, é dizer, sobre a comunicação de dados.

b) Com a edição do Marco Civil da Internet, a proteção passou a abranger também dados estáticos, armazenados nos aparelhos celulares. Paralelamente a isso, foi possível constatar significativas mudanças na relação das pessoas com seus celulares, à medida que estes ganhavam em potência e funcionalidades. O acesso aos dados armazenados (ou estáticos) de um celular revela muito da privacidade de seu proprietário, o que recomenda cautelas adicionais por parte do Judiciário.

c) Esse novo quadro ensejou decisão da Suprema Corte norte-americana (precedente Riley vs. California), estabelecendo como regra, a necessidade de mandado judicial para acesso a dados armazenados em celulares. A decisão tutela de maneira mais hígida a intimidade das pessoas e impõe limites razoáveis à ação das forças policiais. Sua fundamentação vai ao encontro das mudanças sociais e tecnológicas das últimas décadas.

d) A decisão americana é diametralmente oposta ao paradigma interno: o HC 91.867/PA, julgado pelo Supremo Tribunal Federal, que dispensou de mandado o acesso a dados constantes de celular apreendido com preso em flagrante, embora sem enfrentamento direto da pauta constitucional envolvida.

e) Apesar da existência de precedente do STF a respeito, a jurisprudência do STJ parece se direcionar para a aplicação do entendimento do julgado estrangeiro, existindo inclusive citações expressas a Riley vs. California. Essa postura demonstra a influência do direito comparado na contemporaneidade, postura saudável e cosmopolita.

f) As mudanças fática e de marco legal, aconselham a adoção do procedimento de pleitear previamente mandado judicial para acesso aos dados armazenados nos celulares apreendidos, para evitar trabalho em vão e a contaminação das investigações pela nulidade das provas ilicitamente obtidas.

NOTAS

1 Dados podem ser entendidos como "fatos coletados, analisados e interpretados pelos cientistas sociais – um conjunto de dados é designado *data* (do latim *data*, plural de *datum*, 'dado')" ou como "representação de fatos, conceitos ou instruções, através de sinais de uma maneira formalizada, passível de ser transmitida ou processada pelos seres humanos ou por meios automáticos" (RABAÇA, Carlos Alberto; BARBOSA, Gustavo Guimarães. *Dicionário de Comunicação*. 2.ed., Rio de Janeiro: Elsevier, 2001, p. 207, *apud* FIORILLO, 2015, p. 13).

2 CASTELLS, Manuel. *A Sociedade em Rede.* São Paulo: Paz e Terra, 2013, p. 119. Mas o autor também adverte (*Op. cit.*, p. 40) acerca dos novos problemas que surgem: "(...) as atividades criminosas e organizações ao estilo da máfia de todo o mundo também se tornaram globais e informacionais, propiciando os meios para o encorajamento de hiperatividade mental e desejo proibido, juntamente com toda e qualquer forma de negócio ilícito procurado por nossas sociedades, de armas sofisticadas à carne humana"

3 Um painel do surgimento de um direito das tecnologias móveis (*Mobile & Wearable Law*) pode ser encontrado em TEIXEIRA, Tarcisio; LOPES, Alan Moreira. *Direito das Novas Tecnologias*. São Paulo: Editora Revista dos Tribunais, 2015, p. 243-296. Os autores entendem a mobilidade como baseada na "desnecessidade de um computador com *mouse* e teclado para acesso à Internet" (fl. 245). A tecnologia *mobile* é a encontrada em smartphones, por exemplo; a *wearable* teria como exemplos o *Google Glass* e os relógios inteligentes.

4 BARROSO, Luís Roberto: A Dignidade da Pessoa Humana no Direito Constitucional Contemporâneo: a construção de um conceito jurídico à luz da jurisprudência mundial. Belo Horizonte: Editora Fórum, 2012, p.11.

5 WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy.* Harvard Law Review, Vol. 4, N. 5 (15 de dezembro de 1890), p. 193-220. Disponível em http://links.jstor.org/sici?sici=-

0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C. Acesso em 02 de maio de 2017.

6 Literalmente, no original: "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone' Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'" (*Op. cit.,* p. 195). Adiante (p. 220), consta o trecho que inspira o título deste artigo: "The common law has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands".

7 FERRAZ JUNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da USP, nº 88 (1993). Disponível em: http://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em 22 de dezembro de 2016.

8 XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

9 *Op. cit.*, p. 446.

10 Vale lembrar que o artigo 57, II, 'e' da Lei 4117/62 considerava não haver violação de telecomunicações quando se desse conhecimento ao juiz competente, mediante requisição ou intimação deste. Entretanto, o marco constitucional então vigente (Constituição de 1967, após a EC 1/69) resguardava o sigilo das comunicações telefônicas sem qualquer ressalva, em seu artigo 153, §9º, gerando controvérsia doutrinária acerca da constitucionalidade do dispositivo. Nesse sentido: RASSI, João Daniel; CASCALDI, Luís de Carvalho. *Considerações sobre a quebra do sigilo de dados telefônicos.* Revista de Direito das Comunicações, vol. 3/2011.

11 No mesmo sentido: HC 74.586, rel. min. Marco Aurélio, j. 5-8-1997, 2ª T, DJ de 27-4-2001; HC 69.912 segundo, rel. min. Sepúlveda Pertence, j. 16-12-1993, P, DJ de 25-3-1994 (este aparentemente o *leading case*).

12 O julgado é de 1995, antes da edição da Lei 9296/96; o inciso XII surgiu apenas como matéria auxiliar, posto que o cerne do julgamento foi o sigilo bancário.

13 HC 91.867 / PA, rel. Min. Gilmar Mendes. O *leading case*, no ponto, é o RE 418.416/SC, rel. Min. Sepúlveda Pertence. A ementa deste, no particular, consigna: "(...) 3. Não há violação do art. 5º. XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve 'quebra de sigilo das comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial'. 4. A proteção a que se refere o art.5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador. (cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270)".

14 Comentários à Constituição do Brasil, p.293.

15 X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

16 Art. 244. A busca pessoal independerá de mandado, no caso de prisão ou quando houver fundada suspeita de que a pessoa esteja na posse de arma proibida ou de objetos ou papéis que constituam corpo de delito, ou quando a medida for determinada no curso de busca domiciliar.

17 O número de celulares no Brasil foi estimado (abril de 2016) em cerca de cento e sessenta e oito milhões de aparelhos; dados da 27ª Pesquisa Anual de Administração e Uso de Tecnologia da Informação nas Empresas, da Fundação Getúlio Vargas de São Paulo (FGV-SP), atestam que no país existem mais smartphones que computadores (entre desktops, notebooks e tablets, cerca de cento e sessenta milhões de aparelhos).

18 https://www.terra.com.br/noticias/ciencia/ha-43-anos-homem-chegava-a-lua-com-computador-de-2-kb-de-ram,582a8116492da310VgnCLD200000bbcceb0aRCRD.html, acesso em 12 de outubro de 2017.

19 É oportuna a referência a RUDDER, Christian. *Dataclisma. Quem somos quando achamos que ninguém está vendo.* Rio de Janeiro: Bestseller, 2015, p. 246: "Sempre que o Facebook atualiza seus Termos de Serviço para aumentar ainda mais o alcance sobre nossos dados, ficamos furiosos

por um dia, e voltamos ao site no dia seguinte, como tantas abelhas que, ao não ter quem ferroar, só podem voltar para a colmeia".

20 *Op. cit*, p. 240.

21 VALENTE, Mariana Giorgetti Valente. Smartphones: Baús do tesouro da Lava-Jato. Disponível em: http://link.estadao.com.br/blogs/deu-nos-autos/smartphones-baus-do-tesouro-da-lava-jato/.

22 Ex-analista da Central Intelligence Agency (CIA) que efetuou vazamento de informações que comprovaram a atuação do governo americano no sentido de uma vigilância digital massiva, inclusive de seus próprios cidadãos. O governo dos EUA contava, em tal empreitada, com a colaboração de várias das empresas de tecnologia do país. Após o vazamento, e para não perder clientes, as empresas passaram a investir pesadamente em criptografia. Para um relato abrangente e vindo de um dos protagonistas do fato, consultar GREENWALD, Glenn. *Sem lugar para se esconder. Edward Snowden, a NSA e a espionagem do governo americano.* Rio de Janeiro: Sextante, 2014.

23 Para Rabaça e Barbosa (2014, p. 63), criptografia é o "Recurso usado para transformar mensagens de correio eletrônico, correios de voz, programas ou arquivos em sinais cifrados, com objetivo de impedir o acesso de pessoas não autorizadas. Feita através de programas de proteção, é muito utilizada na internet para proteger informação."

24 ROHR, Altieres. O fim dos grampos. Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/o-fim-dos-grampos.html. Destaca-se trecho da matéria: "O WhatsApp anunciou a medida mais profunda: usuários da versão Android do aplicativo já contam com criptografia ponto a ponto. Nessa modalidade, nenhum grampo intermediário tem qualquer efeito. Nem o WhatsApp, nem o provedor de serviço de internet podem acessar o conteúdo da mensagem. *O único jeito é obtendo o aparelho*, mas, caso o telefone esteja criptografado – o que é possível em alguns casos –, obter as mensagens pode ser muito difícil" (original sem *grifo*).

25 Em 1997, a Lei 9472, artigo 3º, incisos V e IX, estabeleceu ser direito do usuário de telecomunicações a inviolabilidade e segredo de suas comunicações, bem como o respeito à privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora de serviço. A previsão, entretanto, não gerou maior debate jurisprudencial ou doutrinário.

26 Neste sentido MENDES, Gilmar; PINHEIRO, Jurandi Borges. *Interceptações e privacidade: novas tecnologias e a Constituição.* In: Direito, Inovação e Tecnologia. p. 233.

27 Uma busca pelas palavras-chave "dados celular penal" no sítio do STF aponta o HC 91867 como o mais recente (para não dizer o único) precedente colegiado (2ª Turma) em que o STF enfrentou a matéria, sendo este o critério de escolha. A última pesquisa se deu em 19 de fevereiro de 2017.

28 O precedente trata, na verdade, de dois casos similares: Riley vs. California e Wurie vs. United States. Em prol da concisão e por ser o caso que nominou o precedente, será feita referência apenas ao primeiro.

29 Definido no precedente como "a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity": em tradução livre, "um celular com uma ampla gama de outras funções, baseadas em avançada capacidade computacional, grande capacidade de armazenamento, e conexão com a internet".

30 Conforme Whitebread e Slobogin (2015, p. 164), este aspecto ficou conhecido como "armspan rule". Armspan é a distância entre o fim de um braço de uma pessoa até o fim do outro braço, colocados em linha reta e paralela com o chão.

31 Tradução livre. No original: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized".

32 Warrantless searches conducted in exigent circumstances do not violate the Fourth Amendment so long as the police did not create the exigency by violating or threatening to violate the Fourth amendment. Em tradução livre: "Buscas sem mandado, realizadas em circunstâncias excepcionais não violam a Quarta Emenda desde que a polícia não tenha criado as circunstâncias excepcionais violando ou ameaçando violar a Quarta Emenda".

33 Sacolas revestidas com material (geralmente alumínio) que isola seu conteúdo da ação de ondas eletromagnéticas.

34 Por exemplo, ver United States vs. Robinson, 414 U.S. 218 (1973).

[35] O precedente traz dois exemplos: a existência de uma mensagem suspeita de um cúmplice que se suspeita esteja prestes a detonar uma bomba; e um sequestrador de crianças que possa ter informações sobre paradeiro de seu refém no celular.

[36] DANIELSEN, Erica L. *Cell Phone searches after Riley: establishing probable cause and applying search warrant exceptions.* Disponível em HeinOnLine, 36 Pace L. Rev. 970 2015-2016.

[37] Buscas pelas palavras-chave "dados celular penal" e "celular apreendido penal" no sítio do STF apontam o HC 91867 como o mais recente (para não dizer o único) precedente colegiado (2ª Turma) em que o STF enfrentou a matéria, sendo este o critério de escolha. A última pesquisa se deu em 16 de novembro de 2018.

[38] Fl. 15 do acórdão.

[39] Fl. 14 do acórdão.

[40] Ver fl. 17 do acórdão. O dispositivo mencionado tem a seguinte redação: Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá: I - dirigir-se ao local, providenciando para que não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais; II - apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais; III - colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;

[41] Discordando da fundamentação, no ponto em que compara o celular a uma agenda telefônica: DEZEM, Guilherme Madeira. *A espiritualização do domicílio: o novo conceito de domicílio e o Marco Civil da Internet*, p. 71.

[42] Fl. 17 do acórdão.

[43] Fl. 19 do acórdão.

[44] Cabe realçar que, em artigo doutrinário recente, o Min. Gilmar Mendes, relator do HC 91867/PA, assentou que o novo contexto da telefonia móvel torna "necessário que o acesso aos dados armazenados em tais dispositivos seja precedido de autorização judicial específica e circunstanciada" (*Op. cit.*,p. 236).

[45] Uma análise abrangente da influência do direito constitucional norte-americano pode ser encontrada em BARROSO, Luís Roberto. A Americanização do Direito Constitucional e seus Paradoxos: Teoria e Jurisprudência Constitucional no mundo contemporâneo. *In:* Filosofia e Teoria Constitucional Contemporânea. SARMENTO, Daniel (Coord.). Rio de Janeiro: Editora Lumen Juris, 2009.

[46] *Op. cit.*, p. 34.

[47] Ironicamente, nos EUA o recurso ao direito comparado não encontra grande ressonância, como demonstrado por BARROSO (*Op. cit.*, p.10-11 e 37-38, *v.g.*).

[48] No caso do Superior Tribunal de Justiça, buscou-se precedentes que citaram o caso Riley vs California, através de análise dos julgados que tratavam do tema celulares apreendidos ou que faziam referência ao HC 91.867/PA do STF. A ferramenta de busca do sítio do Tribunal não retorna resultados relevantes para a busca pelos termos "Riley" e "Riley vs California". Última pesquisa em 16 de novembro de 2018.

[49] Divulgado no Informativo 583 do Superior Tribunal de Justiça (maio de 2016). Disponível em https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201402323677&dt_publicacao=09/05/2016. Sinteticamente, cuidava-se de caso em que, no contexto de flagrante por tráfico de drogas, policiais acessaram o aplicativo *Whatsapp* do smartphone do detido. É relevante mencionar, até em abono da argumentação aqui desenvolvida, que o impetrante do Habeas Corpus fundou sua tese na violação do artigo 5º, inciso LVI da Constituição (fl. 1 do acórdão, relatório), e não no inciso X, demonstrando a tendência dos operadores do direito brasileiros aqui discutida.

[50] Divulgado no Informativo nº 593 do Superior Tribunal de Justiça (novembro de 2016). Disponível em https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201602394838&dt_publicacao=26/09/2016. Sinteticamente, a Polícia adentrou o apartamento de um dos réus, onde encontrou significativa quantidade de drogas. Havia mais uma pessoa no apartamento além do dono; apreendidos os celulares de ambos, e verificado o aplicativo *Whatsapp*, constatou-se que estavam em plena transação envolvendo as drogas, quando do flagrante.

[51] Já que mensagens armazenadas no aparelho são dados estáticos, que não estão ao abrigo do art. 5º, XII da Constituição, segundo a jurisprudência do STF, já referida no item 1, acima.

[52] Fls. 5-6 do acórdão.

[53] Um convite a que se reserve especial atenção a tal matéria, quando ela voltar à pauta daquela Corte, pela importância seminal que o caso terá para a investigação criminal no futuro.

[54] Para extensiva e frutífera discussão acerca das exceções à exigência de mandado na jurisprudência norte-americana, consultar DANIELSEN, Erica L., *op. cit.*

[55] "Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon- say, to determine whether there is a razor blade hidden between the phone and its case.".

[56] Embora seja necessário reconhecer que a SCOTUS não aprofundou este ponto, por entender que as alegações, embora reflitam um forte interesse das agências governamentais, não foram deduzidas com respaldo em situações reais, representando, em princípio, um alargamento da *Chimel rule*, melhor encaixáveis em outras exceções à regra da exigência de mandado.

[57] Discussões semelhantes brotam do voto-vista da Ministra Maria Thereza de Assis Moura, que reconheceu a possibilidade do acesso direto caso a situação concreta demonstre prejuízos à investigação ou a bens jurídicos (citando o caso da extorsão mediante sequestro, em que o fator tempo é essencial e o acesso direto pode garantir o resgate da vítima).

[58] A SCOTUS rejeitou a necessidade de assentar exceções mais específicas: "Each of the proposals is flawed and contravenes our general preference to provide clear guidance to law enforcement through categorical rules".

REFERÊNCIAS

BARROSO, Luís Roberto. A americanização do direito constitucional e seus paradoxos: teoria e jurisprudência constitucional no mundo contemporâneo. In: **Filosofia e teoria constitucional contemporânea**. Rio de Janeiro: Editora Lumen Juris, 2009.

BARROSO, Luís Roberto. **A dignidade da pessoa humana no direito constitucional contemporâneo**: a construção de um conceito jurídico à luz da jurisprudência mundial. Belo Horizonte: Editora Fórum, 2012.

BRASIL. Constituição da República Federativa do Brasil. **Diário Oficial da União**, Brasília, 05.out.1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm Acesso em: 22.dez.2016

BRASIL. **Decreto-Lei 3689, de 3 de outubro de 1941**. Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm Acesso em 22.dez.2016

BRASIL. **Lei 12965, de 23 de abril de 2014**: estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em 22.dez.2016

BRASIL. Supremo Tribunal Federal. **Habeas Corpus 72.588/PB**. Relator Ministro Maurício Corrêa. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=73874 Acesso em 22.dez.2016

BRASIL. Supremo Tribunal Federal. **Mandado de Segurança 21729/DF**. Relator Ministro Marco Aurélio. Relator para o acórdão: Ministro Néri da Silveira. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=85599 Acesso em 22.dez.2016

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário 418.416/SC**. Relator Ministro Sepúlveda Pertence. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=395790 Acesso em 25.mar.2017

BRASIL. Supremo Tribunal Federal. **Habeas Corpus 91867/PA**. Relator Ministro Gilmar Mendes. Disponível em : http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2792328 Acesso em 22.dez.2016

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus 51531/RO**. Relator Ministro Nefi Cordeiro. Disponível em: https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201402323677&dt_publicacao=09/05/2016 Acesso em 22.dez.2016

BRASIL. Superior Tribunal de Justiça**. Recurso em Habeas Corpus 67379/RN**. Relator Ministro Ribeiro Dantas. Disponível em: https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201600186073&dt_publicacao=09/11/2016 Acesso em 22.dez.2016

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus 75800/PR**. Relator Ministro Felix Fischer. Disponível em: https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201602394838&dt_publicacao=26/09/2016 Acesso em 22.dez. 2016

CANOTILHO, J.J. Gomes; MENDES, Gilmar F.; SARLET, Ingo W.; STRECK, Lenio L. (coords). **Comentários à Constituição do Brasil**. São Paulo: Saraiva / Almedina, 2013. 2380 p.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 2013.

DANIELSEN, Erica L. **Cell phone searches after Riley**: establishing probable cause and applying search warrant exceptions. 36 Pace L. Rev. 970 2015-2016.

DEZEM, Guilherme Madeira. A espiritualização do domicílio: o novo conceito de domicílio e o marco civil da internet. In: MASSO, Fabiano Del; ABRUSIO, FLORÊNCIO FILHO, Juliana; Marco Aurélio (Coord.). **Marco civil da internet**: Lei 12.965/2014. São Paulo: Editora Revista dos Tribunais, 2014.

ESTADOS UNIDOS DA AMÉRICA. Suprema Corte dos Estados Unidos. **Riley vs. California**. Disponível em: https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf Acesso em 22.dez.2016.

FERRAZ JUNIOR, Tércio Sampaio. **Sigilo de dados**: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da USP, nº 88 (1993). Disponível em: http://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em 10 de novembro de 2016.

FIORILLO, Celso Antônio Pacheco. **O marco civil da internet e o meio ambiente digital na sociedade da informação**: comentários à lei n. 12.965/2014. São Paulo: Saraiva, 2015.

FOWLEY, Stephen; BRADSHAW, Tim. Bill Gates apoia solicitação do FBI para hackear iPhone de terrorista. **Folha de São Paulo**, 2016. Disponível em: http://www1.folha.uol.com.br/tec/2016/02/1742383-bill-gates-apoia-solicitacao-do-fbi-para-hackear-iphone-de-terrorista.shtml. Acesso em 23.fev.2016.

GARCIA, Rafael de Deus. **Acesso a dados em celular exige autorização judicial**. Disponível em: <http://www.conjur.com.br/2017-fev-06/rafael-garcia-acessodados-celular-exige-autorizacao-judicial>. Acesso em 16.nov.2018.

GREENWALD, Glenn. **Sem lugar para se esconder**: Edward Sonwden, a NSA e a espionagem do governo americano. Rio de Janeiro: Sextante, 2014.

LIMA, Renato Brasileiro de. **Manual de processo penal**. Salvador: Editora Jus Podivm, 2014.

MANJOO, Farhad. Briga de Apple e FBI mostra batalha de empresas contra vigilância. **Folha de São Paulo**, 2016. Disponível em: http://www1.folha.uol.

com.br/tec/2016/02/1740813-briga-entre-apple-e-fbi-evidencia-setor-mais-combativo-quanto-a-privacidade.shtml. Acesso em 22.fev.2016.

MENDES, Gilmar Ferreira. PINHEIRO, Jurandi Borges. Interceptações e privacidade: novas tecnologias e a Constituição. In: MENDES , Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015.

OLDHAM, Tami ; TUCKER, Eric. Por que EUA e apple estão em guerra sobre o desbloqueio de um celular?. **Jornal Folha**. São Paulo, 2019. Disponível em: http://www1.folha.uol.com.br/mundo/2016/02/1741781-por-que-eua-e-apple-estao-em-guerra-sobre-o-desbloqueio-de-um-celular.shtml. Acesso em 22.fev.2016.

RASSI, João Daniel; CASCALDI, Luís de Carvalho. Considerações sobre a quebra do sigilo de dados telefônicos. **Revista de Direito das Comunicações**, vol. 3/2011, p. 97-124, Jan-Jun 2011 DTR 2011/1891

ROHR , Altieres. O fim dos grampos?. **G1**, Rio de janeiro, 2016. Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/o-fim-dos-grampos.html. Acesso em 22.fev.2016.

ROSA, Alexandre Morais da; HEIL, Danielle Mariel. **O celular do preso em flagrante pode ser vasculhado? o** caso do matador incauto e o STF. Disponível em: http://emporiododireito.com.br/o-celular-do-preso-em-flagrante-pode-servasculhado-o-caso-do-matador-incauto-e-o-stf-por-alexandre-morais-da-rosae-danielle-mariel-heil/. Acesso em 16.nov.2018.

RUDDER, Christian. **Dataclisma**: quem somos quando achamos que ninguém está vendo. Rio de Janeiro: Bestseller, 2015.

SÁ, Priscilla Placha. Questões político-criminais e processuais penais sobre a investigação criminal de chacinas protagonizadas por facções criminais nos presídios brasileiros. **Revista brasileira de direito processual penal**, S.l., v. 3, n. 2, p. 567-604., 2017. Disponível em: <http://201.23.85.222/biblioteca/index.asp?codigo_sophia=135470>. Acesso em: 18 nov. 2018.

TEIXEIRA, Tarcisio; LOPES, Alan Moreira. **Direito das novas tecnologias**: legislação eletrônica comentada, mobile law e segurança digital. São Paulo: Editora Revista dos Tribunais, 2015.

VALENTE. Mariana Giorgetti. Smartphones: baús do tesouro da lava jato. **Jornal Estadão**, São Paulo, 2016. Disponível em: http://link.estadao.com.br/blogs/deu-nos-autos/smartphones-baus-do-tesouro-da-lava-jato/ Acesso em 22.dez.2016.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy** : Harvard Law Review, Vol. 4, N. 5 (15 de dezembro de 1890), p. 193-220. Disponível em http://links.jstor.org/sici?sici=0017-811X%2818901215%294%3A5%3C193%3ATRTP%3E2.0.CO%3B2-C Acesso em 02 de maio de 2017.

WHITEBREAD, Charles H. e SLOBOGIN, Christopher. **Criminal procedure**: an analysis of cases and concepts. 6. ed. Nova Iorque: University Textbook Series, Foundation Press, 2015.

Enviado em: 4-11-2017
Recebido em: 27-11-2018

Luís Renato Vedovato

Doutor (2012), mestre (2002) e graduado (1995) pela Faculdade de Direito da Universidade de São Paulo; professor MS-3 da UNICAMP; professor do Programa de Mestrado em Direito da Universidade Metodista de Piracicaba (UNIMEP); professor de Direito Internacional da Pontifícia Universidade Católica de Campinas (PUC de Campinas); e professor Convidado do Programa de Pós-Graduação em Educação (Mestrado e Doutorado) da Faculdade de Educação da Universidade Estadual de Campinas (UNICAMP).

E-mail: lrvedovato@gmail.com

Leandro Zedes

Mestrando em Direitos Difusos e Coletivos pela Universidade Metodista de Piracicaba; bacharel em Direito pela Universidade Federal de Goiás; e especialista em Sistemas de Justiça Criminal pela Escola Superior do Ministério Público da União. Procurador da República no Município de Piracicaba, São Paulo. E-mail: leandrozedes@gmail.com

Universidade Metodista de Piracicaba

Rod. do Açúcar, km- 156 - Taquaral, Piracicaba - SP