ESCOLA DA MAGISTRATURA DO ESTADO DO RIO DE JANEIRO

INVESTIGAÇÃO CRIMINAL E OS DADOS OBTIDOS SEM AUTORIZAÇÃO JUDICIAL DE APARELHOS CELULARES APREENDIDOS, SOB A ÓTICA DO ABUSO DE AUTORIDADE

Ruy Zaidan Azevedo

Rio de Janeiro
2020

RUY ZAIDAN AZEVEDO

INVESTIGAÇÃO CRIMINAL E OS DADOS OBTIDOS SEM AUTORIZAÇÃO JUDICIAL DE APARELHOS CELULARES APREENDIDOS, SOB A ÓTICA DO ABUSO DE AUTORIDADE

Artigo científico apresentado como exigência de conclusão de Curso de Pós-Graduação *Lato Sensu* da Escola da Magistratura do Estado do Rio de Janeiro.
Professores Orientadores:
Mônica C. F. Areal
Nelson C. Tavares Junior

Rio de Janeiro
2020

INVESTIGAÇÃO CRIMINAL E OS DADOS OBTIDOS SEM AUTORIZAÇÃO JUDICIAL DE APARELHOS CELULARES APREENDIDOS, SOB A ÓTICA DO ABUSO DE AUTORIDADE

Ruy Zaidan Azevedo

Graduado pela Faculdade de Direito da Universidade Federal de Juiz de Fora. Advogado.

Resumo – com o desenvolvimento tecnológico, o conflito entre a violação da privacidade e a garantia da segurança pública ganhou destaque na discussão acerca da possibilidade de quebra de sigilo de aparelho celular apreendido sem prévia autorização judicial. Com isso, a verificação das distintas proteções conferidas às comunicações telefônicas e aos dados telefônicos, sob a ótica da doutrina e jurisprudência, é essencial para a verificação da aplicação da reserva jurisdicional na hipótese, a qual se entende por inadequada diante da importância de uma investigação criminal eficaz. Outrossim, com a recente entrada em vigor da nova Lei de Abuso de Autoridade, surge mais um aspecto a ser observado pela Autoridade Policial, no tocante à violação do princípio do *nemo tenetur se detegere*.

Palavras-chave – Direito Processual Penal. Aparelhos celulares apreendidos. Quebra de sigilo. Autorização judicial. Abuso de Autoridade.

Sumário – Introdução. 1. A importância dos dados dos aparelhos celulares apreendidos para uma investigação criminal eficaz: uma análise do conflito entre a violação da privacidade e a garantia da segurança pública. 2. A distinção de proteções conferidas à comunicação telefônica e aos dados e registros telefônicos como pressuposto essencial para a apuração da necessidade de reserva jurisdicional. 3. A nova Lei do abuso de autoridade e a possível caracterização de crime diante da quebra do sigilo dos dados sem autorização judicial: mais um aspecto a ser enfrentado. Conclusão. Referências.

INTRODUÇÃO

A presente pesquisa científica discute se o ordenamento jurídico pátrio admite a obtenção de dados e registros em aparelhos celulares apreendidos sem autorização judicial específica para tanto, a fim de instruírem investigações criminais efetivas, bem como se tal prática configuraria crime de abuso de autoridade.

A popularização e o desenvolvimento tecnológico dos aparelhos celulares modificaram a forma de interação das pessoas. O telefone celular, que há relativamente pouco tempo somente efetuava ou recebia chamadas, passou a ser um aparelho multifuncional, possibilitando o envio e recebimento de mensagens, fotografar, filmar, ter conexão com Internet

móvel, determinar a sua posição geográfica, enviar e receber e-mails, armazenar os mais diversos dados, entre outras funções.

Assim, em um processo natural, o telefone celular passou a ser muito utilizado como meio para o cometimento dos mais variados crimes, desde a simples ameaça, até o estelionato, a extorsão mediante sequestro e o tráfico de drogas, bem como para a estruturação de organizações criminosas, muitas vezes de dentro de presídios e penitenciárias.

No primeiro capítulo do trabalho, assim, analisa-se o cenário atual da criminalidade, em que os infratores se utilizam dos aparelhos celulares como potencializadores e meios diretos de suas ações. Dessa forma, a polícia judiciária tem enfrentado certa dificuldade na investigação de crimes, principalmente no que se refere à licitude da obtenção de dados sem autorização judicial, sob o argumento de que os mesmos são constitucionalmente acobertados por sigilo, o que traz à tona o conflito entre a violação da privacidade e a garantia da segurança pública.

Segue-se, no segundo capítulo, analisando as proteções jurídicas e garantias legais distintas entre comunicação telefônica e registros e dados telefônicos, necessárias para se apurar a necessidade ou desnecessidade da autorização judicial específica no caso concreto, a partir de exames doutrinários e jurisprudenciais.

Por fim, o terceiro capítulo aborda a potencial caracterização do crime de abuso de autoridade, em destaque com a recente entrada em vigor da Lei nº 13.869/19, frente a determinadas hipóteses de quebra do sigilo de aparelho celular apreendido sem prévia autorização judicial.

Dessa forma, pelo método dedutivo, valendo-se da bibliografia pertinente à temática em foco – analisada e fichada na fase exploratória da pesquisa (legislação, doutrina e jurisprudência), busca-se sustentar a tese de que os aparelhos celulares apreendidos regularmente na posse de investigados não só podem, como devem ser submetidos ao exame pericial por constituírem corpo do delito, sendo prescindível e desproporcional, nesses casos, a exigência de autorização judicial específica.

A pesquisa desenvolvida, assim, é de natureza qualitativa, do tipo descritiva e exploratória, com abordagem teórica, recorte transversal com perspectiva longitudinal e fundamentada em dados secundários.

1. A IMPORTÂNCIA DOS DADOS DOS APARELHOS CELULARES APREENDIDOS PARA UMA INVESTIGAÇÃO CRIMINAL EFICAZ: UMA ANÁLISE DO CONFLITO ENTRE A VIOLAÇÃO DA PRIVACIDADE E A GARANTIA DA SEGURANÇA PÚBLICA

O advento das tecnologias de informação, principalmente no que se refere ao desenvolvimento tecnológico dos aparelhos celulares, trouxe consigo enormes benefícios à humanidade, sobretudo no que se refere ao encurtamento da distância entre as pessoas, introduzindo uma nova era em todos os campos da vida cotidiana. Assim, o avanço tecnológico permite que se saiba a localização exata de uma pessoa através do GPS de seu aparelho celular, bem como que o seu portador tenha uma central multimídia ao alcance dos dedos, bastando apenas ter seu aparelho conectado à Internet e/ou em área de cobertura para interagir.

Diante desse cenário de encurtamento de distâncias, as ações criminosas ganharam novas linhas e passaram a se caracterizar por sua alta velocidade de realização, sendo relevante destacar a capacidade de adaptação dos agentes às novas tecnologias, com modificação quase que instantânea de seus *modus operandi* para fazer frente a novos padrões de segurança de empresas ou instituições.

Em reportagem publicada no "Jornal O Dia", em 19 de janeiro de 2020, o jornalista Anderson Justino[1] apurou que o número de estelionatos no ano de 2019 no Rio de Janeiro cresceu 19,6% em relação ao ano anterior, sendo que grande parte deles se deu através de um golpe consistente na invasão de contas do aplicativo de mensagens "*WhatsApp*". Na reportagem, o jornalista pontuou, também, os cinco golpes mais famosos aplicados pelo telefone celular. Por fim, informou a ocorrência de crimes de extorsão virtual envolvendo a ameaça de divulgação de imagens de nudez de mulheres, prática que tem se tornado comum.

Nesse sentido, é induvidoso que as novas tecnologias de informação e interação, que influenciam diversas áreas das atividades econômicas, sociais, culturais e políticas, acabam por também ensejar o aparecimento de novos crimes, principalmente envolvendo golpes e privacidade. Além disso, outros crimes recorrentes, como a associação para o tráfico de drogas, por exemplo, se adequam à essa nova realidade, de modo que os aparelhos celulares e, especialmente seus aplicativos de mensagens, servem à estruturação dessas organizações.

[1] JUSTINO, Anderson. *Estelionato via WhatsApp cresce 19% no Rio*. Disponível em: < https://odia.ig.com.br/rio-de-janeiro/2020/01/5856704-estelionato-via-whatsapp-cresce-19--no-rio.html>. Acesso em: 10 abr. 2020.

O legislador, dentro de sua competência, não ignorou por completo tal cenário de modificação social, pelo que foi inserido no Código de Processo Penal[2], a partir da Lei nº 13.344/16[3], o art. 13-B. Referido dispositivo possibilita que, nos crimes associados ao tráfico de pessoas, o membro do Ministério Público ou o Delegado de Polícia requisitem, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicação e/ou telemática a disponibilização imediata dos meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso.

Em complemento, o §4º[4] do supracitado dispositivo, o qual merece destaque, dispõe que caso não haja manifestação judicial no prazo de 12 horas acerca da requisição, a autoridade competente poderá requisitar a disponibilização imediata dos meios técnicos diretamente às empresas prestadoras de serviço de telecomunicação e/ou telemática, ou seja, sem a autorização judicial específica, apenas comunicando o juiz de imediato.

Nessa linha, dentro da persecução penal que, em regra, é dever do Estado, tem-se que uma vez praticada a infração penal, cumpre também a ele, em princípio, a apuração e o esclarecimento dos fatos e de todas as suas circunstâncias. Nos termos do art. 6º do Código de Processo Penal[5], assim que tomar conhecimento da prática de um crime, o Delegado de Polícia deverá realizar diversas diligências no sentido de identificar a sua autoria e resguardar o conjunto probatório, apreendendo, por exemplo, qualquer objeto que tenha relação com o fato investigado.

Assim, a apreensão do celular do flagranteado é permitida e não precisa de autorização judicial. Porém, o entendimento atual do Superior Tribunal de Justiça é o de que os dados constantes nesses aparelhos celulares estão protegidos pelo sigilo telefônico, conforme se verifica por dois Informativos de Jurisprudência publicados pelo Tribunal:

> Na ocorrência de autuação de crime em flagrante, ainda que seja dispensável ordem judicial para a apreensão de telefone celular, as mensagens armazenadas no aparelho estão protegidas pelo sigilo telefônico, que compreende igualmente a transmissão, recepção ou emissão de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza, por meio de telefonia fixa ou móvel ou, ainda, por meio de sistemas de informática e telemática.

---

[2] BRASIL. *Código de Processo Penal*. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 02 set. 2019.
[3] BRASIL. *Lei nº 13.344*, de 06 de outubro de 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13344.htm>. Acesso em: 02 set. 2019.
[4] Ibid.
[5] BRASIL, op. cit., nota 2.

> STJ. 5ª Turma. RHC 67.379-RN, Rel. Min. Ribeiro Dantas, julgado em 20/10/2016 (Info 593).[6]
>
> Sem prévia autorização judicial, são nulas as provas obtidas pela polícia por meio da extração de dados e de conversas registradas no whatsapp presentes no celular do suposto autor de fato delituoso, ainda que o aparelho tenha sido apreendido no momento da prisão em flagrante.
> STJ. 6ª Turma. RHC 51.531-RO, Rel. Min. Nefi Cordeiro, julgado em 19/4/2016 (Info 583).[7]

Entretanto, conforme será melhor examinado no próximo capítulo, o acesso pela Autoridade Policial aos dados constantes em aparelho celular apreendido no flagrante não encontra o mesmo impedimento da interceptação telefônica, pelo que a jurisprudência do Superior Tribunal de Justiça, com a devida vênia, não guarda o devido rigor técnico, configurando um obstáculo à uma investigação criminal célere e eficiente. O acesso aos dados e registros se caracteriza apenas como uma das providências previstas no art. 6º do Código de Processo Penal[8], a qual não se sujeita à reserva de jurisdição.

A liberdade é o bem, depois da vida, mais importante do indivíduo. Entretanto, mesmo com esse grau de importância, qualquer pessoa pode ser presa em flagrante delito, ou seja, mesmo sem haver processo e juízo de culpabilidade. Dessa forma, com relação à privacidade, se faz necessária a ponderação de valores constitucionais, estando de um lado o direito fundamental à privacidade e de outro o direito à segurança pública.

Na presença deste conflito entre direito à intimidade e direito à segurança, o caso concreto impõe um processo de ponderação, que leve em conta os interesses em jogo e a realidade social. A restrição de um dos direitos em detrimento do outro deve obedecer ao princípio da proporcionalidade.

Assim, tem-se que a investigação criminal produz provas buscando a verdade real. É legítima na medida em que o faz respeitando o limite intransponível dos direitos e garantias individuais. Estes, por sua vez, constituem condição de possibilidade de um Estado Democrático de Direito, pelo que não se deve buscar a verdade a qualquer custo, ou seja, afrontando garantias fundamentais.

Contudo, há que se destacar que, com o avanço da tecnologia, surgiu a possibilidade de se acessar remotamente os dispositivos móveis, através das contas exigidas pelos sistemas operacionais para a utilização dos telefones, e, dessa forma, apagar todos os dados e registros

---

[6] BRASIL. Superior Tribunal de Justiça. *Informativo de Jurisprudência nº 593*. Disponível em: <https://scon.stj.jus.br/docs_internet/informativos/PDF/Inf0593.pdf>. Acesso em: 19 mai. 2020.
[7] BRASIL. Superior Tribunal de Justiça. *Informativo de Jurisprudência nº 583*. Disponível em: < https://scon.stj.jus.br/SCON/SearchBRS?b=INFJ&tipo=informativo&livre=@COD=%270583%27>. Acesso em: 19 mai. 2020.
[8] BRASIL, op. cit., nota 2.

contidos nos aparelhos. Nos sites da Apple[9], da Microsoft[10] e do Google[11], principais empresas do meio, há tutorial de como apagar remotamente o dispositivo, restaurando o dispositivo para as condições de fábrica.

Assim, no prazo para se obter a decisão judicial autorizativa, nos moldes exigidos pelo Superior Tribunal de Justiça, há plena viabilidade técnica de os dados contidos nos aparelhos celulares serem remotamente apagados. A possibilidade de restaurar o dispositivo se revela de extrema valia para quem teve seu bem subtraído, por exemplo, mas não se pode ignorar que tal alternativa também serve para fins ilícitos, com a destruição das provas de um crime.

A expectativa de privacidade, portanto, não pode servir para amparar crimes que estão em plena consumação, tal como o tráfico de drogas, e muito menos para salvaguardar associações e organizações criminosas, legitimando a impunidade. No cenário atual da criminalidade, respostas que poderiam ser dadas rapidamente em uma investigação de determinado crime ficam prejudicadas aguardando por uma ordem judicial não necessária, diante de uma interpretação do Superior Tribunal de Justiça em desconformidade com a legislação.

2. A DISTINÇÃO DE PROTEÇÕES CONFERIDAS À COMUNICAÇÃO TELEFÔNICA E AOS DADOS E REGISTROS TELEFÔNICOS COMO PRESSUPOSTO ESSENCIAL PARA A APURAÇÃO DA NECESSIDADE DE RESERVA JURISDICIONAL

Nos termos do art. 5º, XII, da Constituição Federal[12], é assegurada, como direito fundamental, a proteção das comunicações telefônicas, cujo sigilo somente pode ser quebrado para fins de investigação criminal ou instrução processual penal mediante ordem judicial, diante de hipóteses previstas e reguladas em lei – atualmente vigorando no país sobre o tema a Lei nº 9.296/96[13].

Não se discute, dessa forma, que as comunicações telefônicas recebem especial proteção constitucional, sendo ilícito qualquer acesso a elas sem prévia decisão judicial.

---

[9] APPLE. *Find my iPhone:* Apagar seu dispositivo. Disponível em: <https://support.apple.com/kb/PH19300?locale=pt_BR#:~:text=Se%20ele%20estiver%20off%2Dline,senha%20de%20seu%20ID%20Apple>. Acesso em: 10 abr. 2020.

[10] MICROSOFT. *Realizar uma limpeza remota em um telefone móvel.* Disponível em: <https://docs.microsoft.com/pt-br/exchange/clients/exchange-activesync/remote-wipe?view=exchserver-2019>. Acesso em: 10 abr. 2020.

[11] GOOGLE. *Localize, bloqueie ou apague um dispositivo Android perdido*. Disponível em: < https://support.google.com/nexus/answer/6160491?hl=pt>. Acesso em: 10 abr. 2020.

[12] BRASIL. *Constituição da República Federativa do Brasil*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm>. Acesso em: 02 set. 2019.

[13] BRASIL. *Lei nº 9.296*, de 24 de julho de 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em: 02 set. 2019.

Entretanto, o Superior Tribunal de Justiça utilizou-se da supracitada disposição constitucional para consolidar o entendimento de que os dados telefônicos estão protegidos pelo mesmo sigilo, o que não se revela tecnicamente adequado.

Os dados telefônicos constituem registros e informações contidas na memória de aparelho de telefone celular, ao passo que a proteção dada pelo art. 5º, XII, da Constituição Federal[14] é quanto a proibição da intervenção de um terceiro num ato de comunicação para se obter esta prova, que de outro modo perder-se-ia, através da interceptação telefônica.

A proteção conferida é da inviolabilidade do fluxo de dados em trânsito, tecnicamente denominada comunicação. Tércio Sampaio Ferraz Júnior[15] distingue dois tipos de comunicação: há, de um lado, formas de comunicação marcadas por "instantaneidade", como a comunicação telefônica, que "só é enquanto ocorre"; e há, de outro, aquelas que deixam vestígios físicos, sendo, portanto, suscetíveis de investigação sem necessitar de interceptação.

Assim, a obtenção de registros telefônicos, fotos, vídeos e, principalmente de conversas mantidas por aplicativos de mensagens, não constitui captação em tempo real, instantânea, muito por conta inclusive da proteção da criptografia utilizada pela tecnologia dos aplicativos de mensagens. Nesse sentido, ensina Eduardo Cabette[16] que na interceptação telefônica está ínsita a presença de um terceiro que não seja um dos interlocutores e que, ademais, não lhe seja de conhecimento, sem a qual descaracteriza-se a figura da interceptação, havendo terminologias mais apropriadas.

Portanto, o que a norma fundamental do art. 5º, XII, da Constituição Federal[17] pretende evitar é tão somente a interferência de terceiros no processo comunicativo estabelecido entre os interlocutores. Nas palavras de Tércio Sampaio Ferraz Júnior[18]:

> [...] a distinção é decisiva: o objeto protegido no direito a inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações (comunicação) privativa é que não pode ser violada por sujeito estranho à comunicação.

Nessa linha, o Supremo Tribunal Federal, ao apreciar caso envolvendo a análise dos últimos registros telefônicos em aparelhos celulares apreendidos após a prisão em flagrante de

---

[14] BRASIL, op. cit., nota 12.
[15] FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista Da Faculdade De Direito*, Universidade De São Paulo, v. 88, 1 jan. 1993, p. 447. Disponível em: < http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. Acesso em: 10 abr. 2020.
[16] CABETTE, Eduardo Luiz Santos. *Interceptação Telefônica*. 3. ed. São Paulo: Saraiva, 2015, p.31.
[17] BRASIL, op. cit., nota 12.
[18] FERRAZ JÚNIOR, op. cit., nota 15.

determinado acusado, deixou clara a diferença de proteção conferida aos registros telefônicos e à comunicação telefônica, como se vê:

> HABEAS CORPUS. NULIDADES: (1) INÉPCIA DA DENÚNCIA; (2) ILICITUDE DA PROVA PRODUZIDA DURANTE O INQUÉRITO POLICIAL; VIOLAÇÃO DE REGISTROS TELEFÔNICOS DO CORRÉU, EXECUTOR DO CRIME, SEM AUTORIZAÇÃO JUDICIAL; (3) ILICITUDE DA PROVA DAS INTERCEPTAÇÕES TELEFÔNICAS DE CONVERSAS DOS ACUSADOS COM ADVOGADOS, PORQUANTO ESSAS GRAVAÇÕES OFENDERIAM O DISPOSTO NO ART. 7º, II, DA LEI 8.906/96, QUE GARANTE O SIGILO DESSAS CONVERSAS. VÍCIOS NÃO CARACTERIZADOS. ORDEM DENEGADA. [...] 2. Ilicitude da prova produzida durante o inquérito policial - violação de registros telefônicos de corréu, executor do crime, sem autorização judicial. 2.1 Suposta ilegalidade decorrente do fato de os policiais, após a prisão em flagrante do corréu, terem realizado a análise dos últimos registros telefônicos dos dois aparelhos celulares apreendidos. Não ocorrência. 2.2 Não se confundem comunicação telefônica e registros telefônicos, que recebem, 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 dos dados. 2.3 Art. 6º do CPP: dever da autoridade policial de proceder à coleta do material comprobatório da prática da infração penal. Ao proceder à pesquisa na agenda eletrônica dos aparelhos devidamente apreendidos, meio material indireto de prova, a autoridade policial, cumprindo o seu mister, buscou, unicamente, colher elementos de informação hábeis a esclarecer a autoria e a materialidade do delito (dessa análise logrou encontrar ligações entre o executor do homicídio e o ora paciente). Verificação que permitiu a orientação inicial da linha investigatória a ser adotada, bem como possibilitou concluir que os aparelhos seriam relevantes para a investigação. 2.4 À guisa de mera argumentação, mesmo que se pudesse reputar a prova produzida como ilícita e as demais, ilícitas por derivação, nos termos da teoria dos frutos da árvore venenosa (*fruit of the poisonous tree*), é certo que, ainda assim, melhor sorte não assistiria à defesa. É que, na hipótese, não há que se falar em prova ilícita por derivação. Nos termos da teoria da descoberta inevitável, construída pela Suprema Corte norte-americana no caso Nix x Williams (1984), o curso normal das investigações conduziria a elementos informativos que vinculariam os pacientes ao fato investigado. Bases desse entendimento que parecem ter encontrado guarida no ordenamento jurídico pátrio com o advento da Lei 11.690/2008, que deu nova redação ao art. 157 do CPP, em especial o seu § 2º. [...] (HC 91867, Relator(a): Min. GILMAR MENDES, Segunda Turma, julgado em 24/04/2012, ACÓRDÃO ELETRÔNICO DJe-185 DIVULG 19-09-2012 PUBLIC 20-09-2012)[19]

Ademais, a Suprema Corte possui precedente no qual assentou que a proteção a que se refere o art. 5º, XII, da Constituição Federal[20] assegura a inviolabilidade da comunicação de dados, mas não dos dados em si mesmos, ainda quando armazenados em computador, devendo o mesmo entendimento ser adotado quando se tratar de dados armazenados em aparelhos celulares. Nesse sentido:

---

[19] BRASIL. Supremo Tribunal Federal. *HC nº 91867*. Relator: Ministro Gilmar Mendes. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%2891867%29&base=baseAcordaos&url=http://tinyurl.com/y5za3tw4>. Acesso em: 19 mai. 2020.

[20] BRASIL, op. cit., nota 12.

> [...] IV - Proteção constitucional ao sigilo das comunicações de dados - art. 5º, XVII, da CF: ausência de violação, no caso. 1. Impertinência à hipótese da invocação da AP 307 (Pleno, 13.12.94, Galvão, DJU 13.10.95), em que a tese da inviolabilidade absoluta de dados de computador não pode ser tomada como consagrada pelo Colegiado, dada a interferência, naquele caso, de outra razão suficiente para a exclusão da prova questionada - o ter sido o microcomputador apreendido sem ordem judicial e a conseqüente ofensa da garantia da inviolabilidade do domicílio da empresa - este segundo fundamento bastante, sim, aceito por votação unânime, à luz do art. 5º, XI, da Lei Fundamental. 2. Na espécie, ao contrário, não se questiona que a apreensão dos computadores da empresa do recorrente se fez regularmente, na conformidade e em cumprimento de mandado judicial. 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). [...]
> (RE 418416, Relator (a): Min. SEPÚLVEDA PERTENCE, Tribunal Pleno, julgado em 10/05/2006, DJ 19-12-2006 PP-00037 EMENT VOL-02261-06 PP-01233)[21]

O postulado da reserva constitucional de jurisdição importa em submeter à esfera única de decisão dos magistrados a prática de determinados atos cuja realização, por efeito de explícita determinação constante da própria Constituição Federal[22], somente pode emanar do juiz, e não de terceiros, inclusive daqueles a quem se haja atribuído o exercício de poderes de investigação.

O texto constitucional definiu, assim, quais direitos estarão sob a exigência de uma reserva absoluta e quais sob uma reserva relativa. Tal distinção é de suma importância para se traçar os limites ou em que situações qual órgão será detentor da primeira palavra, sendo certo que ao Judiciário caberá sempre a última palavra, não importando de quem for a primeira.

Dessa forma, exigir-se prévia autorização judicial para a obtenção de dados encontrados em aparelhos celulares apreendidos é seguir conforme uma tendência contemporânea de parte da doutrina e jurisprudência no sentido da absolutização da reserva jurisdicional, o que não se adequa ao contexto atual da criminalidade e da importância da obtenção de dados e registros para uma investigação policial efetiva.

O alargamento de uma pretensa "proteção", em âmbitos em que a própria Lei Maior sequer o fez, não se sustenta, diante da relatividade dos direitos fundamentais, que não se revestem de caráter absoluto e estão sujeitos à ponderação no caso concreto. Ademais, conforme exaustivamente examinado, a cláusula de inviolabilidade das comunicações abrange tão somente o ato comunicativo instantâneo, não os dados em si mesmos.

---

[21] BRASIL. Supremo Tribunal Federal. *RE nº 418416*. Relator: Ministro Sepúlveda Pertence. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%28418416%29&pagina=4&base=baseAcordaos&url=http://tinyurl.com/yxvookw2>. Acesso em: 19 mai. 2020.

[22] BRASIL, op. cit., nota 12.

Destarte, a partir do dever da Autoridade Policial em colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias, conforme a previsão do art. 6º do Código de Processo Penal[23], complementada pelo art. 2º, §2º da Lei nº 12.830/2013[24], a verificação de registros e dados gravados em aparelho celular apreendido não configura qualquer prejuízo ao direito fundamental do sigilo das comunicações telefônicas, mas simples acesso a dados contidos em objeto apreendido na cena do crime.

Nesse caso, cumpre observar que deverá a Autoridade Policial responsável desabilitar a conexão do celular à Internet e à operadora de telefonia, limitando-se assim a consultar a troca de mensagens pretéritas e demais dados armazenados no aparelho, o que evitará a interceptação de qualquer comunicação em tempo real, com a consequente nulidade das provas obtidas em virtude da cláusula de reserva de jurisdição imposta pela ordem constitucional.

Destaca-se, por fim, que a situação acima examinada está sendo discutida pelo Supremo Tribunal Federal no bojo do Recurso Extraordinário com Agravo (ARE) 1.042.075[25], da relatoria do ministro Dias Toffoli, com repercussão geral já reconhecida, quando então será pacificada a questão no país e se verificará se a tendência da absolutização da reserva jurisdicional ganhará ou não fôlego.

3. A NOVA LEI DO ABUSO DE AUTORIDADE E A POSSÍVEL CARACTERIZAÇÃO DE CRIME DIANTE DA QUEBRA DO SIGILO DOS DADOS SEM AUTORIZAÇÃO JUDICIAL: MAIS UM ASPECTO A SER ENFRENTADO

No dia 03 de janeiro de 2020 entrou em vigor no ordenamento jurídico brasileiro a nova Lei do Abuso de Autoridade – Lei nº 13.869/2019[26], em substituição à Lei nº 4.898/65[27], editada na época da ditadura militar e que, até a nova Lei vigorar, regulou a figura do abuso de autoridade no país.

Nessa linha, é extremamente relevante destacar, de prontidão, que os tipos penais da Lei nº 4.898/65[28] eram muito mais abertos em relação aos da nova Lei, marcada pela

[23] BRASIL, op. cit., nota 2.
[24] BRASIL. *Lei nº 12.830*, de 20 de junho de 2013. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12830.htm>. Acesso em: 02 set. 2019.
[25] BRASIL. Supremo Tribunal Federal. *ARE nº 1042075*. Relator: Ministro Dias Toffoli. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5173898>. Acesso em: 19 mai. 2020.
[26] BRASIL. *Lei nº 13.869*, de 05 de setembro de 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13869.htm>. Acesso em: 10 abr. 2020.
[27] BRASIL. *Lei nº 4.898*, de 09 de dezembro de 1965. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l4898.htm>. Acesso em: 02 set. 2019.
[28] BRASIL, op. cit., nota 26.

taxatividade das condutas descritas. Ademais, cumpre o destaque de que todos os tipos penais configuradores de crime de abuso de autoridade na Lei nº 13.869/19[29] exigem, além do dolo, a especial finalidade do agente público de "prejudicar outrem ou beneficiar a si mesmo ou a terceiro, ou, ainda, por mero capricho ou satisfação pessoal", nos termos do seu art. 1º, §1º.

Assim, no que se refere ao acesso pela Autoridade Policial a dados e registros de aparelhos celulares apreendidos sem autorização judicial, enquanto não há pacificidade jurisprudencial sobre a licitude de tal conduta, pode-se ver configurado, em algumas hipóteses, o tipo penal descrito no art. 13, III, da Lei nº 13.869/19[30].

Nos termos do supracitado dispositivo, configura abuso de autoridade constranger o preso ou o detento, mediante violência, grave ameaça ou redução de sua capacidade de resistência, a produzir prova contra si mesmo ou contra terceiro. Dessa forma, uma hipótese de caracterização do crime de abuso de autoridade descrito no art. 13, III, da nova Lei, seria o caso de desbloqueio do aparelho celular apreendido somente com o constrangimento ilegal realizado por um agente público.

Em um cenário tecnológico em que os aparelhos celulares possibilitam ao usuário a introdução de senha para proteger o acesso às suas informações, ou até mesmo recursos mais modernos como o reconhecimento biométrico, seja facial ou das impressões digitais, são raros os casos em que aparelhos celulares apreendidos não possuem restrição de acesso via tais mecanismos de segurança e proteção. Destarte, o imediato acesso dos dados pelo agente público, na grande maioria dos casos, somente seria possível com a participação do investigado, através do fornecimento da senha ou consentindo com o reconhecimento biométrico.

O direito ao silêncio, previsto no art. 5º, LXIII, da Constituição Federal[31], e reproduzido no art. 186 do Código de Processo Penal[32], é tradução de uma das manifestações da não autoincriminação e do princípio do *nemo tenetur se detegere* (ninguém é obrigado a se descobrir). Em relação a este princípio, destaca-se a lição de Maria Elizabeth Queijo[33]:

> Nessa ótica, o princípio *nemo tenetur se detegere*, como direito fundamental, objetiva proteger o indivíduo contra excessos cometidos pelo Estado, na persecução penal, incluindo-se nele o resguardo contra violências físicas e morais, empregadas para compelir o indivíduo a cooperar na investigação e apuração de delitos, bem como contra métodos proibidos de interrogatório, sugestões e dissimulações.

[29] BRASIL, op. cit., nota 25.
[30] BRASIL, op. cit., nota 25.
[31] BRASIL, op. cit., nota 12.
[32] BRASIL, op. cit., nota 2.
[33] QUEIJO, Maria Elizabeth. *O direito de não produzir prova contra si mesmo:* o princípio nemo tenetur se detegere e suas decorrências no processo penal. São Paulo: Saraiva, 2003, p. 54-55.

Com efeito, o princípio do *nemo tenetur se detegere* possui imensurável validade no âmbito processo penal brasileiro, constituindo garantia constitucional indispensável para o respeito ao devido processo legal, à presunção de inocência e à ampla defesa. Dessa forma, evidentemente o art. 13, III, da Lei nº 13.869/19[34] foi editado em privilégio a este princípio e visando a proteção da garantia da não autoincriminação.

Ressalta-se, contudo, que a garantia da não autoincriminação não constitui qualquer direito subjetivo a não produzir prova contra si mesmo. O que existe, em regra, é a proibição de a pessoa ser compelida, contra a sua vontade, a realizar exames previstos em lei, tal como soprar o bafômetro e escrever de próprio punho para comparações grafotécnicas, mas há que se fazer a devida diferenciação entre espécies de colaboração do investigado. Nesse sentido, Renato Brasileiro de Lima[35] ensina que:

> [...] o acusado tem o direito de não colaborar na produção da prova sempre que se lhe exigir um *comportamento ativo*, um *facere*. Portanto, em relação às provas que demandam apenas que o acusado *tolere* a sua realização, ou seja, aquelas que exijam uma cooperação meramente passiva, não se há falar em violação ao *nemo tenetur se detegere*. O direito de não produzir prova contra si mesmo não persiste, portanto, quando o acusado for mero objeto de verificação.

A partir desta diferenciação, apresenta-se a seguinte situação hipotética: o aparelho celular apreendido pode ser desbloqueado mediante reconhecimento facial e, para fazê-lo, o agente público aponta seu sensor, sem utilizar de violência, grave ameaça ou meio de redução da capacidade de resistência, para o rosto do investigado, acessando seus dados. Seria esta uma hipótese de cooperação passiva em que não se viola o princípio do *nemo tenetur se detegere* e em que não se configura crime de abuso de autoridade? Não parece razoável tal flexibilização, sendo certo que não houve, nessa hipótese, manifestação expressa de colaboração ou consentimento, ultrapassando o limite da tolerância que deve dar o investigado.

Assim, certo é que caso o aparelho celular apreendido para ser acessado, sem autorização judicial, requeira a introdução de senha ou o reconhecimento biométrico, somente com a colaboração ativa, voluntária e expressa do investigado será possível. O constrangimento, mediante violência, grave ameaça ou meio de redução da capacidade de resistência, por parte dos agentes públicos responsáveis, com o objetivo de acessar os dados constantes no aparelho celular, caracterizará crime de abuso de autoridade, nos termos do art. 13, III, da Lei nº 13.869/19[36], desde que devidamente provado o elemento subjetivo exigido no §1º do art. 1º.

---

[34] BRASIL, op. cit., nota 25.
[35] LIMA, Renato Brasileiro de. *Manual de Processo Penal.* 4. ed. Salvador: JusPODIVM, 2016, p. 98.
[36] BRASIL, op. cit., nota 25.

Portanto, com a entrada em vigor da nova legislação que trata do abuso de autoridade, tem-se a importância da autorização pelo investigado para que sejam acessados os dados em seu aparelho celular apreendido e protegido por senha, sob pena de se ver potencialmente caracterizado crime punível com detenção de 1 (um) a 4 (quatro) anos, e multa, sem prejuízo da pena cominada à violência. Destaca-se, ainda, que tal autorização, quando obtida, deve ser presumida lícita e alcançada de forma livre, visto que não o fazer é inverter a presunção da legitimidade e veracidade dos atos policiais, imantados com tais efeitos de licitude.

Por fim, cumpre o destaque de que, caso o investigado forneça a senha para desbloqueio do celular ou consinta com seu reconhecimento biométrico para acesso, configurando autorização expressa e inequívoca que se recomenda reduzir a termo, não prosperará, no âmbito de uma eventual ação penal, o pleito de nulidade destas provas obtidas, haja vista a abdicação da sua intimidade quando da autorização.

CONCLUSÃO

Com o desenvolvimento tecnológico e todas as transformações sociais dele decorrentes, os aparelhos celulares promoveram uma importante alteração na dinâmica da criminalidade. Essa nova realidade implicou não só no surgimento de novas modalidades de crimes, mas também em um novo cenário de estruturação de organizações criminosas, utilizando-se do encurtamento de distâncias possibilitado pela tecnologia.

Com efeito, acrescentou-se neste cenário a possibilidade de acesso remoto e formatação do aparelho à distância, o que tornou a quebra do sigilo de dados de um aparelho celular apreendido sem prévia autorização judicial um dos temas mais polêmicos na doutrina e jurisprudência envolvendo o conflito entre a violação da privacidade e a garantia da segurança pública. Nessa linha, o sigilo das comunicações telefônicas, que recebem a especial proteção do art. 5º, XII, da Constituição Federal, sendo cobertos pela reserva jurisdicional, foi utilizado pelo Superior Tribunal de Justiça para conferir a mesma proteção aos dados telefônicos.

Todavia, os dados telefônicos constituem registros e informações contidos na memória de aparelho de telefone celular, pelo que a quebra do sigilo não constitui intervenção de um terceiro num ato de comunicação para se obter esta prova, nos moldes do que ocorre na interceptação. A comunicação telefônica, caso não interceptada, perder-se-ia, por ser instantânea e não ser gravada, ao passo que os dados telefônicos já estão documentados e gravados na memória do dispositivo, destacando-se que ainda, no caso dos aplicativos de

mensagens, as conversas são protegidas por criptografia, o que não ocorre nas comunicações telefônicas.

A Constituição Federal, portanto, assegura a inviolabilidade da comunicação de dados enquanto fluxo comunicativo, mas não dos dados em si mesmos, pelo que a equiparação feita pelo Superior Tribunal de Justiça entre comunicação telefônica e dados telefônicos, a fim de justificar a ilicitude da prova em tela obtida sem prévia autorização judicial, não se revela, com a devida vênia, tecnicamente adequada. Com a palavra final, diante da repercussão geral reconhecida ao tema, caberá ao Supremo Tribunal Federal, no julgamento do ARE nº 1.042.075, pacificar a questão.

Dessa forma, o posicionamento adotado neste trabalho foi o de, através de um juízo de ponderação, pautado no princípio da proporcionalidade, não se tolerar que organizações criminosas utilizem do manto protetor dos direitos fundamentais e da tendência contemporânea de absolutização da reserva jurisdicional, para justificar a prática de crimes. Destarte, exigir-se autorização judicial prévia para se quebrar o sigilo e ter acesso aos dados telefônicos é medida extremamente burocratizada, em descompasso com a legislação e, sobretudo, desproporcional diante da realidade da criminalidade no país.

Contudo, destaca-se que, caso o aparelho celular apreendido para ser acessado, sem a autorização judicial específica, requeira a introdução de senha ou reconhecimento biométrico, somente na hipótese de o investigado colaborar ativa, voluntária e expressamente, o desbloqueio e o consequente acesso aos dados ocorrerá sem o potencial cometimento, por parte do agente público responsável, do crime de abuso de autoridade previsto no art. 13, III, da Lei nº 13.869/19.

Assim, não bastasse a discussão doutrinária e jurisprudencial acerca da equiparação entre os institutos, da ponderação a ser feita diante do conflito apontado, bem como as diversas nuances tecnológicas que enriquecem o tema, com a entrada em vigor da nova Lei do Abuso de Autoridade - Lei nº 13.869/2019, deverá a Autoridade Policial se atentar para mais um aspecto problematizador que poderá potencialmente se ver configurado.

REFERÊNCIAS

APPLE. *Find my iPhone:* Apagar seu dispositivo. Disponível em: <https://support.apple.com/kb/PH19300?locale=pt_BR#:~:text=Se%20ele%20estiver%20off%2Dline,senha%20de%20seu%20ID%20Apple>. Acesso em: 10 abr. 2020.

BRASIL. *Código de Processo Penal*. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm>. Acesso em: 02 set. 2019.

_____. *Constituição da República Federativa do Brasil*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constitui%C3%A7ao.htm>. Acesso em: 02 set. 2019.

_____. *Lei nº 4.898*, de 09 de dezembro de 1965. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l4898.htm>. Acesso em: 02 set. 2019.

_____. *Lei nº 9.296*, de 24 de julho de 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em: 02 set. 2019.

_____. *Lei nº 12.830*, de 20 de junho de 2013. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Lei/L12830.htm>. Acesso em: 02 set. 2019.

_____. *Lei nº 13.344*, de 06 de outubro de 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13344.htm>. Acesso em: 02 set. 2019.

_____. *Lei nº 13.869*, de 05 de setembro de 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13869.htm>. Acesso em: 10 abr. 2020.

_____. Superior Tribunal de Justiça. *Informativo de Jurisprudência nº 583*. Disponível em: <https://scon.stj.jus.br/SCON/SearchBRS?b=INFJ&tipo=informativo&livre=@COD=%270583%27>. Acesso em: 19 mai. 2020.

_____. Superior Tribunal de Justiça. *Informativo de Jurisprudência nº 593*. Disponível em: <https://scon.stj.jus.br/docs_internet/informativos/PDF/Inf0593.pdf>. Acesso em: 19 mai. 2020.

_____. Supremo Tribunal Federal. *RE nº 418416*. Relator: Ministro Sepúlveda Pertence. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%28418416%29&pagina=4&base=baseAcordaos&url=http://tinyurl.com/yxvookw2>. Acesso em: 19 mai. 2020.

_____. Supremo Tribunal Federal. *HC nº 91867*. Relator: Ministro Gilmar Mendes. Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=%2891867%29&base=baseAcordaos&url=http://tinyurl.com/y5za3tw4>. Acesso em: 19 mai. 2020.

_____. Supremo Tribunal Federal. *ARE nº 1042075*. Relator: Ministro Dias Toffoli. Disponível em: <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5173898>. Acesso em: 19 mai. 2020.

CABETTE, Eduardo Luiz Santos. *Interceptação Telefônica*. 3. ed. São Paulo: Saraiva, 2015.

FERRAZ JÚNIOR, T. S. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista Da Faculdade De Direito*, Universidade De São Paulo, v. 88, 1 jan. 1993, p. 439-456. Disponível em: < http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. Acesso em: 10 abr. 2020.

_____. *Sigilo de dados:* o direito à privacidade e os limites à função fiscalizadora do Estado. Disponível em: <http://www.terciosampaioferrazjr.com.br/?q=/publicacoes-cientificas/28>. Acesso em: 10 abr. 2020.

GOOGLE. *Localize, bloqueie ou apague um dispositivo Android perdido*. Disponível em: <https://support.google.com/nexus/answer/6160491?hl=pt>. Acesso em: 10 abr. 2020.

JUSTINO, Anderson. *Estelionato via WhatsApp cresce 19% no Rio.* Disponível em: <https://odia.ig.com.br/rio-de-janeiro/2020/01/5856704-estelionato-via-whatsapp-cresce-19--no-rio.html>. Acesso em: 10 abr. 2020.

LIMA, Renato Brasileiro de. *Manual de Processo Penal.* 4. ed. Salvador: JusPODIVM, 2016.

MICROSOFT. *Realizar uma limpeza remota em um telefone móvel.* Disponível em: <https://docs.microsoft.com/pt-br/exchange/clients/exchange-activesync/remote-wipe?view=exchserver-2019>. Acesso em: 10 abr. 2020.

QUEIJO, Maria Elizabeth. *O direito de não produzir prova contra si mesmo:* o princípio *nemo tenetur se detegere* e suas decorrências no processo penal. São Paulo: Saraiva, 2003.