ESCOLA DA MAGISTRATURA DO ESTADO DO RIO DE JANEIRO

A VIOLAÇÃO DE DADOS DE *SMARTPHONES* NA PRISÃO EM FLAGRANTE: UMA ANÁLISE SOBRE A CONSTITUCIONALIDADE DAS PROVAS OBTIDAS

Maria Fernanda Costa Pinto Cabral de Oliveira e Souza

Rio de Janeiro
2019

MARIA FERNANDA COSTA PINTO CABRAL DE OLIVEIRA E SOUZA

A VIOLAÇÃO DE DADOS DE *SMARTPHONES* NA PRISÃO EM FLAGRANTE: UMA ANÁLISE SOBRE A CONSTITUCIONALIDADE DAS PROVAS OBTIDAS

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
Néli L. C. Fetzner
Nelson C. Tavares Junior

Rio de Janeiro
2019

A VIOLAÇÃO DE DADOS DE *SMARTPHONES* NA PRISÃO EM FLAGRANTE: UMA ANÁLISE SOBRE A CONSTITUCIONALIDADE DAS PROVAS OBTIDAS

Maria Fernanda Costa Pinto Cabral de Oliveira e Souza

Graduada pela Fundação Getúlio Vargas – FGV Direito Rio. Advogada.

Resumo – com o avanço tecnológico e a popularização dos meios de comunicação, os *smartphones* viraram uma realidade mundial. A cada ano que passa esses aparelhos armazenam mais informações sobre seus donos, tais como fotos, vídeos, conversas, áudios, e-mails e mais uma infinidade de dados. Explorar o celular de uma pessoa pode ser mais íntimo do que investigar a sua própria casa. Essa nova realidade fática impõe que o Direito repense alguns conceitos clássicos e certos procedimentos, pois, nesse caso, não se adaptar implica deixar de investigar ou deixar de punir. O objetivo do trabalho é discutir a licitude das provas obtidas por meio do acesso a dados dos *smartphones* dos presos em flagrante sem autorização judicial, analisando o conceito de interceptação telefônica trazido pela Lei nº 9.296/96.

Palavras-chave – Direito Processual Penal. Provas no processo penal. Lei de Interceptações Telefônicas.

Sumário – Introdução. 1. A vedação às provas ilícitas no Direito Processual Brasileiro e o acesso de dados de aparelho celular na prisão em flagrante. 2. A Lei nº 9.296/96 e a abrangência do conceito de interceptação telefônica. 3. A posição dos Tribunais Superiores acerca do acesso aos dados obtidos no aparelho celular do preso em flagrante sem prévia autorização judicial. Conclusão. Referências.

INTRODUÇÃO

O presente artigo científico discute a possibilidade de acesso aos dados armazenados no *smartphone* do agente no momento da prisão em flagrante, tais como ao conteúdo de aplicativos de mensagens, como o *WhatsApp*, e a necessidade, ou não, de autorização judicial para que as eventuais provas extraídas sejam consideradas lícitas.

Para tanto, serão abordados os entendimentos doutrinários e jurisprudenciais acerca do tema, de modo a discutir direitos fundamentais previstos na Constituição Federal de 1988, tais como a proteção à vida privada, à intimidade e o sigilo das comunicações telefônicas.

É inegável que, nos tempos modernos, os *smartphones* são uma realidade para os brasileiros. Com a facilidade de comprá-los, a redução de seus custos, somada à popularização da *Internet*, é difícil encontrar alguém, hoje, que não tenha um para chamar de seu.

O fato é que esses aparelhos armazenam uma gama enorme de informações. Explorar o celular de uma pessoa pode ser mais íntimo do que investigar a sua própria casa, tendo em vista que ele contém fotos, vídeos, conversas, áudios, e-mails e mais uma infinidade de dados pessoais e profissionais de seus donos.

As principais questões que suscitam debate são: os dados provenientes de aplicativos de mensagem, como o *WhatsApp*, encaixam-se no objeto de proteção da Lei nº 9.296/96, que trata da interceptação telefônica regulamentando o art. 5º, XII, da Carta Magna? Há necessidade de autorização judicial para acessá-los? Qual o limite de atuação das autoridades policiais no momento da prisão em flagrante, considerando que o próprio Código de Processo Penal determina que se apreenda todos os objetos que tenham relação com o fato criminoso?

O tema gera acaloradas discussões entre os órgãos de acusação e de defesa e merece atenção, uma vez que envolve a produção e a valoração de provas no processo penal, assunto de grande relevância prática, a serem analisadas à luz de direitos e garantias fundamentais, cuja importância no Estado Democrático de Direito é indiscutível.

O primeiro capítulo aborda aspectos da produção probatória no processo penal brasileiro, bem como o que torna uma prova lícita ou ilícita à luz das disposições constitucionais. O objetivo, aqui, é iniciar o debate se as provas obtidas por meio do acesso aos dados telefônicos do acusado, sem autorização judicial, encaixam-se no conceito de prova lícita ou não.

Em seguida, o segundo capítulo tratará sobre a Lei nº 9.296/96, a Lei das Interceptações Telefônicas, com a finalidade de questionar se a análise dos dados provenientes de aplicativos de mensagens sem autorização judicial fere o sigilo das comunicações telefônicas.

E, por fim, o terceiro capítulo versará sobre os entendimentos atuais das Cortes Superiores sobre o tema, com o objetivo de discutir as implicações práticas de se defender uma ou outra posição, qual seja, pela necessidade ou não de autorização judicial para que as mencionadas provas sejam consideradas lícitas.

A abordagem da pesquisa será, necessariamente, qualitativa, de modo que a pesquisadora pretende utilizar a referência bibliográfica para sustentar sua tese.

1. A VEDAÇÃO ÀS PROVAS ILÍCITAS NO DIREITO PROCESSUAL BRASILEIRO E O ACESSO DE DADOS DE APARELHO CELULAR NA PRISÃO EM FLAGRANTE

Quando o assunto é a produção de provas no processo penal, trata-se de tema quase que sem fim, complexo e que envolve inúmeros conceitos e discussões do ponto de vista teórico e também prático.

O presente capítulo tem o objetivo de apresentar o conceito fornecido pela melhor doutrina acerca da licitude e da ilicitude da prova, bem como introduzir a discussão se as provas obtidas por meio do acesso aos dados telefônicos do acusado, sem autorização judicial, enquadram-se no conceito de prova lícita ou não.

Segundo Eugênio Pacelli, "a prova judiciária tem um objetivo claramente definido: a reconstrução dos fatos investigados no processo, buscando a maior coincidência possível com a realidade histórica [...]" [1]. Trata-se de incumbência difícil, quando não impossível: a reconstrução da verdade.

É importante esclarecer, contudo, que o processo penal visa à produção de uma verdade processual, ou seja, de uma certeza jurídica que é assumidamente imperfeita e falha em alguns casos. Em outras palavras, a verdade processual pode corresponder à verdade dos fatos ou não.

Para alcançar a construção dessa verdade processual, diversos meios de prova estão disponíveis no ordenamento jurídico pátrio, ao qual se aplica o princípio da liberdade da prova.

Nas lições de Paulo Rangel[2]:

> O princípio da liberdade da prova é um consectário lógico do princípio da verdade processual, ou seja, se o juiz deve buscar sempre a verdade dos fatos que lhe são apresentados, óbvio nos parece que tem toda a liberdade de agir, com o fim de reconstruir o fato praticado e aplicar a ele a norma jurídica que for cabível.

O aludido princípio, todavia, não é ilimitado. A liberdade da produção probatória não é absoluta, esbarrando em limites de ordem material e processual.

---

[1]OLIVEIRA, Eugênio Pacelli de. *Curso de Processo Penal*. 18. ed. São Paulo: Atlas, 2014, p. 327.
[2]RANGEL, Paulo. *Direito Processual Penal*. 22. ed. São Paulo: Atlas, 2014, p. 468.

Uma das limitações impostas à liberdade probatória, talvez a mais importante de todas, encontra-se prevista no art. 5º, LVI, da Constituição da República Federativa do Brasil de 1988 (CRFB/88) [3], que, em nome da tutela dos direitos e garantias individuais do acusado, proíbe expressamente a utilização de provas obtidas por meio ilícito.

Disposição semelhante foi inserida também no Código de Processo Penal[4] (CPP) por meio da Lei nº 11.690/08:

> Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais. (Redação dada pela Lei nº 11.690, de 2008)
> § 1º São também inadmissíveis as provas derivadas das ilícitas, salvo quando não evidenciado o nexo de causalidade entre umas e outras, ou quando as derivadas puderem ser obtidas por uma fonte independente das primeiras. (Incluído pela Lei nº 11.690, de 2008)
> § 2º Considera-se fonte independente aquela que por si só, seguindo os trâmites típicos e de praxe, próprios da investigação ou instrução criminal, seria capaz de conduzir ao fato objeto da prova. (Incluído pela Lei nº 11.690, de 2008)
> § 3º Preclusa a decisão de desentranhamento da prova declarada inadmissível, esta será inutilizada por decisão judicial, facultado às partes acompanhar o incidente. (Incluído pela Lei nº 11.690, de 2008)
> § 4º (VETADO) (Incluído pela Lei nº 11.690, de 2008)

A inadmissibilidade das provas ilícitas é uma decorrência lógica do Estado Democrático de Direito. Como bem salienta Paulo Rangel, "no Estado Democrático de Direito, os fins não justificam os meios" [5].

Essa norma tem como finalidade precípua a tutela de direitos e garantias fundamentais caros ao sistema jurídico brasileiro, tais como o direito à vida privada, à intimidade e ao sigilo das comunicações, além de proteger a própria qualidade do material probatório produzido.

Não se pode deixar de frisar, também, que tal limitação é revestida de um caráter quase que pedagógico, uma vez que veda e desestimula a utilização de meios arbitrários para a obtenção de uma prova. Isso porque a consequência do reconhecimento da ilicitude da prova é o seu desentranhamento dos autos, ou seja, a sua retirada obrigatória.

Em suma, a prova é um direito subjetivo do acusado e, como tal, goza de extensa liberdade de produção. Porém, em observância aos direitos fundamentais previstos na

---

[3]BRASIL. *Constituição da República Federativa do Brasil*, de 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 27 fev. 2019.
[4]BRASIL. *Decreto-Lei nº 3.689, de 3 de outubro de 1941*. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 27 fev. 2019.
[5] RANGEL, op. cit., p. 473.

Carta Magna de 1988, somente se admite, no processo penal, as provas colhidas de forma lícita.

Dito isso, é oportuno destacar, ainda no art. 5º, da CRFB/88, o inciso XII[6], que assim dispõe:

> Art. 5º, 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;

A pergunta que se faz, portanto, é: o acesso às provas contidas em aparelho *smartphone*, tais como conversas em aplicativos de mensagem como o *WhatsApp* e o *Telegram*, fotos, histórico de chamadas, dentre outros, no momento da prisão em flagrante, sem autorização judicial, é lícito?

O tema é polêmico e levanta debates calorosos de ambos os lados.

Para Norberto Avena[7], essas provas são lícitas, uma vez que não se trata de dados em procedimento de transmissão ou recepção, mas sim de dados já produzidos e armazenados. Portanto, não se encaixam na hipótese do art. 5º, XII, da CRFB/88[8], dispensando a exigência da autorização judicial.

Defendendo, ainda, a licitude de tais provas, seria possível argumentar que a autoridade policial que recolhe e acessa os dados já armazenados nesses aparelhos apenas observa o mandamento do próprio CPP, que, no art. 6º[9], determina que se apreendam os objetos que tiverem relação com o fato e que se colham as provas que servem para o esclarecimento do fato e suas circunstâncias.

Em contrapartida, a tese sustentada pela defesa do acusado, geralmente, é no sentido da ilicitude de tais provas, uma vez que essa devassa à sua privacidade sem a respectiva autorização judicial viola frontalmente a Constituição Federal e seus direitos e garantias individuais.

Os próximos capítulos abordarão outros aspectos relevantes para a solução da controvérsia, bem como a posição dos Tribunais sobre o tema.

---

[6]BRASIL, op. cit., nota 3.
[7] AVENA, Norberto. *Processo Penal*. 10. ed. Rio de Janeiro: Forense, São Paulo: MÉTODO, 2018, p. 580.
[8]BRASIL, op. cit., nota 3.
[9]BRASIL, op. cit., nota 4.

2. A LEI Nº 9.296/96 E A ABRANGÊNCIA DO CONCEITO DE INTERCEPTAÇÃO TELEFÔNICA

A sociedade contemporânea tem vivido uma constante evolução da tecnologia e a forma de comunicar-se sofreu grande modificação. Hoje, além da comunicação telefônica, é possível trocar *e-mails*, gravar áudios, enviar mensagens de texto ou por meio de aplicativos gratuitos conectados à *Internet*.

A verdade é que o sistema jurídico precisa se modernizar e se adaptar a essa nova realidade, pois essas inovações constituem novas modalidades de prova no processo penal, diferentes das tradicionais, já previstas na legislação processual penal, como é o caso da prova testemunhal, da prova documental, etc.

O presente capítulo tem o objetivo de apresentar a sistemática trazida pela Lei nº 9.296/96[10], Lei de Interceptações Telefônicas, que regulamenta o art. 5º, XII, da CRFB/88[11], mostrando como seria possível, do ponto de vista legal, o acesso a essas novas formas de comunicação e a esses dados armazenados.

Além disso, há, também, o objetivo de suscitar o seguinte debate: o acesso, e a posterior análise, dos dados contidos nos *smartphones* dos presos em flagrante, enquadram-se no conceito de interceptação telefônica? E, a depender da primeira resposta, surge ainda um segundo questionamento: esse acesso somente poderá ser feito por meio de autorização judicial?

Vale lembrar que o *smartphone*, além de possibilitar inúmeras novas formas de comunicação, também armazena importantes informações sobre a vida e as práticas dos indivíduos. Tal fato reflete no fenômeno criminal, o que torna esses aparelhos grandes aliados das autoridades policiais na investigação e elucidação de infrações penais. Ademais, a título de exemplo, o aplicativo *WhatsApp*, criado em 2009, é um dos mais populares do mundo e o Brasil é o segundo país com mais usuários do aplicativo no *ranking* mundial[12]. Esses dados não podem ser ignorados.

---

[10]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: 14 fev. 2019.

[11]BRASIL, op. cit., nota 3.

[12]PEREIRA, Murilo Cézar Antonini. Acesso aos dados armazenados no WhatsApp pela polícia durante investigação criminal: implicações nos direitos fundamentais. *Revista Jus Navigandi*, Teresina, ano 23, n. 5535, 27 ago. 2018. Disponível em: <https://jus.com.br/artigos/68482>. Acesso em: 14 fev. 2019.

Contudo, como chama atenção Luiz Flávio Gomes, citando Montesquieu, o exercício do poder e o seu excesso/desvio caminham lado a lado[13]. Vivemos em um Estado Democrático de Direito e, como tal, ainda que seja indispensável facilitar o andamento das investigações criminais, é preciso observar certas "regras do jogo". A liberdade, a vida privada e a intimidade dos cidadãos são valores muito caros nas democracias atuais.

Antes, contudo, de adentrar nas questões acima mencionadas, é preciso trabalhar conceitos importantes relacionados à interceptação telefônica e sua abrangência, por meio do estudo da aludida Lei nº 9.296/96[14].

Primeiramente, é fundamental destacar que a interceptação telefônica *lato sensu* é gênero, do qual são espécies a escuta telefônica, a gravação telefônica e a interceptação telefônica *stricto sensu.*

A escuta telefônica envolve um terceiro que acessa a conversa telefônica entre duas pessoas, sendo que um desses interlocutores tem conhecimento que os diálogos estão sendo captados. Para a sua licitude, é indispensável a autorização judicial.

Já a gravação telefônica não conta com a figura de um terceiro, uma vez que a conversa é registrada por um de seus interlocutores. Essa situação não configura propriamente uma interceptação, razão pela qual a jurisprudência dos Tribunais Superiores entende ser dispensável a autorização judicial nesses casos.

Todavia, o presente artigo trabalhará apenas com a interceptação telefônica *stricto sensu*, a qual envolve a figura de um terceiro acessando a comunicação entre duas ou mais pessoas sem que elas tenham conhecimento dessa violação. Por óbvio, tal mecanismo exige autorização judicial, sob pena de caracterizar prova ilícita e fazer incidir o tipo penal previsto no art. 10 da referida lei de interceptações telefônicas[15].

Por meio da leitura dos artigos 1º e 2º da Lei nº 9.296/96[16] é possível extrair os requisitos legais para a realização da interceptação telefônica. São eles: finalidade de investigação criminal ou instrução processual penal, ordem judicial fundamentada, indícios de autoria ou participação, excepcionalidade da medida (que é residual) e, por fim, que o crime investigado seja punido com pena de reclusão.

---

[13] GOMES, Luiz Flávio. *Interceptação telefônica:* comentários a Lei 9.296, de 24.07.1996. 3. ed. rev. e atual. - São Paulo: Revista dos Tribunais, 2014. p. 13.
[14]BRASIL, op. cit., nota 10.
[15]Ibidem.
[16]Ibidem.

Faz-se relevante, ainda, distinguir a quebra de sigilo de dados telefônicos da interceptação telefônica.

Os dados telefônicos são aqueles registros sobre as chamadas realizadas, tais como datas, horários, duração, número do telefone chamado, dentre outros. A quebra do sigilo desses dados não se submete à reserva de jurisdição. Em outras palavras, é possível que a autoridade policial obtenha tais dados por conta própria, o que torna a investigação mais célere.

De outro lado, a interceptação telefônica consiste no acesso à chamada telefônica, o que permite captar o conteúdo da conversa. Essa, sim, somente poderá ocorrer com autorização judicial, conforme já mencionado acima, seguindo os requisitos previstos na lei.

Dito isso, adentra-se na análise do art. 1º da Lei de Interceptações Telefônicas para delimitar a sua abrangência e aplicação. Narra o dispositivo[17]:

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
> Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

O *caput* do art. 1º vem para sanar algumas controvérsias levantadas pelo art. 5º, XII, da CRFB/88[18], uma vez que possui redação bem mais clara. É importante destacar que ele menciona a possibilidade de a interceptação recair sobre a comunicação telefônica, o que é diferente, e mais amplo, do que a conversa telefônica[19].

Antigamente, as conversas telefônicas somente envolviam a transmissão e recepção de palavras ou sons. Eram as conhecidas ligações no telefone. Nos dias atuais, as conversas telefônicas vêm sendo cada vez mais substituídas pelas comunicações telefônicas enquanto gênero, conceito que abrange não só as ligações, mas também a troca de mensagens de texto, mensagens via *Internet*, troca de áudios, de imagens e vídeos, dentre outras.

No que tange ao parágrafo único do artigo transcrito, ele dispõe sobre a interceptação de comunicações em sistema de telemática.

Por telemática entende-se, literalmente, a junção da telefonia com a informática, isso é, telemática é a forma de comunicação, geralmente pelo *smartphone*, que precisa

---

[17]BRASIL, op. cit., nota 10.
[18]BRASIL, op. cit., nota 3.
[19]GOMES, op. cit., p. 46.

da conexão com a Internet para funcionar. É nesse ponto que se incluem, por exemplo, o *WhatsApp*, o *Telegram* e o *Messenger* do *Facebook*, dentre outros.

É relevante observar que esses aplicativos, principalmente o *WhatsApp*, por ser o mais popular da categoria, na verdade, possuem uma dupla natureza jurídica: abrangem não só a telemática, caracterizada pela troca de mensagens e outros meios em tempo real, como também uma plataforma de armazenamento de dados[20], que ficam registrados no aparelho do usuário.

Em suma, para Luiz Flávio Gomes[21], a correta interpretação do dispositivo acima determina que tudo aquilo que permite a comunicação a distância é interceptável.

Vale lembrar, ainda, que o aplicativo encontra-se protegido pela criptografia total, o que significa que nem o próprio *WhatsApp* consegue acessar as conversas e registros de seus usuários em caso de determinação judicial, por exemplo.

Portanto, determinar que a autoridade policial não possa acessar o *smartphone* do preso, no momento da prisão em flagrante, implica dificultar, e muito, a análise daqueles dados no futuro, quando se obtiver a autorização judicial.

O que ocorre, na realidade, é que os sistemas penal e processual penal brasileiros como um todo, incluindo o Código Penal (1940)[22], o Código de Processo Penal (1941)[23] e a própria Lei de Interceptações Telefônicas (1996)[24], foram pensados para uma realidade diversa da que se vive hoje. Interpretar esses diplomas legislativos de forma muito restritiva deixa os criminosos da era digital fora do alcance do Estado.

É preciso destacar que o acesso aos dados contidos no s*martphone* de uma forma geral, não só em aplicativos que armazenam conversas, é diferente da interceptação em tempo real de diálogos ou ligações, essas últimas exigindo, indiscutivelmente, a autorização judicial.

A problemática envolve a famosa reflexão jurídica que permeia diversos outros temas: a necessidade de ponderação entre direitos fundamentais que, como não são absolutos, podem ceder espaço a outros a depender da análise do caso concreto. Aqui, chocam-se, de um lado, o direito à liberdade, à intimidade e à vida privada, direitos estes individuais e, de outro, o direito da coletividade à segurança pública.

---

[20]PEREIRA, op. cit..
[21]GOMES, op. cit., p. 50.
[22]BRASIL. *Decreto-lei nº 2.848*, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 06 jun. 2019.
[23]BRASIL, op. cit., nota 4.
[24]BRASIL, op. cit., nota 10.

Tal ponderação, bem como a posição dos Tribunais Superiores sobre o tema, será abordada no próximo capítulo.

3. A POSIÇÃO DOS TRIBUNAIS SUPERIORES ACERCA DO ACESSO DE DADOS OBTIDOS NO APARELHO CELULAR DO ACUSADO SEM PRÉVIA AUTORIZAÇÃO JUDICIAL

Primeiramente, é importante frisar que o tema a ser abordado a partir de agora suscita grandes discussões no universo jurídico atual. A jurisprudência de diversos países, inclusive do Brasil, voltou a debatê-lo ao reconhecer o alto grau de violação da privacidade e da intimidade do agente que tem seu aparelho eletrônico acessado e analisado pelas autoridades policiais.

O cerne da discussão, conforme mencionado anteriormente, consiste em verificar se essa devassa exige prévia autorização judicial ou não.

Há posições para todos os lados, o que acaba por trazer uma insegurança jurídica acerca da licitude (ou ilicitude) das provas obtidas quando esse acesso ocorre sem a respectiva autorização judicial.

O presente capítulo tem por objetivo, portanto, resgatar os conceitos abordados nos outros dois tópicos anteriores deste estudo para apresentar o que vem entendendo os Tribunais Estaduais e, também, os Tribunais Superiores sobre a questão, sem deixar de mencionar, ainda, as implicações práticas de se adotar uma ou outra posição.

Conforme analisado no Capítulo 2, os dados contidos no aplicativo *WhatsApp*, mencionado aqui a título de exemplo, possuem dupla natureza jurídica, uma vez que lá se encontram dados estáticos, produzidos no passado e armazenados no aparelho, mas também dados dinâmicos, ou seja, produzidos em tempo real devido à comunicação telefônica.

Em tese, o acesso aos dados estáticos não se confunde com a interceptação telefônica. Nos termos do que se analisou no Capítulo 2, interceptar é captar, em tempo real, o conteúdo de uma comunicação sem que os interlocutores tenham ciência. Considerando que, em se tratando de dados telefônicos, eles já foram gerados e agora encontram-se tão somente armazenados, não se pode falar em interceptação nesses casos.

Ocorre que a Lei nº 12.965/14[25], que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, tutela a inviolabilidade não só do fluxo das comunicações, mas também dos dados armazenados, ressalvando a hipótese de ordem judicial que autoriza a quebra. Nesse sentido:

> 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;

Pois bem. Dito isso, passa-se agora à análise de como os Tribunais Superiores vem se posicionando diante da problemática.

O Supremo Tribunal Federal possui um julgado, do final de 2012, no qual entendeu ser desnecessária a autorização judicial para o acesso aos dados dos aparelhos celulares dos acusados. Abaixo transcreve-se a Ementa do HC 91.867[26]:

> 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. [...](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)

A Suprema Corte fundamentou a decisão, de Relatoria do Ministro Gilmar Mendes, na diferenciação dos conceitos de interceptação telefônica e registro de dados telefônicos. Entendeu, à época, que comunicação telefônica e registro telefônico não se confundem e que a proteção constitucional do art. 5º, XII, da CRFB/88[27] somente abarcaria a primeira hipótese. Ademais, segundo o STF, o art. 6º, do Código de Processo Penal[28] autorizaria a autoridade policial a coletar todo o material probatório assim que tomasse ciência da prática da infração penal, o que incluiria apreender e analisar o celular do preso em flagrante.

---

[25]BRASIL. *Lei nº 12.965*, de 23 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 27 fev. 2019.
[26]BRASIL. Supremo Tribunal Federal. *HC nº 91.867*. Relator: Ministro Gilmar Mendes. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2792328Acesso em: 27 fev. 2019.
[27]BRASIL, op. cit., nota 3.
[28]BRASIL, op. cit., nota 4.

É preciso destacar, entretanto, que o aludido julgado, além de ser de 2012, analisa uma situação ocorrida no ano de 2004. Não se pode comparar a amplitude dos dados armazenados, atualmente, em *smartphones* com os dados que os aparelhos celulares armazenavam na época do pronunciamento da Corte. É inegável que a devassa dos dados, hoje, causaria uma violação maior e mais grave à intimidade e à vida privada do preso em flagrante, devido à quantidade de informações contidas nesses aparelhos.

No ano de 2016 foi a vez do Superior Tribunal de Justiça proferir decisão sobre o tema, quando do julgamento do RHC nº 51.531/RO[29], de Relatoria do Ministro Nefi Cordeiro.

No caso, o recorrente argumentou que o aparelho apreendido no momento da sua prisão em flagrante somente poderia ser acessado mediante autorização judicial, mas não só isso: seria também necessário que essa devassa fosse acompanhada pelo Ministério Público e por sua defesa, diante dos riscos de desvirtuamento, acréscimo ou exclusão do conteúdo a ser extraído.

Diante do alegado, o Relator afirmou que o aparelho celular deixou de ser apenas um instrumento de conversação a longa distância, permitindo muitas outras funções, como o envio de mensagens, o acesso à *Internet*, dentre outras. Sendo assim, entendeu que o acesso aos dados nele contidos, embora possível, exige prévia autorização judicial motivada, uma vez que representa violação a dados privados do agente. Ademais, a violação do teor do *WhatsApp* seria análoga à violação de outros dados, como os *e-mails*, os quais o STJ já teria entendido ser indispensável o pronunciamento judicial[30].

O Relator foi acompanhado pelos Ministros Rogério Schietti Cruz e Maria Thereza de Assis Moura.

Vale ressaltar, aqui, um ponto interessante do voto proferido pela Ministra Maria Thereza, ao citar precedentes das Cortes Constitucionais de outros países, como os Estados Unidos, o Canadá e a Espanha.

A Suprema Corte do Canadá, por exemplo, ao julgar um caso de roubo, no qual um dos envolvidos estava armado, entendeu, por maioria de 4 votos a 3, pela

---

[29]BRASIL. Superior Tribunal de Justiça. *HC nº 51.531*. Relator: Ministro Nefi Cordeiro. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=54739651&num_registro=201402323677&data=20160509&tipo=51&formato=PDF. Acesso em: 06jun. 2019.

[30]BRASIL. Superior Tribunal de Justiça. *HC nº 315.220/RS*. Relator: Ministra Maria Thereza de Assis Moura. Disponível em:https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=47231121&num_registro=201500197570&data=20151009&tipo=91&formato=PDF. Acesso em: 27 fev. 2019.

legitimidade do acesso, pela polícia, aos dados armazenados em aparelho celular, sem a necessidade de prévia ordem judicial. Frise-se, porém, que o Tribunal mencionou ser essa devassa excepcional e permitida, naquele caso concreto, diante da presença de um elemento de urgência.

Em contrapartida, a Corte estabeleceu alguns requisitos para a legitimidade dessa medida, tais como: a licitude da prisão em flagrante; o acesso aos dados contidos em aparelho celular deve ser incidental à prisão, isso é, ocorrer imediatamente após o ato; e que as autoridades policiais responsáveis anotem detalhadamente o conteúdo dos dados examinados.

Ainda nessa linha, o Tribunal Constitucional espanhol julgou caso em que as autoridades policiais, sem prévia autorização judicial, acessaram a agenda telefônica de agentes presos em flagrante, em um caso envolvendo porte de drogas. Entendeu pela licitude das provas obtidas, ressaltando que se tratava de uma "ingerência leve" na intimidade e privacidade, considerando que apenas a agenda telefônica foi acessada. E destacou que a situação seria diferente se a devassa tivesse sido maior, envolvendo invasão mais substancial na privacidade dos envolvidos.

Os Tribunais Estaduais aqui no Brasil têm decidido pela licitude dessas provas obtidas em tais circunstâncias, ou seja, sem autorização judicial.

Vale destacar que o STF reconheceu a existência de repercussão geral desse tema no ARE 1.042.075[31], que está aguardando julgamento. Nesse processo, o parecer da PGR entendeu pela licitude das provas obtidas por meio da análise de registros e informações contidos no aparelho celular dos acusados, ainda que sem a autorização judicial, pois a exigência de reserva de jurisdição aplica-se somente à quebra de sigilo das comunicações, e não de dados ou registro do aparelho.

A verdade é que, embora a matéria esteja na iminência de ser enfrentada pela Suprema Corte, ainda gerará muita divergência entre doutrina e jurisprudência.

Isso porque, caso se entenda que as autoridades policiais não podem acessar tais registros e dados telefônicos sem o respectivo aval judicial, os efeitos práticos dessa posição são o engessamento da atividade policial e o retardamento das investigações, bem como a sobrecarga do Poder Judiciário, que será constantemente instado a decidir sobre isso.

---

[31]BRASIL. Supremo Tribunal Federal. *ARE 1.042.075/RJ*. Relator: Ministro Dias Toffoli. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5173898. Acesso em: 06 jun. 2019.

Por fim, é importante mencionar que essa questão está abarcada no que foi chamado pela imprensa nacional de “Pacote Anticrimes”, projeto de lei proposto pelo atual Ministro da Justiça, Sérgio Moro. Caso aprovado, permitiria o monitoramento de “qualquer meio tecnológico disponível desde que assegurada a integridade da diligência e poderá incluir a apreensão do conteúdo de mensagens e arquivos eletrônicos já armazenado em caixas postais eletrônicas"[32].

CONCLUSÃO

Essa pesquisa constatou, como problemática essencial, um conflito entre princípios, normas e questões práticas do dia-a-dia jurídico. Tal conflito é agravado pela ausência, até o presente momento, de uma jurisprudência firme que possa solucioná-lo e trazer segurança jurídica para os cidadãos (em especial para aqueles que, eventualmente, serão presos em flagrante) e operadores do Direito.

Conforme analisado no primeiro capítulo, a Carta Constitucional veda, expressamente, a utilização de provas obtidas por meio ilícito no processo penal. Portanto, é de suma importância definir se as provas que foram obtidas até agora, e as que ainda serão colhidas, nos inquéritos policiais e ações penais que se desenvolvem em nosso sistema jurídico, por meio do acesso ao *smartphone* do acusado, sem autorização judicial, são lícitas ou não.

De um lado, Promotores de Justiça e Delegados de Polícia sustentam que o acesso ao conteúdo do aparelho celular do preso em flagrante não se enquadra no conceito de interceptação telefônica e, como tal, não faria incidir a proteção do art. 5º, inciso XII, da CRFB/88, tampouco da Lei nº 9.296/96. Isso porque, como foi explicado ao longo desta pesquisa, quando se acessa o *WhatsApp*, por exemplo, o que se encontra são dados armazenados, estáticos, ao passo que a interceptação pressupõe que a comunicação esteja ocorrendo em tempo real. Sendo assim, tais provas dispensariam autorização judicial, não havendo que se falar em ilicitude ou desentranhamento dos autos.

De outro, advogados e Defensores Públicos sustentam que o referido acesso representa, no mínimo, uma mitigação à privacidade e à intimidade dos cidadãos e,

---

[32] BRASIL. Ministério da Justiça e Segurança Pública. Projeto de lei. Disponível em: https://www.justica.gov.br/news/collective-nitf-content-1550594052.63/pl-mjsp-medidas-contra-corrupcao-crime-organizado.pdf. Acesso em 06 jun. 2019.

como tais direitos são de extrema relevância constitucional, a autorização judicial faz-se indispensável.

No que tange ao aspecto prático da questão, não há dúvidas que a exigência da autorização judicial, por atrasar a análise das informações contidas no aparelho telefônico, pode atrapalhar as investigações, inclusive acarretando perda de dados que podem ser, por exemplo, apagados. Tal problema precisa ser considerado na análise da questão que se discute, uma vez que o avanço da tecnologia é uma realidade e o Direito, ao captar os anseios da sociedade, precisa se adaptar a ele.

A situação fica ainda mais complicada devido à ausência de uma jurisprudência formada em um determinado sentido. Como anteriormente mencionado, o Supremo Tribunal Federal até tem decisão sobre o tema, mas, por ser muito antiga, não trabalha a dimensão e a riqueza de detalhes que esses dados possuem nos dias atuais. O Superior Tribunal de Justiça, por seu turno, pronunciou-se recentemente a respeito, mas o que se tem é um julgado apenas, o que não é suficiente para dissolver toda a controvérsia.

Em que pese se tratar de uma questão delicada, na qual o excesso de formalismo pode gerar impunidade, o entendimento a que chegou esta pesquisadora consubstancia-se na ideia de que a autorização judicial seria indispensável. Apesar de não se tratar do conceito clássico de interceptação telefônica, a hipótese de acesso aos dados já armazenados no aplicativo *WhatsApp*, mensagens, redes sociais, etc., está tutelada no Marco Civil da Internet, logo, para que essa autorização judicial pudesse ser dispensada seria necessária uma alteração legislativa.

REFERÊNCIAS

AVENA, Norberto. *Processo Penal*. 10. ed. Rio de Janeiro: Forense, São Paulo: MÉTODO, 2018.

BRASIL. *Constituição da República Federativa do Brasil*, de 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 27 fev. 2019.

_____. *Decreto-Lei nº 3.689*, de 3 de outubro de 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 27 fev. 2019.

_____. *Lei nº 12.965*, de 23 de abril de 2014. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 27 fev. 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: 14 fev. 2019.

_____. Ministério da Justiça e Segurança Pública. Projeto de lei. Disponível em: https://www.justica.gov.br/news/collective-nitf-content-1550594052.63/pl-mjsp-medidas-contra-corrupcao-crime-organizado.pdf. Acesso em 06 jun. 2019.

_____. BRASIL. Supremo Tribunal Federal. *ARE 1.042.075/RJ*. Relator: Ministro Dias Toffoli. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5173898. Acesso em: 06 jun. 2019.

_____. Supremo Tribunal Federal. *HC nº 315.220/RS*. Relator: Ministra Maria Thereza de Assis Moura. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ATC&sequencial=47231121&num_registro=201500197570&data=20151009&tipo=91&formato=PDF. Acesso em: 27 fev. 2019.

_____. Supremo Tribunal Federal. *HC nº 91.867*. Relator: Ministro Gilmar Mendes. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2792328. Acesso em: 27 fev. 2019.

GOMES, Luiz Flávio. *Interceptação telefônica:* comentários à Lei 9.296, de 24.07.1996. 3. ed. rev. e atual. - São Paulo: Revista dos Tribunais, 2014.

OLIVEIRA, Eugênio Pacelli de. *Curso de Processo Penal*. 18. ed. São Paulo: Atlas, 2014.

PEREIRA, Murilo Cézar Antonini. Acesso aos dados armazenados no WhatsApp pela polícia durante investigação criminal: implicações nos direitos fundamentais. *Revista Jus Navigandi*, Teresina, n. 5535, 27 ago. 2018. Disponível em: <https://jus.com.br/artigos/68482>. Acesso em: 14 fev. 2019.

RANGEL, Paulo. *Direito Processual Penal*. 22. ed. São Paulo: Atlas, 2014.