ISSN 2447-1097

Direito & TI–Porto Alegre / RS www.direitoeti.com.br

PERÍCIA EM CELULAR: NECESSIDADE DE AUTORIZAÇÃO JUDICIAL?

Alesandro Gonçalves Barreto[1]

Everton Ferreira de Almeida Férrer[2]

RESUMO

O artigo analisa tema de grande relevância para o momento, qual seja se há a necessidade ou não de ordem judicial para o acesso a dados constantes de telefones celulares, sejam eles conversas em aplicativos, fotografias, agenda telefônica, etc. Decisões anteriores dos Tribunais, inclusive do Supremo Tribunal Federal - STF, garantiam o acesso independentemente de ordem judicial, contudo, em recente decisão, a 6ª Turma do Superior Tribunal de Justiça - STJ entendeu ser ilícito o acesso aos dados do telefone, ainda que em flagrante delito, sem prévia ordem judicial.

Palavras-chave: Celular; Ordem Judicial; Perícia.

INTRODUÇÃO

A popularização dos smartphones tem modificado a forma de interação das pessoas. O telefone apenas visto com a função de efetuar ou receber chamadas, agora, passou a ser um aparelho multifuncional, possibilitando ao seu usuário: envio e recebimento de mensagens, fotografar, filmar, ter conexão com a *Internet*, envio de e-mails, agenda telefônica, armazenamento de dados e utilização de aplicativos de mensagens. Esta funcionalidade tem contribuído para a migração de todos os serviços num só lugar. Em contrapartida, o telefone móvel tem sido utilizado como meio para o cometimento de vários delitos, desde a simples ameaça até a extorsão mediante sequestro.

A polícia judiciária tem encontrado dificuldades na investigação de delitos, em razão dos criminosos utilizarem de aplicações de *Internet* disponíveis para celulares como potencializadores de suas ações. A contabilidade de um traficante, por exemplo, na realização de uma busca e apreensão, era encontrada em anotações. Hoje, armazenada em um telefone, não

1 Delegado de Polícia Civil do Estado do Piauí e coautor do livro Inteligência Digital da Editora Brasport. delbarreto@gmail.com.

2 Delegado de Polícia Civil do Piauí.

deixou de ser elemento informativo de interesse à individualização da autoria e materialidade delitiva. Da mesma forma, é o conteúdo de aplicativos de mensagens armazenadas no aparelho de um investigado que, ao ser apreendido, pode trazer dados úteis à apuração do fato.

1. DESNECESSIDADE DE ORDEM JUDICIAL

O Código de Processo Penal determina a apreensão de todos os objetos que tenham relação com o fato, bem como todas as provas que servirem ao seu esclarecimento. É dever da autoridade policial proceder como tal, o que, no presente caso, significa saber se os dados constantes da agenda dos aparelhos celulares têm alguma relação com a ocorrência investigada[i].

No decorrer de uma investigação policial, ao proceder à apreensão de celulares, a autoridade policial faz a remessa dos aparelhos, a fim de que sejam periciados e extraídos todos os dados. Entretanto, ao requisitar a Perícia Criminal, é comum o Delegado ser informado que tal procedimento não pode ser realizado sem um mandado judicial, sob o argumento de que os dados contidos no telefone são acobertados pelo sigilo telefônico.

Tal conduta não é compatível com os ditames constitucionais em vigor, sendo, destarte, necessário diferenciar o acesso aos dados contidos no telefone móvel apreendido, da interceptação telefônica, popularmente conhecida como “escuta”. No primeiro caso, a autoridade policial necessita saber se os dados contidos naquele aparelho têm qualquer relação com o evento criminoso ou algum elemento que possa individualizar a autoria e a materialidade delitiva, nos precisos termos do art. 6º, do Código de Processo Penal. Não há, portanto, nenhuma violação ao conteúdo de conversa telefônica, visto que os dados armazenados já trafegaram entre os aparelhos. Na interceptação telefônica há acesso ao áudio e elementos de conversas mantidas entre interlocutores, ou seja, o fluxo de comunicações dos investigados. Nesse último caso, há a necessidade de autorização judicial para se efetivar a medida.

A Constituição Federal consagra a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial. A Lei 9.296, de 1996, que regulamentou a parte final desse inciso constitucional, trata da interceptação das comunicações telefônicas e do fluxo de comunicações em sistemas de informática e telemática. A proteção nesse caso é relacionada ao tráfego dessas

informações e não ao que se encontra registrado no aparelho telefônico. O dado armazenado não está mais exposto à vulnerabilidade de transmissão. Nesse sentido já se manifestou o Min. Gilmar Mendes:

> Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do art. 5º, XII, da CF, de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados. 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 à 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.[ii]

Nesse cenário, é óbvio que, ao realizar a perícia em um telefone celular, extraindo-se o conteúdo da agenda telefônica e demais dados interessantes para a investigação policial, não há que se falar em quebra de sigilo telefônico. Assim, quando se realiza uma perícia em aparelho móvel, não há nenhuma violação ao conteúdo das conversas mantidas entre os interlocutores.

Diversos outros Tribunais manifestaram-se no sentido da legalidade no exame dos dados.[iii]

2. NOVAS TECNOLOGIAS E POLÍCIA JUDICIÁRIA

Os aplicativos de comunicação são utilizados hoje em grande escala, desde um simplório bate-papo, como instrumento para empresas de prestação de serviços e até como contato de serviços de emergência. Por outro lado, os novos meios de comunicação também ofertam a inviolabilidade por intermédio de mecanismos de criptografia, que são utilizados por criminosos para assegurar uma comunicação segura no planejamento e na execução de infrações penais, sendo, pois, um desdobramento natural o uso destas novas tecnologias por delinquentes contumazes, valendo-se os mesmos do manto constitucional da inviolabilidade e intimidade para prática dos mais variados atos.

ISSN 2447-1097

Em que pese o Marco Civil da Internet estabelecer o dever de obediência à legislação pátria, por parte dos provedores de conexão ou de aplicações de *Internet*, mesmo que a empresa esteja sediada no exterior e desde que tenha representante do mesmo grupo econômico e oferte serviço ao público brasileiro, o que temos visto são reiterados descumprimentos às decisões judiciais, causando prejuízos à investigação policial em andamento.

Apesar da gama de decisões favoráveis, conforme acima exposto, o Superior Tribunal de Justiça, em recente decisão prolatada no RHC 51.531 oriunda da 6ª Turma, decidiu, por unanimidade, pela primeira vez, que: "Ilícita é a devassa de dados, bem como das conversas de whatsapp, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial". A presente decisão merece ser analisada sob a ótica do ordenamento jurídico brasileiro, bem como sob o manto de decisões anteriores do STF e do STJ em matérias semelhantes.

A Constituição Federal reza que a intimidade é inviolável e no inciso seguinte dispõe que a casa é asilo inviolável do indivíduo, não se podendo nela adentrar sem consentimento do morador, mas ressalva o caso de flagrante delito. Ademais, a Constituição também determina que ninguém será privado de sua liberdade, isto é, preso, senão em flagrante delito. De acordo com a Carta Magna, por meio deste é possível mitigar a proteção à liberdade e a privacidade/intimidade do indivíduo, na medida em que é possível prendê-lo e adentrar em sua residência. Dessa forma, será que em uma situação de flagrante delito, em que já foram mitigadas importantes garantias constitucionais, onde inclusive já houve violação da privacidade/intimidade no momento em que se adentra no domicílio do indivíduo e são feitas buscas à procura da materialidade delitiva, as mensagens constantes de aparelho celular, sejam elas de aplicativos ou de SMS, estariam sob o manto da proteção constitucional da inviolabilidade das comunicações?

O Tribunal de Justiça do Rio Grande do Sul, ao apreciar a extração de conteúdo de celular em caso de flagrante, admitiu essa possibilidade, conforme se infere da presente decisão:

> APELAÇÃO CRIMINAL. TRÁFICO DE DROGAS. PRELIMINAR DE NULIDADE DA TRANSCRIÇÃO DE MENSAGENS ELETRÔNICAS CONSTANTES DO TELEFONE CELULAR DO RÉU. As transcrições realizadas não violam o direito constitucional (art. 5º, XII), pois não foram obtidas de forma ilícita. Os policiais não se anteciparam à ação do réu e investigaram sua correspondência sem seu conhecimento. Na verdade, o réu

> já havia lido os torpedos e oportunizou seu manuseio pelos policiais que realizaram o flagrante, já que não os deletou. No caso dos autos, portanto, não houve quebra do sigilo de correspondência, pois essa já não era mais sigilosa, tendo sido aberta e mantida incólume por seu destinatário, o qual a deixou à mão da autoridade investigativa que realizou o flagrante. O réu estava praticando um delito e, como é curial, os objetos ligados ao crime são passíveis de apreensão e perícia técnica correspondente. [iv]

A liberdade é o bem, depois da vida, mais importante do indivíduo. Mesmo com esse grau de importância, qualquer pessoa pode ser presa em flagrante delito. Com relação à privacidade/intimidade pode-se analisar a decisão do STJ à luz do que ocorre com o sigilo epistolar do preso. O STF assim já se manifestou, demonstrando que se faz necessária a ponderação de valores constitucionais, 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. A restrição de um dos direitos em detrimento do outro deve obedecer ao princípio da proporcionalidade. No referido RHC 51.531, que firmou o entendimento acima questionado, a Ministra Maria Thereza de Assis Moura fundamenta seu voto na discussão em torno da ponderação das garantias constitucionais, sob a ótica da proporcionalidade, inclusive citando precedentes antagônicos em diversos países.

No âmbito da jurisprudência nacional, podemos citar precedente do STF, que ilustra a aplicação do princípio da proporcionalidade quando do choque de garantias constitucionais, mais especificamente no caso de quebra do sigilo de correspondência de preso:

> A administração penitenciária, com fundamento em razões de segurança pública, de disciplina prisional ou de preservação da ordem jurídica, pode, sempre excepcionalmente, e desde que respeitada à norma inscrita no art. 41, parágrafo único, da lei 7.210/84, proceder à interceptação da correspondência remetida pelos sentenciados, eis que a cláusula tutelar da inviolabilidade do sigilo epistolar não pode constituir instrumento de salvaguarda de práticas ilícitas.[v]

Assim, no caso acima, não se fala em prévia ordem judicial para violação do sigilo epistolar do preso, e nem poderia, porque tais comunicações são rápidas e depois de efetivadas são quase que impossíveis de serem achadas pelos agentes prisionais. Do mesmo modo, na ocorrência de uma situação de flagrante delito, caso a Polícia não acesse rapidamente o

conteúdo de mensagens já trocadas, diligências podem ficar comprometidas no sentido de buscar a materialidade.

Insta realçar ainda sobre a necessidade de acesso rápido ao terminal móvel do investigado ou autuado no momento de sua prisão ou da realização de busca e apreensão, sob pena de se perderem elementos informativos importantíssimos à investigação em curso. Os avanços tecnológicos têm possibilitado o acesso remoto aos dispositivos móveis, possibilitando ao seu proprietário, ou a quem tiver acesso à sua conta, apagar todos os dados, incluindo: cartão SD, e-mail, agenda, contatos, fotos, áudios, vídeos e todo conteúdo armazenado no aparelho. Em dispositivos que utilizem o sistema operacional *IOS* com compartilhamento familiar, será possível remover o conteúdo de todos os *devices* compartilhados.

Durante uma investigação criminal, a autoridade policial, além de colher elementos informativos que servirão para o esclarecimento do fato e de suas circunstâncias, deverá zelar na preservação destes, providenciando para que não se altere seu estado e conservação. No caso de uma prisão em flagrante, por exemplo, se a polícia não tiver acesso rapidamente ao telefone do autuado, impedindo a exclusão remota do conteúdo ali armazenado, certamente a investigação será prejudicada.

A eliminação do teor remotamente pelo criminoso foi referida em matéria da BBC News no ano de 2014, relatando sobre seis aparelhos que estavam sob custódia da polícia de Dorset em que os conteúdos foram apagados. Situação semelhante foi experimentada pelas polícias de Cambridgeshire, Durham e Nottingham[vi].

Para tanto, a polícia deve atuar, evitando o comprometimento de seu trabalho de persecução penal. Sobre isso já nos posicionamos ao tratar sobre como proceder na preservação da evidência digital, ao mencionar que:

> As inovações tecnológicas criam um novo local de crime: o virtual. Diferentemente do local de crime real em que podem ser encontradas testemunhas, imagens de circuitos internos, indícios e vestígios, nele, as evidências encontradas são voláteis e, caso não sejam prontamente preservadas, dificilmente a polícia logrará êxito na individualização da autoria delinquencial, sendo, por conseguinte, comum a modificação, danificação ou destruição, em pouquíssimo tempo, das provas e indícios[vii].

ISSN 2447-1097

CONCLUSÃO

Apesar das divergentes decisões dos tribunais sobre o tema, entendemos que, com base nos argumentos acima expostos, a consulta das últimas mensagens de texto recebidas em aparelho celular não representa quebra de sigilo telefônico, pois não houve acesso às conversas telefônicas realizadas, mas sim simples verificação de registro gravado no próprio aparelho.

Não há que se falar, portanto, que os dados contidos no celular apreendido estejam acobertados pela garantia do sigilo e da reserva jurisdicional. Tal conduta retarda as investigações e vai contra o princípio da oportunidade existente na atividade policial. Assim, respostas que poderiam ser dadas rapidamente por parte de uma delegacia que investiga determinado crime, ficam prejudicadas aguardando por uma ordem judicial não necessária.
Portanto, não se faz necessário mandado judicial para realizar perícia em aparelho telefônico móvel apreendido pela polícia.

É cediço que, no caso de flagrante delito, onde o indivíduo tem privada a liberdade e, por vezes, violado seu domicílio para que seja efetuada sua prisão, não pode se valer de proteção da intimidade/privacidade para acobertar provas do crime imediatamente praticado, dificultando diligências policiais e tornando um risco à futura produção probatória.

Por fim, é importante considerar que em tempos atuais, em que a sociedade convive com índices de criminalidade alarmantes, pode-se asseverar que o “choque” entre as garantias da privacidade/intimidade e a da segurança pública é tema que merece atenção por parte dos Tribunais em todas as decisões a serem tomadas, devendo, no caso em tela, prevalecer o interesse público para que possam ser combatidos os crimes praticados, sem deixar de lado os limites constitucionais e legais impostos pelo ordenamento jurídico nacional.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves. Preservação da Evidência Eletrônica: Desafio à Polícia Judiciária**.** **Direito & TI**. Disponível em: <http://direitoeti.com.br/artigos/preservacao-da-evidencia-eletronica-desafio-a-policia-judiciaria/>. Acesso em: 19 mai. 2016.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >. Acesso em: 18. Mai. 2016.

_____. Decreto-Lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em: 19. mai. 2016.

_____. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9296.htm>. Acesso em: 19. mai. 2016.

_____. Lei nº 12.965, 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/leis/LCP/Lcp105.htm>. Acesso em: 19. mai. 2016.

_____. Supremo Tribunal Federal. **Acórdão de decisão que julgou alegação de interceptação criminosa de carta missiva remetida por sentenciado**. Habeas Corpus nº 70.814-5/SP. Ulisses Azevedo Soares e Tribunal de Justiça do Estado de São Paulo. Relator: Ministro Celso de Melo. Julgado em 01 mar. 1994. Acesso em: 19 mai. 2016.

_____. Supremo Tribunal Federal. **Acórdão de decisão que julgou ilicitude de prova produzida durante inquérito policial.** Habeas Corpus nº 91.867/SP. Davi Resende Soares e Superior Tribunal de Justiça. Relator: Ministro Gilmar Mendes. Julgado em 24 abr. 2012. Acesso em: 19 mai. 2016.

_____. Superior Tribunal de Justiça. **Acórdão de decisão que apreciou a nulidade da prova face ausência de autorização judicial em perícia de celular**. Recurso em Habeas Corpus nº 51.531/RO. Leri Souza Silva e Ministério Público do Estado de Rondônia. Relator: Ministro Nefi Cordeiro. Julgado em 19 abr. 2016. Acesso em: 19 mai. 2016.

_____. Superior Tribunal de Justiça. **Acórdão de decisão que apreciou a nulidade da prova face ausência de autorização judicial em perícia de celular**. Recurso em Habeas Corpus nº 66.368/PA. Davi Resende Soares e Câmaras Criminais Reunidas do Tribunal de Justiça do Estado do Pará. Relator: Ministro Gilson Dipp. Julgado em 05 jun. 2007. Acesso em: 19 mai. 2016.

_____. Tribunal Regional Federal da 3ª Região. **Acórdão do julgamento da legalidade da apreensão e consultas a mensagens de texto recebidas em celular**. Apelação Criminal nº 0011947-59.2009.4.03.6000/MS. Justiça Pública e Edgar Freti Sarataio. Rel. Des. Henrique Herkenhoff. Julgado em 31 ago. 2010. Acesso em: 19 mai. 2016.

_____. Tribunal Regional Federal da 4ª Região. **Acórdão de decisão pela inexistência da violação de sigilo telefônico na verificação de chamadas realizadas e recebidas constantes na memória de telefone celular**. Apelação Criminal nº 29123 PR 2002.04.01.029123-1. José Heitor Ferruci Alves e Ministério Público. Rel.Des. Fábio Bittencourt da Rosa. Julgado em 29 abr. 2003. Acesso em: 19 mai. 2016.

WAKEFIELD, Jane. BBC News. **Devices being remotely wiped in police custody**. Publicado em 09 out.2014. Disponível em: <http://www.bbc.com/news/technology-29464889>. Acesso em: 19. mai. 2016.

[i] STJ. Recurso em Habeas Corpus nº 66.368/PA. Rel. Min. Gilson Dipp.
[ii] STF. Habeas Corpus nº 91.867/SP.Rel. Min.Gilmar Mendes
[iii] TRF4. Apelação Criminal nº 29123 PR 2002.04.01.029123-1. Rel. Des. Fábio Bittencourt da Rosa.

ISSN 2447-1097

[iv] TJRS. AC Nº 70034502781. 1ª C.C. Rel. Des. Manuel José Martinez Lucas.
[v] STF. Habeas Corpus nº 70.814-5/SP. Rel. Min. Celso de Melo.
[vi] BBC News. *Devices being remotely wiped in police custody*.
[vii] Direito & TI. Preservação da Evidência Eletrônica: Desafio à Polícia Judiciária.