



PRP
Pró-Reitoria de
Pesquisa e
Pós Graduação



Universidade
Estadual de Goiás



**UNIVERSIDADE ESTADUAL DE GOIÁS
SECRETARIA DA SEGURANÇA PÚBLICA E ADMINISTRAÇÃO PENITENCIÁRIA
SUPERINTENDÊNCIA DA ACADEMIA ESTADUAL DE SEGURANÇA PÚBLICA
CURSO DE PÓS-GRADUAÇÃO EM ALTOS ESTUDOS EM SEGURANÇA
PÚBLICA – CAESP 2017**

THIAGO JUNQUEIRA RODRIGUES

**O ACESSO ÀS INFORMAÇÕES CONTIDAS EM APARELHOS ELETRÔNICOS
APREENDIDOS**

**GOIÂNIA
2017**

THIAGO JUNQUEIRA RODRIGUES

**O ACESSO AOS DADOS CONTIDOS EM APARELHOS ELETRÔNICOS
APREENDIDOS**

Artigo apresentado ao CAESP/2017, da Secretaria de Segurança Pública e Administração Penitenciária, em cooperação técnica com a Universidade Estadual de Goiás, como requisito parcial para obtenção do título de Especialista em Altos Estudos de Segurança Pública.

Orientador: Profa. Ms. TC Silvana Rosa de Jesus Ramos.

Data da Aprovação: ____ / ____ / ____

Profa. Orientadora Ms. Tenente Coronel Silvana Rosa de Jesus Ramos

Profa. Avaliadora Esp. Nélia Cristina Pinheiro Finotti

Prof. Avaliador Ms. Julio Alejandro Quezada Jelvez

GOIÂNIA

2017

O ACESSO AOS DADOS CONTIDOS EM APARELHOS ELETRÔNICOS APREENDIDOS

Thiago Junqueira Rodrigues¹

RESUMO

A apreensão de aparelhos eletrônicos como objetos relacionados a crime pode servir como meio de prova durante a fase investigativa da persecução penal. Nesta seara, o acesso aos dados existentes na memória de tais aparelhos pode ser imprescindível para a elucidação do crime ou a prevenção de futuros delitos. Todavia, esse acesso é protegido constitucionalmente pelo direito à privacidade e o sigilo das comunicações, quando os dados armazenados estiverem em contexto de comunicação. Nestes casos, o acesso a tais dados deverá respeitar a garantia da reserva jurisdicional, pela qual se exige autorização judicial prévia e mediante decisão fundamentada de um juiz competente. Contudo, há casos em que a urgência da situação concreta e o iminente perigo de lesão a outros bens jurídicos poderá tornar o acesso aos dados inócuo, caso seja necessário um procedimento formal ou mesmo verbal de solicitação de autorização prévia. De outra via, nem todos os dados presentes em aparelhos eletrônicos apreendidos são oriundos de comunicação. Em ambas as situações, o acesso aos dados contidos no aparelho poderá ocorrer independente de autorização judicial.

Palavras-chave: Acesso. Dados. Aparelhos eletrônicos.

ABSTRACT

The seizure of electronic devices as crime-related objects can serve as a means of proof during the investigative phase of criminal prosecution. In this area, the access to data stored in these devices can be indispensable for the elucidation of the crime or prevention of future crimes. However, this access is constitutionally protected by the right to privacy and confidentiality of private communication. In these cases, access to such data must respect the Jurisdictional reservation guarantee, by which there must be prior judicial authorization through by a reasoned decision of a competent court. Nevertheless, there are cases in which the urgency of the concrete situation and the imminent danger of injury to other legal goods may render the access to these data innocuous; if a formal or even verbal request for prior authorization is required. On the other hand, not all data present in seized electronic devices comes from communication. In both situations, access to data contained in the device may occur regardless of judicial authorization.

Key words: Access. Data. Electronic devices.

¹ Perito Criminal da Polícia Técnico-Científica de Goiás. Graduado em Direito, Especialista em Direito Administrativo.

INTRODUÇÃO

O desenvolvimento tecnológico contínuo e acelerado faz surgir frequentemente novas ferramentas tecnológicas que são incorporadas no dia-a-dia dos indivíduos. Todavia, tal velocidade de inovações não é acompanhada pela estrutura estatal, mormente no que diz respeito ao arcabouço jurídico. Não é incomum nos depararmos com ferramentas tecnológicas amplamente usadas pela sociedade e que não dispõe de qualquer regulamentação jurídica. Tal fator pode gerar conflitos na atividade estatal, principalmente em áreas de atuação vinculadas a ramos do Direito que são menos susceptíveis a mudanças e implementações de novos paradigmas. Isto é notório no Direito Penal, no qual as alterações levam tempo demasiadamente grande para acompanhar as constantes inovações tecnológicas. Tampouco se acompanham as novas ferramentas desenvolvidas para serem utilizadas dentro da persecução penal. Por vezes, a mudança se dá mediante técnicas de hermenêutica jurídica, pelas quais se busca suprir lacunas ou terminologias ultrapassadas utilizadas pelo legislador. Logo, a dinâmica dos fatos sociais obriga o operador do Direito a buscar a vontade da lei e não a do legislador.

Fato que gera bastante controvérsia no mundo jurídico diz respeito ao acesso aos dados contidos na memória de aparelhos eletrônicos apreendidos pelos órgãos policiais. Nestes casos, o aparelho serve não apenas para elucidar o delito já conhecido, como também poderia auxiliar na prevenção de futuros delitos. Entretanto, a celeuma se concentra entre a defesa das garantias fundamentais ao sigilo das comunicações e à intimidade em oposição à defesa dos bens jurídicos tutelados que foram ofendidos pelo ato delituoso.

Conforme disposição constitucional, a liberdade de comunicação pessoal é um direito fundamental que apresenta o sigilo das comunicações como uma garantia de não intervenção estatal na intimidade do indivíduo. Todavia, a própria Constituição traz uma espécie de intervenção restritiva deste direito. Trata-se da possibilidade de violação das comunicações nos casos de investigação criminal ou de instrução processual penal.

No entanto, dúvida persiste quanto à necessidade de autorização judicial prévia para acesso aos dados que não foram objeto de comunicação. Trata-se de

arquivos fotográficos, sonoros ou mesmo o registro de histórico de localização do aparelho via sistemas de navegação por coordenadas em GPS, por exemplo. Nestes casos, é importante estabelecer até que ponto tais dados estariam amparados pela garantia da privacidade. Também é importante estabelecer nestes casos a necessidade ou não da autorização judicial prévia.

Na mesma seara, surge outra possibilidade factível no cotidiano policial. São os casos em que há urgência na intervenção policial com o fito de se fazer cessar um crime em andamento ou mesmo de se evitar a execução de outro crime. É o caso, por exemplo, da detenção de um suspeito de participar de um grupo que estaria mantendo uma vítima em cárcere privado. Caso se apreenda o aparelho de telefonia móvel do suspeito, quais seriam os limites do acesso aos dados do aparelho frente à inviolabilidade das comunicações e à garantia da privacidade do suspeito? Em outras palavras, havendo perigo na demora e indícios suficientes para comprovar a situação delituosa, o policial poderia agir sem a necessidade de uma autorização judicial prévia? Estas questões que o presente artigo pretende discutir.

Portanto, este trabalho tem como objetivo contribuir para o estabelecimento dos limites quanto ao acesso sobre os dados contidos em aparelhos eletrônicos apreendidos. Apresentará em quais situações o policial poderá acessar os dados sem a necessidade de prévia autorização judicial e em quais casos ele deverá esperar a decisão fundamentada do juiz competente para que realize o acesso.

A metodologia foi baseada em pesquisa bibliográfica, utilizando-se o posicionamento de doutrinadores pátrios bem como a jurisprudência dos Tribunais Superiores nacionais. Buscou-se assim um referencial teórico para que se pudesse adequar os procedimentos operacionais e investigativos ao que poderá ser aceito como prova nos processos criminais.

O presente artigo aborda a apreensão de aparelhos eletrônicos e a possibilidade de acesso aos dados contidos nos mesmos, para os quais a principal bibliografia utilizara fora Bernardes e Ferreira (2016), Lima (2016), Avena (2014), e Knijnik (2014), além dos julgados colegiados do Supremo Tribunal Federal e do Superior Tribunal de Justiça.

1 A APREENSÃO DE APARELHOS ELETRÔNICOS

Conforme lição de Avena (2014, p. 573), apreensão é o “ato de retirar alguma coisa que se encontre em poder de uma pessoa ou em determinado lugar, a fim de que possa ser utilizada com caráter probatório ou assecuratório de direitos”.

Da própria definição, podem-se extrair duas situações gerais em que é possível se realizar a apreensão. A primeira diz respeito aos casos em que o objeto está em poder direto de uma pessoa, junto ao seu corpo ou em suas roupas. Este caso está previsto como busca pessoal no art. 240, §2º do Código de Processo Penal. Na atuação policial, este exemplo é diretamente ligado aos casos de prisão em flagrante. Contudo, a busca pessoal também poderá ser feita fundamentada na simples suspeita de que o indivíduo esteja portando um objeto ilícito. Nestes casos, a busca poderá ser realizada por mandado expedido pela Autoridade Policial.

No entanto, há casos que dispensam a expedição de mandado, sendo estes previstos especificamente no art. 244 do mesmo diploma legal, dentre os quais destacamos as situações em que “houver fundada suspeita de que a pessoa esteja na posse de arma proibida ou de objetos ou papéis que constituam corpo de delito”.

A outra situação trazida pela definição trata da possibilidade de se realizar a apreensão nos casos em que há objetos dispostos em determinado local. Aqui entraria tanto a busca e apreensão domiciliar quanto os casos de objetos encontrados em cenas de crime. Nestas, há verdadeira obrigação dirigida à Autoridade Policial no que tange a apreensão dos objetos que tiverem relação com o fato criminoso.

Assim, observamos que aparelhos eletrônicos podem ser objeto de apreensão quando forem constatados na busca pessoal, nos casos em que forem encontrados em cenas de crimes, bem como quando estiverem em residência, escritório, repartições públicas ou outros locais que forem alvos de mandado de busca e apreensão.

Dentro deste contexto, é valiosa a lição trazida por Távora e Alencar (2009, p. 337) ao definirem o que vem a ser corpo de delito:

Corpo de delito é o conjunto de vestígios materiais deixados pela infração

penal, os elementos sensíveis da mesma, a própria materialidade, em suma, aquilo que pode ser examinado através dos sentidos. Ex: a mancha de sangue deixada no local da infração; as lesões corporais; a janela arrombada no crime de furto, etc.

Percebe-se então que o aparelho eletrônico apreendido pode constituir-se no próprio corpo de delito. E os dados de sua memória compõem o conjunto de vestígios materiais deixados pela infração penal. Em que pese ser legítima a apreensão destes bens, o acesso ao conteúdo dos mesmos é objeto de controvérsias jurisprudenciais. Isto porque, na lição de Knijnik (2014), o acesso aos dados seria uma prova invasiva que é inatingível pelos sentidos, colocando-os como provas de terceira geração. Analisada isoladamente, a apreensão seria apenas um meio de prova destinada a assegurar a utilização do objeto nas investigações criminais e nos processos judiciais. Logo, para aquele autor, não seria inócua a apreensão de aparelhos eletrônicos sem a possibilidade imediata de transcrição de dados contidos nos mesmos.

2 O ACESSO AO CONTEÚDO DOS DADOS CONTIDOS EM APARELHOS ELETRONICOS APREENDIDOS

Inicialmente é importante definir o que vem a ser dado dentro de um sistema informacional. Para Côrtes (2008, p.25), dados são:

Sucessões de fatos brutos, que não foram organizados, processados, relacionados, avaliados ou interpretados, representando apenas partes isoladas de eventos, situações ou ocorrências. Constituem as unidades básicas a partir das quais informações poderão ser elaboradas ou obtidas.

Portanto, isoladamente os dados não trazem informações. Estas se configuram em verdadeiro juízo de valor obtido após a avaliação, interpretação e a conexão entre os dados. Ou seja, para se ter alguma informação e se poder construir conhecimento, é necessário relacionar e organizar de forma coerente os dados disponíveis.

Em que pesem as definições técnicas, os dados contidos em aparelhos eletrônicos são resguardados como sigilosos, tutelados como direitos individuais e

garantidos pela Constituição Federal de 1988, consoante art. 5º, inciso X: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” bem como no inciso XII, *in verbis*:

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.

Por oportuno, é importante a distinção trazida por Bernardes e Ferreira (2016, p. 54) na qual os dados são classificados como sensíveis ou não sensíveis. Aqueles dizem respeito à vida privada e a intimidade dos indivíduos, enquanto este traz informações de natureza pública. Logo, caso o aparelho apreendido seja de uso pessoal, estaremos diante de dados sensíveis. Note-se que a proteção constitucional genérica, dada ao direito à intimidade refere-se aos dados sensíveis.

De mesmo modo, observando-se os dois dispositivos constitucionais supracitados, deparamo-nos com uma situação dicotômica. Assim, os dados sensíveis contidos nos aparelhos apreendidos e que não foram objetos de comunicação poderiam ter sua proteção dada somente pelo inciso X, somente pelo inciso XII ou por ambos. Quanto a esta questão, Bernardes e Ferreira (2016) apontam a existência de três correntes de pensamento:

1ª Corrente – Teoria da Proteção Ampla, segundo a qual, o sigilo seria estipulado genericamente no inciso X e, de maneira mais específica, no inciso XII.

2ª Corrente – Teoria da Proteção Restrita, na qual este tipo de dado é exclusivamente protegido pelo inciso X, haja vista que não houve comunicação com transferência dos dados. Caso houvesse, os dados em comunicação seriam protegidos pelo inciso XII. Contudo, os dados propriamente ditos que não refletem o conteúdo do que fora comunicado não seriam protegidos por este inciso.

3ª Corrente – Teoria Intermediária. Nesta o inciso XII protege não apenas as comunicações pessoais como também os dados dela resultantes.

O Supremo Tribunal Federal já adotou a primeira corrente no Recurso Extraordinário (RE) número 389.808/PR, bem como na Reclamação (Rcl) número

9.428/DF. Em outras oportunidades, adotou a segunda corrente, conforme RE 601.314/SP e a Ação Direta de Inconstitucionalidade (ADIn) 2.390/DF.

A completude das mencionadas garantias previstas na Constituição Federal é dada em duas leis ordinárias. Trata-se das Leis 9.296/1996 e 12.965/2014. A primeira regulamenta os casos de interceptação telefônica, enquanto a segunda estabelece as garantias e os direitos para o uso da Internet no Brasil, sendo denominada de Marco Civil da Internet.

Ao analisar o primeiro diploma legal mencionado no parágrafo anterior, a doutrina mais moderna vem ampliando o conceito de comunicação telefônica, conforme explicação abaixo:

Considerando o fantástico desenvolvimento da informática na atualidade, a expressão comunicação telefônica não deve se restringir às comunicações por telefone. Por força de interpretação progressiva, a expressão comunicação telefônica deve também abranger a transmissão, emissão ou recepção de símbolos, caracteres, sinais escritos, imagens, sons ou informações de qualquer natureza, por meio de telefonia, estática, ou móvel (celular). Por conseguinte, é possível a interceptação de qualquer comunicação via telefone, conjugada ou não com a informática, o que compreende aquelas realizadas direta (fax, modens) e indiretamente (internet, e-mail, correios eletrônicos) (Lima, 2016, p. 144)

Este é o entendimento mais recente perfilado inclusive pelo Tribunal de Justiça de Goiás, consoante restou demonstrado no julgamento dos HC's 466215-76.2014.8.09.000 e 191692-09.2016.8.09.000, nos quais decidiu-se, respectivamente, pela ilicitude de provas produzidas através da transcrição de comunicação telemática (conversas inbox do Facebook) obtida em aparelho de computador devidamente apreendido mediante expedição de mandado de busca e apreensão por juiz competente, assim como a transcrição de conversas realizadas através do aplicativo WhatsApp existentes em aparelho de telefonia móvel apreendido por autoridade policial junto ao suspeito da prática de crime de homicídio.

Portanto, os direitos e garantias individuais relativos à comunicação telefônica abrangem também os meios mais modernos de comunicação, tais como as mensagens relativas aos aplicativos/sistemas WhatsApp, Facebook Messenger,

Telegram, Hangouts, Viber, Skype, Snapchat, IMO, WeChat, dentre outros existentes e aqueles que poderão ser lançados com objetivos similares.

Contudo, a abrangência do conceito de interceptação telefônica ainda não é tema pacífico dentro da jurisprudência dos tribunais superiores. Julgados recentes do Superior Tribunal de Justiça (STJ) mostram uma divergência no entendimento relativo ao que seria ou não subordinado às regras previstas na Lei 9.296/96. A divergência abrange o entendimento firmado pela Quinta e pela Sexta Turmas. Conforme o Recurso em *Habeas Corpus* (RHC) número 75800/PR, julgado no dia 15/09/2016 pela Quinta Turma, “a obtenção do conteúdo de conversas e mensagens armazenadas em aparelho de telefone celular ou smartphones não se subordina aos ditames da Lei 9.296/96”. A seu turno, o RHC 51531/RO julgado em 19/04/2016 pela Sexta Turma considerou “ilícita a devassa de dados, bem como das conversas de whatsapp, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial”.

Atentando-se ao fato de que a autoridade policial é responsável pela apreensão dos objetos que tiverem relação com o delito, imperiosa se faz a consideração acerca da possibilidade de transcrição dos dados telefônicos de chamadas originadas e recebidas, bem como os dados da agenda, avaliação de áudios e fotografias não compartilhadas que estejam armazenadas na memória dos aparelhos celulares e smartphones apreendidos, bem como registros de localização existentes em alguns aplicativos de navegação por GPS possivelmente instalados nos aparelhos. Neste caso, há entendimento nos tribunais superiores de que a simples indicação dos registros dos dados telefônicos relativos à agenda e às chamadas efetuadas e recebidas não se trata de prova obtida por meios ilícitos, por não se configurar quebra de sigilo telefônico. Isto porque não houve requerimento à empresa responsável pelas linhas telefônicas, no tocante à lista geral das chamadas originadas e recebidas. Ao contrário, constitui-se como verdadeira obrigação da autoridade policial que é a de apreender os objetos que tiverem relação com o fato, o que pode implicar em saber se os dados constantes na agenda do aparelho teriam alguma relação com a ocorrência investigada. Este é o entendimento que fora adotado pelo STJ no HC 66.368/PA, publicada em 29/06/2007. Em mesma linha foi

o posicionamento do Supremo Tribunal Federal (STF) no HC 91.867/PA, na qual o Exmo. Min. Gilmar Mendes² asseverou que:

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.

Desta forma, em interpretação extensiva, quando não implique o acesso ao teor de comunicações, o policial poderá acessar os dados contidos no aparelho eletrônico, independentemente de autorização judicial específica. Situações nas quais o exame prévio dos dados poderá ser feito, mesmo que haja necessidade de quebra da senha de acesso ao aparelho, haja vista que este é um meio indispensável para o acesso às informações. Ademais, tais informações presumem-se indispensáveis à investigação criminal.

Nos dias atuais, em que o acesso aos sistemas da maioria dos aparelhos eletrônicos requer uma senha do usuário, restringir o exame somente àqueles aparelhos que não apresentarem senha de acesso tornaria inócua a grande maioria de atividades de investigação urgentes desta natureza e prejudicaria sobremaneira a prevenção de ocorrências criminais. Além disso, entendimento contrário seria ir de encontro ao cerne do entendimento doutrinário e jurisprudencial quanto a este meio de prova. Logo, a simples existência de senha no aparelho não configuraria afronta maior à garantia da intimidade.

Por seu turno, a Lei 12.965/2014 trouxe no rol de direitos e garantias dos usuários de internet a inviolabilidade e o sigilo do fluxo das comunicações pela rede, bem como das comunicações privadas que estiverem armazenadas. Tais garantias foram mitigadas, podendo ser suprimidas desde que observada a cláusula da reserva jurisdicional. Acerca do tema, eis o que diz o Marco Civil da Internet (Lei 12.965/2014):

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

² <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=279232>, acessado em 01 maio 2017.

- 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;

A nova lei dirimiu uma divergência jurisprudencial e doutrinária existente no mundo jurídico até então. Esta se relacionava à possibilidade de acesso aos dados de comunicação que estivessem apenas armazenados. Ou seja, havia dúvidas se só seria considerados como dados de comunicação aqueles que estivessem no exato momento da transmissão.

Outra situação que enseja o acesso sem a prévia autorização judicial diz respeito aos casos em que há urgência na resposta estatal em defesa de direitos de terceiros. Assim, havendo o *fumus comissi delicti*, ou seja, a comprovação da existência de um crime e sua autoria, bem como o perigo na demora em resolver a situação não há de se cogitar em autorização judicial prévia para o acesso aos dados. Assim foi o posicionamento no voto-vista da Ministra do Superior Tribunal de Justiça, Min. Maria Thereza de Assis Moura³, no Recurso em *Habeas Corpus* número 51531/RO. Em seu voto, assim falou a Ministra:

Não descarto, de forma absoluta, que, a depender do caso concreto, caso a demora na obtenção de um mandado judicial pudesse trazer prejuízos concretos à investigação ou especialmente à vítima do delito, mostre-se possível admitir a validade da prova colhida através do acesso imediato aos dados do aparelho celular. Imagine-se, por exemplo, um caso de extorsão mediante sequestro, em que a polícia encontre aparelhos celulares em um cativeiro recém-abandonado: o acesso incontinenti aos dados ali mantidos pode ser decisivo para a libertação do sequestrado.

Conforme se depreende do voto da eminente Ministra, o direito à intimidade, a privacidade e o sigilo das comunicações telefônicas não são garantias absolutas, devendo haver o convívio das liberdades para o adequado convívio social.

³<https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=59892972&tipo=3&nreg=201402323677&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20160509&formato=PDF&salvar=false>, acessado em 22 de junho de 2017.

3 METODOLOGIA

Para atingir o êxito esperado, fizemos uma pesquisa bibliográfica, descritiva, mediante a utilização de compilação que consiste na exposição do pensamento de vários autores que escreveram sobre o tema escolhido.

A metodologia adotada foi a hipotético-dedutiva, embasada em um referencial teórico dialético-argumentativo. Buscou-se uma coerência entre os materiais bibliográficos consultados, que trouxeram o pensamento doutrinário em livros e artigos científicos, bem como as leis pátrias vigentes e a jurisprudência dos tribunais nacionais.

4 RESULTADOS E DISCUSSÕES

O presente trabalho foi concluído após análise de que nem todos os tipos de dados contidos em aparelhos eletrônicos apreendidos são protegidos pela reserva de jurisdição. Isso significa que, após a regular apreensão do aparelho, haverá dados que poderão ser acessados pelos policiais que estiverem em sua posse, mesmo sem a autorização judicial.

Destarte, a pesquisa jurisprudencial e doutrinária apontou para a restrição de acesso apenas em duas situações. A primeira diz respeito aos dados que foram alvo de comunicação. Neste ponto, independe se o acesso se dá aos dados armazenados ou durante a sua transmissão, conforme visto em Lima (2016). A segunda situação de restrição refere-se aos chamados dados sensíveis e foi trazida por Bernardes e Ferreira (2016). Trata-se daqueles dados que geram informações que dizem respeito à vida privada e à intimidade do indivíduo.

Destaque-se que o conjunto total de dados que podem estar armazenados em aparelhos eletrônicos engloba informações que vão além da comunicação. E, dentre aqueles que não foram objeto de comunicação, haverá ainda os dados que não estão vinculados à privacidade e intimidade do usuário do aparelho. Logo, o aparelho apreendido poderá conter fotografias, registros de localização por coordenadas geodésicas (GPS), comprovantes bancários, arquivos de texto e

áudios que não foram transmitidos em comunicação e não sejam necessariamente de âmbito da intimidade. Nestes casos, não há que se falar em inviolabilidade do sigilo das comunicações e intimidade.

Como exemplo, podemos analisar uma situação hipotética na qual uma pessoa é detida por suspeita de envolvimento em um crime de homicídio ocorrido há algumas horas em via pública. Com ele é apreendido um aparelho celular. Para confirmar a possibilidade de participação do detido, os policiais procedem então a uma pesquisa nos registros de localização do aparelho. Como, em regra, a localização apontada pelos aparelhos é voltada para as vias públicas, não há que se falar em privacidade já que se tratava de ambiente público e no qual o suspeito poderia ser visto por qualquer cidadão que por ali transitasse.

O exemplo acima é característico e serve para mostrar que nem todos os dados contidos na memória dos aparelhos apreendidos podem ser considerados sensíveis e protegidos pelo direito à intimidade. No mesmo diapasão, temos os casos de fotografias retiradas de armamento proibido ou de drogas ilícitas, anotações de vendas ou planilha de clientes, compradores de produtos ilícitos.

Uma terceira situação em que o acesso seria permitido mesmo sem a prévia autorização judicial é trazida pela jurisprudência em voto colecionado no mencionado Habeas Corpus 51531/RO do STJ. Engloba-se aqui a possibilidade da pesquisa de dados no interesse da investigação criminal quando esta se der em situações que demandem extrema urgência em sua resolução. Nesta situações, o acesso será permitido desde que haja forte indícios de autoria e evidente perigo na demora.

Também independem de prévia autorização judicial os casos em que os dados a serem acessados não forem objeto de qualquer tipo de comunicação, ou seja, não foram recebidos ou enviados para terceiros. Nesta situação, também deverá ser observado o direito à intimidade. Logo, além de não terem sido objeto de comunicação, os dados objetos de acesso não poderão ser considerados sensíveis, isto é, não poderão dizer respeito à intimidade e à vida privada do indivíduo.

É patente a importância de se ter acesso imediato aos dados contidos em aparelhos eletrônicos apreendidos pelas forças policiais. Muitas vezes, o acesso rápido pode significar a desarticulação de uma quadrilha, a resolução da

investigação de um crime ou mesmo a prevenção de outros delitos. Por outro lado, a convivência em um Estado de Direito introduz uma limitação à atuação estatal frente aos direitos e garantias fundamentais do indivíduo. Por isso, a delimitação de situações em que são permitidos acessos aos dados é de suma importância para as investigações criminais. Esperamos assim contribuir não apenas para a célere resolução de crimes como também sua prevenção e o resguardo da aplicação da lei penal ao diminuir a incidência de casos de decretação judicial da nulidade da prova relativa à transcrição de dados produzida durante as investigações criminais.

CONSIDERAÇÕES FINAIS

O presente estudo visou dirimir dúvidas quanto à possibilidade do uso de dados existentes na memória dos aparelhos eletrônicos apreendidos no curso da investigação criminal. Destarte, é de suma importância que o policial conheça os dados que são possíveis de se acessar sem a prévia autorização judicial, bem como as circunstâncias em que tal autorização poderá ser diferida. Este tipo de acesso torna-se de extrema relevância para os casos em que a urgência da atuação policial poderá não apenas proteger um bem jurídico de terceiros como também evitar o cometimento de novas infrações penais.

Em que pese o acesso aos dados poder constituir uma transgressão ao direito de intimidade do usuário do aparelho, tem-se que seu direito não poderá sobrepujar aos direitos de terceiros. Assim, observando-se que nem todo direito é absoluto, adotando-se o princípio da convivência das liberdades, temos que o acesso aos dados poderá ser realizado sempre que houver *periculum in mora* e o *fumus comissi delicti* até mesmo quando estes estiverem em contexto de comunicação.

Finalizado o presente estudo, esperamos contribuir com as forças policiais quanto à adoção de procedimentos a serem adotados logo após a apreensão de quaisquer tipos de aparelhos eletrônicos com memória. Tais procedimentos visam diminuir os casos de incidência de declaração de ilicitude da prova durante o trâmite do processo penal, bem como aumentar a eficácia da proteção policial aos bens

jurídicos tutelados pelo Estado. Isto porque o pronto acesso a alguns dados poderá acarretar em uma resposta repressiva e preventiva mais rápida, evitando-se a perda de provas e/ou a destruição das mesmas por outros indivíduos ligados ao evento delitivo.

REFERÊNCIAS BIBLIOGRAFICAS

AVENA, Norberto. **Processo Penal Esquematizado**. 6. ed. rev., atual. e ampl., São Paulo: Editora Método, 2014.

BERNARDES, Juliano Taveira; FERREIRA, Olavo Augusto Vianna Alves. **Direito Constitucional – Tomo II – Direito Constitucional Positivo**. 5. ed. rev. e atual., Salvador: Editora JusPodivm, 2016. 2v.

BRASIL. **Constituição da República Federativa do Brasil de 1988**, Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm> Acesso em: 10 de maio de 2017

_____. **Código de Processo Penal**. Decreto-Lei nº 3.689, de 03 de outubro de 1941, Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689Compilado.htm > Acesso em: 22 de maio de 2017

_____. **Lei nº 9.296, de 24 de julho de 1996**, Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/1996/L9.296.htm > Acesso em: 10 de maio de 2017

_____. **Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)**, Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2014/Lei/L12965.htm> Acesso em: 10 de maio de 2017

_____. Superior Tribunal de Justiça. Recurso em *Habeas-corpus* nº 75.800/PR, da Quinta Turma. **Lex**: informativo 590 de 16 set. 2016.

_____. Superior Tribunal de Justiça. Recurso em *Habeas-corpus* nº 51.531/RO, da Sexta Turma. Recorrente: Leri Souza e Silva. Recorrido: Ministério Público do Estado de Rondônia. Relator: Min. Nefi Cordeiro. Brasília, 19 abr. 2016.

_____. Supremo Tribunal Federal. Reclamação nº 9.428/DF. Reclamante: Estado de São Paulo. Reclamado: Tribunal de Justiça do Distrito Federal e dos Territórios. Relator: Min. Cezar Peluso. Brasília, 10 de dezembro de 2009. **Lex**: DJe número 116 de 25 de jun. 2010.

_____. Supremo Tribunal Federal. *Habeas-corpus* nº 91.867/PA, da Segunda Turma. Paciente: Davi Resende Soares e outro. Impetrante: José Luis Mendes de Oliveira Lima e outro. Relator: Min. Gilmar Mendes. Brasília, 24 de abril de 2012. **Lex**: DJe de 20 de set. 2012.

_____. Supremo Tribunal Federal. Recurso Extraordinário nº 601.314/SP. Recorrente: Marcio Holcman e outros. Recorrido: União. Relator: Min. Edson Fachin. Brasília, 24 de fevereiro de 2016.

_____. Supremo Tribunal Federal. Recurso Extraordinário nº 389.808/PR. Recorrente: G.V.A. Indústria e Comércio S/A. Recorrido: União. Relator: Min. Marco Aurélio de Melo. Brasília, 10 de maio de 2011. **Lex:** DJe de 10 de maio 2011.

_____. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade nº 2.390/DF, do Plenário. Impetrante: Partido Social Liberal. Impetrado: União. Relator: Min. Edson Fachin. Brasília, 17 de fevereiro de 2016.

CÔRTEZ, Pedro Luiz. **Administração de Sistemas de Informação**. São Paulo: Editora Saraiva, 2008.

GOIÁS. Tribunal de Justiça. Habeas Corpus nº 466215-76.2014.8.09.000. Impetrante: Tiago Felipe de Oliveira e outro. Paciente: Valdiney Souza Fidelis. Relator: Des. Luiz Cláudio Veiga Braga. Goiânia, 05 de fev. de 2015. **Lex:** DJe de 06 de fev. 2015.

_____. Tribunal de Justiça. Habeas Corpus nº 191692-09.2016.8.09.000. Impetrante: Fabianny Costa Rodrigues. Paciente: Yan Victor Silva Martins. Relator: Des. Luiz Cláudio Veiga Braga. Goiânia, 06 de jun. de 2016. **Lex:** DJe de 07 de jun. 2016.

KNIJNIK, Danilo. **Temas de direito penal, criminologia e processo penal. A trilogia Olmstead-Katz-Kyllo: o art. 5º da Constituição Federal do Século XXI**. Porto Alegre: Livraria do Advogado, 2014.

LIMA, Renato Brasileiro de. **Legislação Criminal Especial Comentada**. 4. ed. rev., ampl. e atual., Salvador: Editora JusPodivm, 2016.

TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**. 3. ed. rev. ampl. e atual., Salvador: Editora Juspodivm, 2009.