

Tribunal da Relação de Évora
Processo nº 9/20.8GAMTL-A.E1

Relator: FÁTIMA BERNARDES

Sessão: 14 Julho 2020

Votação: UNANIMIDADE

LEI DO CIBERCRIME

LOCALIZAÇÃO CELULAR CONSERVADA

OBTENÇÃO DE PROVA

Sumário

1 - O regime processual da Lei n.º 109/2009 de 15 de Setembro (Lei do Cibercrime) é aplicável à recolha de prova em suporte eletrónico (informático) reportada a todos os dados que não estejam especificamente previstos no artigo 4º, n.º 1, da Lei n.º 32/2008, de 17 de Julho (Lei relativa a conservação de dados gerados ou tratados no contexto oferta de serviços de comunicações electrónicas), sendo que relativamente a estes últimos, o regime estabelecido na Lei n.º 32/2008, constitui um regime especial relativamente ao regime processual geral que consta dos artigos 12º a 17º da Lei n.º 109/2009.

2 - O argumento preponderante para que se considere que o regime processual estabelecido na Lei n.º 32/2008 se trata de um regime especial que se sobrepõe às disposições processuais de carácter geral previstas nos artigos 12º a 17º da Lei n.º 109/2009, é o de na definição do âmbito de aplicação das disposições processuais previstas nesta última Lei existir a expressa ressalva, no n.º 2 do artigo 11º, a que essas disposições “não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho.”

3 - Assim, à obtenção de prova reportada aos “dados conservados” previstos no artigo 4º, n.º 1, da Lei n.º 32/2008, entre os quais aos relativos à “localização celular conservada” (al. f) do n.º 1 do artigo 4º), aplica-se o regime constante dessa Lei, designadamente, os seus artigos 3º e 9º, exigindo-se que esteja em causa um crime que se integre na categoria de “crimes graves” (n.º 1 do artigo 3º), definida na al. g) do n.º 2 do artigo 2º e que seja dirigido contra pessoa(s) de entre as previstas no n.º 3 do artigo 9º.

4 - Daí que a obtenção de dados de localização celular e de registos de

realização de conversações ou comunicações conservados, não deve ser autorizada quando reportada a um número indeterminado de pessoas incertas, exigindo-se que se tratem de pessoas identificáveis ou determináveis.

Texto Integral

Acordam, em conferência, na Secção Criminal do Tribunal da Relação de Évora:

1 - RELATÓRIO

1.1. Nos autos de Inquérito n.º 9/20.8GAMTL, que correm termos nos Serviços do Ministério Público junto do Tribunal Judicial da Comarca de Beja, por despacho proferido pela Sr.ª JIC, de 02/03/2020, foi indeferido o requerimento do Ministério Público de obtenção de dados de localização celular.

1.2. Inconformado com o assim decidido, o Ministério Público interpôs recurso, apresentando a correspondente motivação, da qual extraiu as seguintes conclusões:

«A. O Ministério Público, acolhendo a sugestão trazida aos autos pela GNR, e com vista a viabilizar a recolha de prova da prática do crime de furto qualificado, p. e p. pelo 203.º, n.º 1, 204.º, n.º 1, alínea a), n.º 2, alínea e), do Código Penal, apresentou os autos ao Mmo. Juiz de Instrução promovendo se ordenasse às operadoras telefónicas nacionais (MEO, Vodafone e Optimus) a junção a estes autos dos dados de tráfego, nomeadamente, todos os números de cartões, de IMEI que activaram as células BTS, incluindo chamadas e mensagens recebidas e efectuadas, hora e duração das comunicações e os denominados eventos de rede, nos termos do nosso despacho de fls. 46 a 49, o qual se dá por integralmente reproduzido para todos os efeitos legais.

B. Fundamentou o seu pedido no disposto nos artigos 11.º alínea c) e 17.º da Lei 109/2009 de 15 de Setembro (Lei do Cibercrime).

C. O Mm.º. Juiz de Instrução indeferiu a pretensão do Ministério Público, por despacho do seguinte teor:

“No requerimento que antecede, o Ministério Público veio expor e requerer o seguinte:

«Os presentes autos tiveram origem no auto de notícia de fls. 3, onde se reportam factos susceptíveis de integrar o crime de furto qualificado, previsto e punido pelos arts. 203.º e 204.º n.º 2 alínea e) do Código Penal.

Concretizando:

- Nestes autos investigam-se factos suscetíveis de consubstanciar, em

abstrato, a prática de um crime de furto qualificado, ocorrido numa habitação, em (...), entre as (...) do dia (...) e as (...) do dia (...).

*- Dos autos resulta indiciado que desconhecidos, acederam ao interior da residência e daí recolheram **e fizeram seus: (...)**;*

Atenta a matéria carreada para os autos, as diligências realizadas não levaram à obtenção de elementos que, por si só, nos permitam identificar os autores do crime investigado nos presentes autos, porquanto:

- Dos factos não existem testemunhas;

- As inspeções lofoscópicas ao local do furto resultaram negativas;

Considerando que a investigação tem por objeto um crime de elevada gravidade que assume preocupação comunitária;

É de presumir, com elevada probabilidade, que os autores possam ter atuado utilizando telemóveis para comunicar entre si, momentos antes e depois dos factos que deram origem aos presentes autos.

Atenta a escassez de meios de prova, é absolutamente fundamental solicitar aos três Operadores Móveis - MEO, VODAFONE e NOS:

- Listagens em suporte digital de dados de tráfego que contenham todos os números de cartões e de IMEI que ativaram as células BTS abaixo identificadas, incluindo chamadas e mensagens recebidas e efetuadas, hora e duração das comunicações e os denominados eventos de rede, correspondentes ao local abaixo assinalados e respetivos períodos temporais.»

Após o Digno Magistrado do Ministério Público descreveu as células BTS em causa em número total de 15 (quinze) e invocou o preceituado nos arts.^o 11 alínea c) e 17.^o da Lei do Cibercrime (sic).

Cumpra apreciar e decidir.

Conforme é entendimento jurisprudencial maioritário:

«Solicitar a operadoras de telemóveis todos os dados de tráfego dos cartões SIM que operaram num determinado período de tempo em 19 antenas, mas não estando concretizados alvos determináveis e atingindo a diligência pretendida um universo ilimitado e indiferenciado de cidadãos que não se integram no conceito jurídico-penal de suspeitos é proibido por lei e não respeita os princípios constitucionais da proporcionalidade e da adequação» - conf. Acórdão do Tribunal da Relação de Lisboa de 22.06.2016, citado no site da pgdl, sendo nosso o destaque a negrito.

« Não é permitido, em inquérito, solicitar às operadoras de comunicações que forneçam todos os números de telefone que num determinado período de tempo, se conectaram a uma determinada antena, sem que, previamente, se determinem previamente os suspeitos o que, em caso de desconhecimento da respetiva identificação, pressupõe a existência de dados factuais tendentes à sua individualização, não sendo admissível que sejam consideradas suspeitas

de determinada ação criminosa, todas as pessoas que se encontrassem naquele local e tempo» - vide Acórdão do Tribunal da Relação de Lisboa de 03.05.2016, citado no site da pgdl, sendo nosso o destaque a negrito.

«A falta de suspeito ou suspeitos determinados contra quem dirigir as escutas telefónicas, os pedidos de obtenção de dados de tráfego ou os pedidos de localização celular, é obstáculo intransponível á realização deste tipo de meios de obtenção de prova. II - Recolher informações de pessoas inocentes, na esperança de, de entre estas, se «apanhar» algum suspeito, é desproporcional aos fins visados, sendo, pois, uma compressão inconstitucional e ilícita do direito á privacidade e á inviolabilidade das comunicações» - vide, Acórdão do Tribunal da Relação de Évora de 19.05.2015, disponível na base de dados da DGSJ, sendo nosso o destaque a negrito e a jurisprudência ali igualmente citada: Ac. da Rel. de Évora de 10/18/2011, proc. n.º 19/11.6GGEVR-A.E1; Ac. da Rel. de Évora de 06/26/2012, proc. n.º 342/11.0JAFAR.E1 e Ac. Rel. de Coimbra de 05/22/2013, proc. n.º 141/12.1GBTCS-A.C1, todos in www.dgsj.pt. Ora, aderindo, in casu, a tal entendimento, importa dizer, igualmente, que o resultado acima aludido, que adviria do acolhimento da promoção que o presente despacho desatende, não pode deixar de ser considerado, no mínimo, como excessivo por confronto com os fins visados, que não podem ser obtidos a todo o custo e com sacrifício injustificado dos direitos de terceiros, representando a decisão que o consentisse uma clara violação do princípio da proporcionalidade, o que a feriria de ilegalidade. Além de que subsistem sérias dúvidas de que a diligências pretendidas vissem a lograr a obtenção dos resultados pretendidos, mormente, a identificação dos agentes dos crimes. Pelo exposto, sem necessidade de outras considerações, por escusadas, indefiro o pelo Ministério Público requerido.

Notifique.

Devolvam-se os autos ao Ministério Público.”

D. É desde despacho e que o Ministério Público recorre, por considerar ser o mesmo ilegal, por ser nulo e consubstanciar uma errada interpretação dos artigos 3.º 9.º e 11.º alínea c) da Lei 109/2009 de 15 de Setembro.

E. O despacho de indeferimento proferido pelo Mmº. Juiz de Instrução não analisa qualquer questão nem de facto nem de direito, não invoca qualquer normativo legal para o indeferimento, limita-se, singelamente, a transcrever jurisprudência, pelo que nem tão pouco se compreende qual o motivo da rejeição do requerimento.

F. Mas mais, num pedido exatamente idêntico, com o mesmo enquadramento legal, e relativamente ao mesmo tipo de crime, o mesmo Mmº. Juiz de Instrução, no mesmo Tribunal, decidiu em sentido contrário no âmbito do

despacho que proferiu no inquérito 556/19.4PBBJA (fls. 57 e seguintes) e, apenas uns dias antes do despacho proferido nestes autos.

G. Daí que, mais uma vez, não se compreenda o sentido da decisão aqui proferida, até porque o despacho ora em crise não a explica.

H. Resulta assim evidente que o despacho de que se recorre é nulo, nos termos do art.º 32.º n.º 1 da Constituição da República Portuguesa, e do art.º 97.º n.º 5 do C.P.P.

I. Será por o Mmo. Juiz entender que não há suspeitos nos autos? Não sabemos.

J. Mas se assim for, na consideração de que, nos termos do disposto no artigo 189º, n.º 2 do CPP, os elementos solicitados pelo MP só poderiam ser fornecidos quanto às pessoas mencionadas no n.º 4 do artigo 187º, do CPP, relevando, no caso dos autos a apreciação da alínea a), na parte em que se refere ao suspeito, uma vez que não existem arguidos constituídos nos autos.

K. Não poderíamos concordar com tal interpretação, por introduzir um grau de exigência na definição de suspeito que extravasa a definição legal, pressupõe uma exigência de concretização de características do suspeito que não se encontra legalmente prevista e cujos contornos não são definidos, e se traduz, na prática, num entrave ao exercício da acção penal pelo Ministério Público.

L. Nos termos do artigo 1º alínea e) do CPP, é suspeito “toda a pessoa relativamente à qual exista indício de que cometeu ou se prepara para cometer um crime, ou que nele participou ou se prepara para participar.”

M. Ora, a lei não exige que o suspeito seja pessoa identificada.

N. O conceito legal de suspeito basta-se com a existência de uma pessoa, responsável pelos seus actos, sobre a qual exista indício de que cometeu ou se prepara para cometer um crime ou nele participar. Centrando-nos na questão da definição do agente (e não do facto em si), isto permite, desde logo, afastar as demais pessoas relativamente às quais não seja possível imputar os factos a qualquer dos títulos previstos no artigo 26º a 28º do Código Penal. Por exemplo, à luz destas normas legais não se permite o fornecimento dos elementos pretendidos tendo em vista identificar as pessoas que se encontravam num local do crime, que se sabe não o terem praticado, mas que porventura o possam ter visto e possam ser testemunhas dos factos.

O. Ora o que se pretende no caso dos autos são indubitavelmente dados relativos aos suspeitos da prática do crime, visando, através deles, a sua identificação.

P. É que a diligência solicitada, como é sugerida pela GNR apenas nos dará os números de telefone que activaram as células naquela noite, de quem tenha estado naquele local ermo onde se situa a habitação.

Q. Em termos de probabilidade, parece-nos evidente que só os autores dos factos terão estado naquele local erno naquele período temporal.

R. Como bem se aponta no Acórdão do Tribunal da Relação do Porto de 26 de setembro de 2018, disponível em www.dgsi.pt, num caso muito parecido a este: “... a doutrina e jurisprudência têm sustentado o entendimento de que não será necessário conhecer os dados de identificação civil da pessoa visada mas terá, pelo menos, que ser uma pessoa concreta, passível de individualização. Quer dizer, não se exigindo a determinação da pessoa impõe-se que seja determinável”

Daqui decorre que uma coisa é um processo correr termos contra incertos e coisa diversa é o mesmo conter já algum suspeito ou suspeitos que carecem apenas de ser identificados.

É certo que a diligência que se pretende vai abranger outras pessoas que pudessem estar presentes nas imediações, mas a mesma não é direcionada para essas pessoas, mas apenas para o suspeito já existente, cuja conduta é circunscrita a uma específica hora e local e, ademais, correlacionada com o seu indiciado e específico comportamento, o que, logicamente, vai conduzir ao natural afastamento de quem assuma condutas perfeitamente distintas, já que inseridas numa normalidade vivencial que as destrinça, ao que acresce o facto de não estar aqui em causa a determinação dos suspeitos do crime, mas apenas qual o número de telefone e IMEI do suspeito já determinado, mas ainda não concretamente identificado.

E aqui, e tal como anotava o recorrente, é bom relembrar que as informações recolhidas que nos afastem do referenciado suspeito deverão ser eliminadas, tal como sucede com a não transcrição de escutas que nenhum interesse revelem para a descoberta da verdade, ou porque os visados nada tenham que ver com a matéria em investigação, ou porque, mesmo no casos de os visados serem suspeitos ou até já arguidos, respeitam a assuntos das suas vidas privadas em nada interferentes ou relacionados com o objeto da investigação. Sem esquecer, obviamente, como também alega o recorrente, que em boa parte das escutas apenas se conhece um número de telefone e/ou a alcunha de alguém alegadamente suspeito da prática de um crime e tal não obsta a que se proceda à interceção de comunicações, devendo relembrar-se ainda que nesta não é apenas escutado o visado, mas todas as pessoas para quem o mesmo telefone ou as que também lhe telefonem, logo, um conjunto indeterminado de possíveis sujeitos sem uma qualquer relação com o suposto crime.

Assim sendo, e dado o completo paralelismo, limitar-nos-emos a aderir a um recente acórdão proferido neste tribunal, no qual se sustentou que “Esta diligência de prova não é lícita apenas para verificar a localização celular ou a realização de comunicações telefónicas por suspeitos cujo número de

telemóvel e/ou IMEI se encontra já determinado. Ela também pode ser realizada para apurar o número de telefone e/ou IMEI de suspeitos já determinados mas cuja identificação completa ainda não é conhecida. O que releva para o efeito da verificação do requisito do artigo 187º n.º 4 al. a) é que o meio de prova vise diretamente a obtenção de dados sobre a pessoa suspeita e não sobre um conjunto de pessoas indeterminadas. No caso em apreço é evidente que a investigação não está direccionada para todas as pessoas que estiveram no local à hora do rebentamento da caixa ATM, mas sim para aqueles quatro ou cinco indivíduos já determinados e suspeitos do crime”.

S. Daqui decorre que, efectivamente, o que se pretende nos autos é conhecer os dados relativos às comunicações entre os agentes do crime, ou seja, as pessoas que praticaram os factos sob investigação.

T. As informações solicitadas afiguram-se, pois, como a única forma viável à investigação de proceder à identificação dos suspeitos, tal como sucede nos casos de furtos de ATM nos quais a jurisprudência tem entendido ser de fornecer os dados uma vez que sem os mesmos não haverá possibilidade de identificar os agentes do crime, que são crimes graves e de grande alarme social.

U. Como já se disse, não é exigência legal da definição de suspeito que se trate de pessoa identificada.

V. A diferença entre poderem ou não poderem ser fornecidos os elementos solicitados à investigação não pode estar dependente da enumeração de características indeterminadas do sujeito, indefinidas e não concretizadas, e cuja exigência jurisprudencial vai além daquilo que foi plasmado na norma legal.

W. Os elementos solicitados pelo Ministério Público são essenciais à investigação, visam identificar os autores do crime, e o seu fornecimento aos autos encontra-se legalmente previsto.

X. O indeferimento da pretensão do Ministério Público com base na ausência de elementos que permitam indicar quem são os autores do crime constitui um contra-senso face às finalidades da investigação (art. 262.º, n.º 1, do CPP).

Y. Ao recusar o fornecimento dos dados solicitados com os fundamentos plasmados no despacho recorrido, o Mmo. Juiz laborou num ciclo vicioso, susceptível de paralisar a investigação criminal, e de despojar o Ministério Público de ferramentas que lhe permitam cumprir o dever de exercício da acção penal, com assento constitucional no artigo 219º, n.º 1, assim assumindo uma interpretação da norma penal susceptível de por em causa o texto constitucional.

Z. Os elementos solicitados pelo Ministério Público foram-no no âmbito da Lei do Cibercrime (Lei 109/2009 de 15 de Setembro), designadamente no art.º

11.º alínea c) e 17.º desse diploma legal, por estar em causa, apenas, a pesquisa em sistema informático de dados armazenados (dados conservados) e não “intercepções telefónicas”.

AA. De facto os dados que se pretende aceder, e independentemente de autorização judicial ou não, dados relativos a localização celular e comunicações estabelecidas mediante o accionamento de antenas BTS são sempre armazenados em ficheiro informático, o qual agora se pretende aceder.

BB. Conforme e se referiu no Acórdão do Tribunal da Relação de Évora de 6 de Janeiro de 2015, *“O regime processual da Lei 32/2008 (designadamente o Artigo 3º, nº 1 e 2 e o Artigo 9º) está revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no Artigo 4º, nº 1 daquela lei, ou seja, dados conservados em geral; está em vigor para todos os dados que estejam especificamente previstos naquele Artigo 4º, nº 1 (por exemplo para dados conservados relativos à localização celular).”*

CC. Ora é precisamente o caso dos autos uma vez que o que se pretende é a pesquisa e recolha para prova de dados já produzidos.

DD. O Ministério Público pretende aceder a “localização celular conservada” em determinado sistema informático, previsto no art.º 17.º da Lei do Cibercrime pelo que o único requisito para aceder aos mesmos são os previstos no art.º 11.º do mesmo diploma, *in casu*, a invocada alínea c) do art.º 11.º, sem qualquer necessidade de recurso aos catálogos de crimes previstos quer no art.º 2.º e 9.º da Lei 32/2008 de 17 de Julho, quer ao catálogo previsto no art.º 187.º do Código de Processo Penal, aplicável *ex vi* art.º 189.º também do Código de Processo Penal.

EE. Aliás, é esse o entendimento do Venerando Tribunal da Relação de Évora, no Acórdão de 20 de Janeiro de 2015,

FF. Em face do exposto, deve o despacho recorrido ser revogado e substituído por outro que entenda estarem verificados, nos autos, os requisitos plasmados nos 11.º n.º 1 alínea c) e 17.º da Lei 109/2009 de 15 de Setembro, considerando que os dados pretendidos se reportam aos suspeitos da prática do crime, e em consequência, deferindo o requerimento do Ministério Público no sentido de ser ordenado às operadoras telefónicas nacionais (MEO, Vodafone e Optimus) a entrega a estes autos dos dados de tráfego, nomeadamente, todos os números de cartões, de IMEI que activaram as células BTS, incluindo chamadas e mensagens recebidas e efectuadas, hora e duração das comunicações e os denominados eventos de rede, nos exctos termos peticionados pelo Ministério Público no despacho de fls.

Assim se fazendo a costumada JUSTIÇA!»

1.3. O recurso foi regularmente admitido, tendo o Sr. Juiz *a quo* proferido despacho de sustentação da decisão recorrida.

1.4. Neste Tribunal da Relação, o Exm.^o Procurador-Geral Adjunto emitiu parecer no sentido de dever ser dado provimento ao recurso.

1.5. Efetuado exame preliminar e colhidos os vistos, vieram os autos à conferência, cumprindo agora apreciar e decidir.

2 - FUNDAMENTAÇÃO

2.1. Delimitação do objeto do recurso

É consabido que as conclusões da motivação do recurso balizam ou delimitam o respetivo objeto – cf. artigos 402º, 403º e 412º, todos do C.P.P. –, sem prejuízo do conhecimento dos vícios e nulidades principais, como tal tipificadas na lei, de conhecimento oficioso.

No caso vertente, atentas as conclusões extraídas pelo recorrente da motivação de recurso apresentada, a questão suscitada é a de saber se estão verificados os necessários requisitos ou pressupostos para que seja deferida a promoção do Ministério Público no sentido de que sejam solicitados às operadoras MEO, Vodafone e Optimus, com referência ao período temporal situado entre as 07h:30m do dia 21/01/2020 e as 07h:00m do dia 22/01/2020 e às quinze células BTS identificadas, os dados de tráfego e de localização celular pretendidos.

Para que possamos apreciar a enunciada questão, importa ter presente o teor do despacho recorrido, que se passa a transcrever:

2.2. Despacho recorrido

«No requerimento que antecede, o Ministério Público veio expor e requerer o seguinte:

«Os presentes autos tiveram origem no auto de notícia de f1s. 3, onde se reportam factos susceptíveis de integrar o crime de furto qualificado, previsto e punido pelos arts. 203.º e 204.º n.º 2 alínea e) do Código Penal.

Concretizando:

- Nestes autos investigam-se factos suscetíveis de consubstanciar, em abstrato, a prática de um crime de furto qualificado, ocorrido numa habitação, em (...), entre as (...) do dia (...) e as (...) do dia (...).

- Dos autos resulta indiciado que desconhecidos, acederam ao interior da residência e daí recolheram e fizeram seus: (...);

Atenta a matéria carreada para os autos, as diligências realizadas não levaram à obtenção de elementos que, por si só, nos permitam identificar os autores do crime investigado nos presentes autos, porquanto:

- Dos factos não existem testemunhas;

- As inspeções lofoscópicas ao local do furto resultaram negativas;

Considerando que a investigação tem por objeto um crime de elevada gravidade que assume preocupação comunitária;

É de presumir, com elevada probabilidade, que os autores possam ter atuado utilizando telemóveis para comunicar entre si, momentos antes e depois dos factos que deram origem aos presentes autos.

Atenta a escassez de meios de prova, é absolutamente fundamental solicitar aos três Operadores Móveis - MEO, VODAFONE e NOS:

Listagens em suporte digital de dados de tráfego que contenham todos os números de cartões e de IMEI que ativaram as células BTS abaixo identificadas, incluindo chamadas e mensagens recebidas e efetuadas, hora e duração das comunicações e os denominados eventos de rede, correspondentes ao local abaixo assinalados e respetivos períodos temporais.»

Após o Digno Magistrado do Ministério Público descreveu as células BTS em causa em número total de 15 (quinze) e invocou o preceituado nos arts.º 11 alínea c) e 17.º da Lei do Cibercrime (sic).

Cumpre apreciar e decidir.

Conforme é entendimento jurisprudencial maioritário:

«Solicitar a operadoras de telemóveis todos os dados de tráfego dos cartões SIM que operaram num determinado período de tempo em 19 antenas, mas não estando concretizados alvos determináveis e atingindo a diligência pretendida um universo ilimitado e indiferenciado de cidadãos que não se integram no conceito jurídico-penal de suspeitos é proibido por lei e não respeita os princípios constitucionais da proporcionalidade e da adequação» - conf. Acórdão do Tribunal da Relação de Lisboa de 22.06.2016, citado no site da pgdl, sendo nosso o destaque a negrito.

«Não é permitido, em inquérito, solicitar às operadoras de comunicações que forneçam todos os números de telefone que num determinado período de tempo, se conectaram a uma determinada antena, sem que, previamente, se determinem previamente os suspeitos o que, em caso de desconhecimento da respetiva identificação, pressupõe a existência de dados factuais tendentes à sua individualização, não sendo admissível que sejam consideradas suspeitas de determinada ação criminosa, todas as pessoas que se encontrassem naquele local e tempo» - vide Acórdão do Tribunal da Relação de Lisboa de 03.05.2016, citado no site da pgdl, sendo nosso o destaque a negrito.

«A falta de suspeito ou suspeitos determinados contra quem dirigir as escutas telefónicas, os pedidos de obtenção de dados de tráfego ou os pedidos de localização celular, é obstáculo intransponível à realização deste tipo de meios de obtenção de prova. " - Recolher informações de pessoas inocentes, na esperança de, de entre estas, se «apanhar» algum suspeito, é desproporcional

aos fins visados, sendo, pois, uma compressão inconstitucional e ilícita do direito à privacidade e à inviolabilidade das comunicações» - vide, Acórdão do Tribunal da Relação de Évora de 19.05.2015, disponível na base de dados da DGSÍ, sendo nosso o destaque a negrito e a jurisprudência ali igualmente citada: Ac. da Rel. de Évora de 10/18/2011, proc. n.º 19/11.6GGEVR-A.E1; Ac. da Rel. de Évora de 06/26/2012, proc. n.º 342/11.0JAFAR.E1 e Ac. Rel. de Coimbra de OS/22/2013, proc. n.º 141/12.1 GBTCS-A.C1, todos in www.dgsi.pt.

Ora, aderindo, *in casu*, a tal entendimento, importa dizer, igualmente, que o resultado acima aludido, que adviria do acolhimento da promoção que o presente despacho desatende, não pode deixar de ser considerado, no mínimo, como excessivo por confronto com os fins visados, que não podem ser obtidos a todo o custo e com sacrifício injustificado dos direitos de terceiros, representando a decisão que o consentisse uma clara violação do princípio da proporcionalidade, o que a feriria de ilegalidade. Além de que subsistem sérias dúvidas de que a diligências pretendidas vissem a lograr a obtenção dos resultados pretendidos, mormente, a identificação dos agentes dos crimes. Pelo exposto, sem necessidade de outras considerações, por escusadas, indefiro o pelo Ministério Público requerido.

Notifique.

Devolvam-se os autos ao Ministério Público.»

2.3. Apreciação do recurso

Tal como já referimos a questão suscitada e que há que decidir nos presentes autos é a de saber se estão verificados os necessários requisitos ou pressupostos para que seja deferida a promoção do Ministério Público no sentido de serem solicitados às operadoras MEO, Vodafone e Optimus, com referência ao período temporal situado entre as (...) do dia (...) e as (...) do dia (...) e às quinze células BTS identificadas na promoção, os dados de tráfego pretendidos, reportados a todos os números de cartões e de IMEI que ativaram as células BTS identificadas, incluindo chamadas e mensagens recebidas e efetuadas, hora e duração das comunicações e os denominados eventos de rede.

No despacho recorrido foi indeferida a indicada promoção do Ministério Público, com fundamento em que a falta de suspeito(s) determinado(s) contra quem dirigir os pedidos de obtenção de dados de tráfego ou os pedidos de localização celular, é obstáculo intransponível à realização deste tipo de meios de obtenção de prova e ter-se-á de considerar, no mínimo, como excessivo, por confronto com os fins visados, violando a decisão que o consentisse o princípio da proporcionalidade, o que a feriria de ilegalidade, além de que, no caso,

subsistem sérias dúvidas de que a diligências pretendidas vissem a lograr a obtenção dos resultados pretendidos, mormente, a identificação dos agentes do crime em investigação.

O Ministério Público, recorrente, insurge-se contra esta decisão de indeferimento, que entende ser ilegal, por violação do disposto no artigo 11º, al. c) e 17º, ambos da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), defendendo estarem reunidos, no caso, os requisitos plasmados naqueles dois preceitos legais. Sustenta o Ministério Público que os dados pretendidos se reportam aos suspeitos da prática do crime, quais sejam as pessoas que praticaram os factos sob investigação, não sendo exigência legal da definição de suspeito que se trate de pessoa identificada, nem estando dependente da enumeração de características indeterminadas do sujeito, indefinidas e não concretizadas, e cuja exigência jurisprudencial vai além daquilo que foi plasmado na norma legal.

O Exm.º PGA no parecer emitido pronunciou-se no sentido de que estando em causa a investigação de crime não enquadrável no conceito de crimes graves, previstos no artigo 2º, n.º 1, al. g) da Lei n.º 32/2008, de 17 de julho, mas sendo pretendidos dados de tráfego conservados definidos no artigo 2º, al. c) da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), pode a autoridade judiciária competente, tendo em vista a descoberta da verdade, solicitar que sejam disponibilizados tais dados, ao abrigo do disposto nos artigos 11º, n.º 1, alínea c) e 14º, n.º 1, ambos da Lei n.º 109/2009, pelo que, na ponderação do conflito de interesses ou valores dignos de proteção do ordenamento jurídico, por um lado a necessidade de perseguir criminalmente os autores do crime e, por outro lado, a proteção dos cidadãos na sua privacidade, que não deve ser devassada sem, motivo justificativo sério e grave, no caso concreto, este último deve soçobrar perante o primeiro que se lhe sobrepõe e, como tal, deverá o recurso interposto pelo MP ser julgado procedente, com as consequências daí decorrentes.

Vejamos:

Nos autos de inquérito de que se trata, está em investigação um crime de furto qualificado p. e p. pelos artigos 203º, n.º 1 e 204º, n.º 2, al. e), ambos do Código Penal.

Os dados de tráfego e de localização celular que o Ministério Público promoveu fossem solicitados às operadoras MEO, Vodafone e Optimus - com referência ao período temporal situado entre as (...) do dia (...) e as (...) do dia (...) e às quinze células BTS identificadas na promoção, os dados de tráfego reportados a todos os números de cartões e de IMEI que ativaram as células BTS identificadas na promoção, incluindo chamadas e mensagens recebidas e efetuadas, hora e duração das comunicações e os denominados eventos de

rede – reconduzem-se a prova eletrónica preservada ou conservada, em sistemas informáticos.

O regime processual da recolha de “prova eletrónica” preservada ou conservada, é regulado pela Lei n.º 32/2008, de 17 de julho (diploma que transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações [1]) e pela Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime), tendo deixado de ter aplicação, nesse domínio, o regime das comunicações telefónicas, previsto nos artigos 187º a 190º do Código de Processo Penal. A delimitação do âmbito de aplicação da Lei n.º 32/2008 e da Lei n.º 109/2009, tem gerado controvérsia, na doutrina e na jurisprudência, acolhendo-se o entendimento que vem sendo majoritariamente defendido [2], de que as enunciadas Leis se complementam, cabendo ao intérprete delimitar os âmbitos de aplicação em campos sobrepostos, mas contíguos [3].

E dando um contributo de grande relevância na delimitação do âmbito de aplicação, das enunciadas Leis n.º 32/2008 e n.º 109/2009, surgiu o Acórdão deste Tribunal da Relação de Évora, de 20/01/2015 [4], cujo sumário se passa a transcrever, na parte que releva para a questão que está em causa nos presentes autos:

«(...)

3 - Para a prova electrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face à prova por “localização celular conservada”.

4 - Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11º a 17º e o regime dos artigos 18º e 19º do mesmo diploma. O regime processual dos artigos 11º a 17º surge como o regime processual “geral” do cibercrime e da prova electrónica. Isto porquanto existe um segundo catálogo na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. (...).

5 - As normas contidas nos artigos 12º a 17º da supramencionada Lei contêm um completo regime processual penal para os crimes que, nos termos das alíneas do n. 1 do artigo 11º, estão (a) previstos na lei nº 109/2009, (b) são ou foram cometidos por meio de um sistema informático ou (c) em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico.

6 - A diferenciação de regimes assenta na circunstância de os dados preservados nos termos dos artigos 12º a 17º se referirem à pesquisa e recolha, para prova, de dados já produzidos mas preservados, armazenados, enquanto o artigo 18º do diploma se refere à interceptação de comunicações electrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático.

7 - (...)

8 - Tratando-se de obter prova por “localização celular conservada”, isto é, a obtenção dos dados previstos no artigo 4º, n. 1 da Lei 32/2008, de 17-07, o regime processual aplicável assume especialidade nos artigos 3º e 9º desta lei.

9 - Em suma, numa interpretação conjugada das Leis 32/2008, 109/2009 e da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa (aprovada pela Resolução da Assembleia da República nº 88/2009, publicada no DR de 15-09-2009), devem ter-se em consideração os seguintes catálogos de crimes quanto a dados preservados ou conservados:

- o catálogo de crimes do n. 1 do artigo 11º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11º a 17º dessa Lei;
- o catálogo de crimes do n. 1 do artigo 18º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei aos crimes previstos na al. a) do artigo 18º;
- o catálogo de crimes do n. 1 do artigo 187º do Código de Processo Penal, por remissão expressa da Lei 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei para os crimes previstos na al. b) do artigo 18º;
- o catálogo de crimes (“crimes graves”) do artigo 3º da Lei nº 32/2008 quanto a especiais “dados conservados” (localização celular), como requisito de aplicação dos artigos 3º e 9º da Lei nº 32/2008.

10 - O artigo 189º do Código de Processo Penal nunca é aplicável a crimes informáticos, seja qual for o catálogo aplicável.

11 - O objecto de ambas as leis – de 2008 e 2009 – é parcialmente coincidente. Ambas se referem e regulam “dados conservados” (Lei nº 32/2008) e “dados preservados” (Lei nº 109/2009) ou seja, depositados, armazenados, arquivados, guardados. A Lei de 2009 assume um carácter geral no seu âmbito de aplicação, não distinguindo dados arquivados pela sua natureza, o que abrange todos eles, portanto (à excepção do correio electrónico, especificamente previsto no seu artigo 17º).

12 - O regime processual da Lei nº 32/2008 constitui relativamente aos dados “conservados” que prevê no seu artigo 4º, um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11º a 19º da Lei nº 109/2009.

13 - Consequentemente devemos concluir que o regime processual da Lei 32/2008, designadamente o artigo 3º, nº 1 e 2 e o artigo 9º:

- mostra-se revogado e substituído pelo regime processual contido na Lei nº 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008 ou seja, dados conservados em geral;
- revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4º, n. 1 da Lei nº 32/2008, isto é, para os dados conservados relativos à localização celular. Só para este último caso ganha relevo o conceito de “crime grave”.»

Em conformidade com esta orientação, que vem sendo acolhida pela jurisprudência maioritária e que se sufraga, o regime processual da Lei n.º 109/2009 é aplicável à recolha de prova em suporte eletrónico (informático) reportada a todos os dados que não estejam especificamente previstos no artigo 4º, n.º 1, da Lei n.º 32/2008, de 17 de julho^[5], sendo que relativamente a estes últimos, o regime estabelecido na Lei n.º 32/2008, constitui um regime especial relativamente ao regime processual geral que consta dos artigos 12º a 17º da Lei n.º 109/2009.

Dito de outro modo, como se refere no Acórdão desta Relação, de 25/10/2016^[6] «A Lei nº 32/2008 tem um regime processual “privativo” da matéria por si regulada, assente na existência de “dados conservados”, nos termos do artigo 4º, n.º 1 pelos fornecedores de serviços.»

O argumento preponderante para que se considere que o regime processual estabelecido na Lei n.º 32/2008 se trata de um regime especial que se sobrepõe às disposições processuais de carácter geral previstas nos artigos 12º a 17º da Lei n.º 109/2009, é o de na definição do âmbito de aplicação das disposições processuais previstas nesta última Lei existir a expressa ressalva, no n.º 2 do artigo 11º, a que essas disposições “*não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho.*”

As disposições processuais contidas no Capítulo III da Lei n.º 109/2009, artigos 12º a 17º, tal como resulta do n.º 1 do artigo 11º, aplicam-se aos crimes nela previstos (nos artigos 3º a 8º, quais sejam, os crimes de falsidade informática, de dano relativo a programa ou outros dados informáticos, de sabotagem informática, de acesso ilegítimo, de interceção ilegítima e de reprodução ilegítima de programa protegido), aos crimes cometidos por meio de um sistema informático e, ainda, aos crimes em que seja necessário proceder à recolha de prova em suporte eletrónico. Em relação a estes últimos crimes, a que alude a al. c) do n.º 1 do artigo 11º da Lei n.º 109/2009, ainda que o âmbito de aplicação abranja qualquer crime tipificado na lei em que se revela necessário para a sua investigação a recolha da prova digital, a interpretação e a aplicação dessa norma, não pode, salvo o devido respeito

pela opinião contrária, levar a “contornar” a norma-catálogo, obrigatória e imperativa, prevista no artigo 3º da Lei n.º 32/2008, «com o recurso a mecanismos de outro diploma, pensado para tutelar situações diversas, e criar assim uma via verde para virtualmente todos os delitos, ponderada judicialmente a respetiva proporcionalidade, virem a poder beneficiar do mecanismo de exceção lesivo do direito fundamental»^[7] à inviolabilidade das telecomunicações, consagrado no artigo 34º, n.º 4, da CRP, como é o mecanismo da obtenção/transmissão de dados de tráfego e de localização celular, conservados.

Por conseguinte, considerando que as disposições processuais gerais previstas na Lei n.º 109/2009, regulam a obtenção de prova através da pesquisa de dados informáticos (artigo 15º); da apreensão de dados informáticos (artigo 16º) e da apreensão de correio eletrónico e de registos de comunicações de natureza semelhante (artigo 17º) [ainda que o conceito de registo de comunicações de natureza semelhante ao correio eletrónico não seja isento de dúvidas^[8], tratando-se de comunicações que podem ser feitas através de serviço telefónico ou através da internet, abrangendo as SMS, as MMS – serviço de mensagens, respetivamente, curtas e desenvolvido –, as MMS – serviço de mensagens multimédia –, as conversações no Messenger, as mensagens de voz relativas a comunicações ou arquivos de som e/ou imagem via Whatsapp, Viber, Skype, Facebook, etc.], entendemos a obtenção de dados de tráfego, cuja definição consta da al. g) do artigo 2º da Lei n.º 109/2009^[9], abrangendo os dados conservados ou armazenados em sistemas informáticos (cf. v.g. artigo 14º, n.º 1 do mesmo diploma legal), neles não se incluindo os dados previstos no artigo 4º, n.º 1, da Lei n.º 32/2008, designadamente, os dados referentes à localização celular preservada.

Importa referir que o regime processual que consta do artigo 18º (“Interceção de Comunicações”) da Lei n.º 109/2009, que prevê a recolha de dados de tráfego, abrangendo a localização celular, respeita a interceções de comunicações, em tempo real, que não cabe aqui considerar.

Assim, em nosso entender, à obtenção de prova reportada aos “dados conservados” previstos no artigo 4º, n.º 1, da Lei n.º 32/2008, entre os quais aos relativos à “localização celular conservada” (al. f) do n.º 1 do artigo 4º), aplica-se o regime constante dessa Lei, designadamente, os seus artigos 3º e 9º^[10].

De harmonia com o disposto no artigo 3º, n.º 1, da Lei n.º 32/2008, «A conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes».

E estatui o artigo 9º - *Transmissão dos dados* - da Lei 32/2008:

«1 - A transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada, por despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, detecção e repressão de crimes graves.

2 - A autorização prevista no número anterior só pode ser requerida pelo Ministério Público ou pela autoridade de polícia criminal competente.

3 - Só pode ser autorizada a transmissão de dados relativos:

a) Ao suspeito ou arguido;

b) A pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou

c) A vítima de crime, mediante o respectivo consentimento, efectivo ou presumido.

4 - A decisão judicial de transmitir os dados deve respeitar os princípios da adequação, necessidade e proporcionalidade, designadamente no que se refere à definição das categorias de dados a transmitir e das autoridades competentes com acesso aos dados e à protecção do segredo profissional, nos termos legalmente previstos.

5 - O disposto nos números anteriores não prejudica a obtenção de dados sobre a localização celular necessários para afastar perigo para a vida ou de ofensa à integridade física grave, nos termos do artigo 252.º-A do Código de Processo Penal.

6 - As entidades referidas no n.º 1 do artigo 4.º devem elaborar registos da extracção dos dados transmitidos às autoridades competentes e enviá-los trimestralmente à CNPD.»

Temos assim, de acordo com o entendimento que se sufraga, que a obtenção de dados conservados que integrem as categorias previstas no artigo 4º, n.º 1, da Lei n.º 32/2008, de 17 de julho, como o são os dados de tráfego (referentes a comunicações telefónicas) e de localização celular que, no caso concreto, o Ministério Público pretende obter, só pode ocorrer se estiverem verificados os seguintes pressupostos:

1º - Ter por finalidade a investigação, detecção e repressão de crimes graves (n.º 1 do artigo 3º da Lei n.º 32/2008), constando a definição de crimes graves, para efeitos, do mesmo diploma legal da al. g) do n.º 1 do artigo 2º, reportando-se a «crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por

convenção sobre a segurança da navegação aérea ou marítima.»

2º - Que esses dados respeitem a pessoas referidas no n.º 3 do artigo 9º, ou seja, a) o suspeito ou arguido; b) a pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou c) a vítima de crime, mediante o respetivo consentimento, efetivo ou presumido.

3º - Que existam razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves (n.º 1 do artigo 9º da Lei n.º 32/2008), isto é, devendo ser respeitados os princípios da adequação, necessidade e proporcionalidade (artigo 9.º, n.ºs 1 e 2).

No caso a que respeitam os presentes autos, o Ministério Público pretende a obtenção, junto das operadoras MEO, Vodafone e Optimus, de dados de tráfego (referentes a comunicações telefónicas) e de localização celular, conservados, que possam conduzir à identificação dos autores dos factos em investigação, suscetíveis de poder integrar a prática de um crime de furto qualificado, p. e p. pelos artigos 203º, n.º 1 e 204º, n.º 2, al. e), ambos do CP, com referência ao local e ao período temporal em que os factos investigados terão ocorrido, dados esses que se integram nas categorias previstas no artigo 4º da Lei n.º 32/2008 e como tal, de acordo com o entendimento que acolhemos, à obtenção/transmissão desses dados é aplicável o regime processual previsto na Lei n.º 32/2008 e não o regime geral previsto na Lei n.º 109/2009, designadamente, no seu artigo 14º, n.º 1^[11].

Sucede que, no caso concreto, não estão reunidos os dois primeiros pressupostos supra enunciados para que seja legalmente permitida a obtenção/transmissão dos pretendidos dados de tráfego e de localização celular conservados.

Com efeito:

Estando em investigação nos autos de inquérito em que o Ministério Público requereu ao JIC que fossem solicitados às operadoras MEO, Vodafone e Optimus, os referenciados dados, factos suscetíveis de integrar um crime de furto qualificado, p. e p. pelos artigos 203º, n.º 1 e 204º, n.º 2, al. e), ambos do Código Penal, este crime não integra a categoria de «crimes graves» definida no n.º 1 do artigo 3º da Lei n.º 32/2008;

Por outro lado, os dados de tráfego e de localização cuja obtenção o Ministério Público pretende não respeitam a qualquer das pessoas referidas no n.º 3 do artigo 9º da Lei n.º 32/2008, não existindo arguido(s) ou sequer suspeito(s) nos autos de inquérito.

E em relação a este último ponto, ainda que não seja inteiramente consensual,

a delimitação do conceito de suspeito para efeitos do disposto na enunciada norma legal, mesmo tendo em conta a definição que consta da al. e) do artigo 1º do CPP – considera-se «Suspeito» toda a pessoa relativamente à qual exista indício de que cometeu ou se prepara para cometer um crime, ou que nele participou ou se prepara para participar” – a jurisprudência converge no sentido de que esse conceito não pode reportar-se a um número indeterminado de pessoas incertas, mas tem de respeitar a pessoas concretas, ainda que não identificadas.

Daí que constitua jurisprudência, que se crê unânime, dos nossos Tribunais Superiores, que a obtenção de dados de localização celular e de registos de realização de conversações ou comunicações não dever ser autorizada quando reportada a um número indeterminado de pessoas incertas, exigindo-se que se tratem de pessoas identificáveis ou determináveis^[12], ou seja, como se refere no Ac. desta Relação de Évora de 03/12/2019^[13] que «se trate de pessoas minimamente “concretizadas” e “contextualizadas”, pessoas de muito provável e previsível identificação, por meio do conhecimento de um mínimo de características que permitam individualizá-las relativamente às demais pessoas que também possam ter estado presentes no local do crime.». Esta última será, por exemplo, a situação em que existindo testemunhas que viram pessoa(s) no local dos factos em investigação, em período temporal compatível com o da respetiva ocorrência, desconhecendo a identificação desses indivíduos ou não conseguindo sequer descrever os seus traços fisionómicos, dão conta de aspetos tais como o número de indivíduos em questão, como se apresentava(m), etc., ou a situação – trazendo à colação o exemplo do rebentamento e furto de máquinas ATM, que é convocado pelo Exm.º PGA, no seu parecer – em que existem imagens de videovigilância recolhidas no local que permitem percecionarmos os indivíduos que praticaram os factos, apresentando-se os mesmos com o rosto encoberto.

Ora, no caso concreto, os dados de tráfego e de localização celular cuja obtenção o Ministério Público pretende não visa suspeito(s), com o alcance e a dimensão da definição supra referidos, visando antes um número indeterminado de pessoas que, no período temporal balizado como o da ocorrência dos factos em investigação estiveram e efetuaram ou receberam comunicações telefónicas (ou participaram em evento de rede) na área de abrangência das 15 células de antenas BTS, indicadas pelo Ministério Público, na expectativa de poder descobrir quem de entre essas pessoas possa ter praticado os factos/crime em investigação, o que não é legalmente permitido, por a obtenção de dados de tráfego e de localização conservados, com essa finalidade, extravasar os apertados limites estabelecidos na Lei n.º 32/2008, para a transmissão de tal tipo dados, não respeitando os princípios jurídico-

constitucionais da adequação e proporcionalidade^[14], a que estão sujeitas as intervenções restritivas dos direitos liberdades e garantias (artigo 18º, n.º 2, da CRP), estando em causa o direito à inviolabilidade das telecomunicações consagrado no artigo 34º, n.º 4, da CRP.

A falta de suspeito(s) determinado(s), nos termos sobreditos, contra quem dirigir os pedidos de obtenção de dados de tráfego ou os pedidos de localização celular conservados «é obstáculo intransponível à realização deste tipo de meios de obtenção de prova»^[15].

Por todo o exposto e em conformidade, entendendo-se não ser aplicável, na situação que está em causa nos autos, o regime processual previsto na Lei n.º 109/2009, de 15 de setembro, designadamente, no seu artigo 17º, mas sim o regime processual estabelecido na Lei n.º 32/2008, de 17 de julho, concluímos não estarem verificados os pressupostos legalmente exigidos, previstos no artigo 3º, n.º 1, com referência à al. g) do artigo 2º e no artigo 9º, n.º 1, al. a), da mesma Lei 32/2008, para que a obtenção/transmissão dos dados de tráfego e localização celular conservada pretendidos pelo Ministério Público.

Bem andou, pois, o Sr. Juiz de Instrução, ao decidir indeferir a promovida obtenção daqueles dados.

O recurso é, por isso, julgado improcedente, mantendo-se a decisão recorrida.

3 - DISPOSITIVO

Nestes termos, em face do exposto, **acordam os Juízes que compõem esta Secção Criminal do Tribunal da Relação de Évora em negar provimento ao recurso** interposto pelo Ministério Público e, em consequência, confirmar o despacho recorrido.

Sem tributação.

Notifique.

Évora, 14 de julho de 2020

[1] Diretiva esta que veio a ser declarada inválida em 8/04/2014 pelo Tribunal de Justiça da União Europeia, tendo vindo a ser entendido que tal decisão não afeta a validade do diploma que transpôs a mesma Diretiva para o direito interno - sobre este assunto vide Ac. da RL de 28/11/2018, proc. n.º 8617/17.8T9LSB-A.L1-3, disponível em www.dgsi.pt.

[2] A tese minoritária, preconizada, entre outros, na doutrina, por Paulo Dá Mesquita, in *Processo Penal, Prova e Sistema Judiciário*, 1ª Edição, 2010, Coimbra Editora, 2010, pág. 123., é no sentido de que a Lei do Cibercrime revogou, no essencial, o regime de acesso aos dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas, previsto na Lei n.º 32/2008, nomeadamente o seu artigo 9º, subsistindo o regime desta Lei apenas «no estabelecimento dos deveres dos fornecedores de serviços de conservação e protecção desses dados, bem como das condições técnicas operativas e destruição desses dados», defendendo ser esse o sentido útil da ressalva feita no n.º 2 do artigo 11º da Lei n.º 109/2009.

[3] Neste sentido, vide, entre outros, na doutrina, Rita Castanheira Neves, “As Ingerências nas Comunicações Electrónicas em Processo Penal – Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova”, Coimbra Editora, 2011, pág. 234.

[4] Proferido no proc. n.º 648/14.6GCFAR-A.E1, relatado pelo Sr. Desemb. João Gomes de Sousa, acessível em www.dgsi.pt.

[5] O enunciado artigo 4º que tem por epígrafe “Categorias de dados a conservar”, dispõe:

1 - Os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar as seguintes categorias de dados:

- a) Dados necessários para encontrar e identificar a fonte de uma comunicação;
- b) Dados necessários para encontrar e identificar o destino de uma comunicação;
- c) Dados necessários para identificar a data, a hora e a duração de uma comunicação;
- d) Dados necessários para identificar o tipo de comunicação;
- e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;
- f) Dados necessários para identificar a localização do equipamento de comunicação móvel.

(...).

7 - Para os efeitos do disposto na alínea f) do n.º 1, os dados necessários para identificar a localização do equipamento de comunicação móvel são os seguintes:

- a) O identificador da célula no início da comunicação;
- b) Os dados que identifiquem a situação geográfica das células, tomando como referência os respectivos identificadores de célula durante o período em que se procede à conservação de dados.»

[6] Proferido no proc. n.º 223/16.0GBLLE.E1, acessível em www.dgsi.pt.

[7] Ac. da RP de 20/11/2010, proc. 54/19.6GDSTS-A.P1, acessível em www.dgsi.pt.

[8] Cf. Rui Cardoso, “A apreensão de mensagens de correio eletrónico e de natureza semelhante”, in *Direito Probatório Substantivo e Processual Penal*, CEJ, 2019, páginas 73 e 74.

[9] Quais sejam «os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente.»

[10] Neste sentido, vide, entre outros, Ac.s da RE de 25/10/2016, proc. 223/16.0GBLLE.E1, de 24/10/2017, proc. 355/16.5GBPSR-A.E1 e de 08/10/2019, proc. 180/19.1GHSTC.E1; Ac.s da RC de 08/11/2017, proc. 380/17.9JACBR.C1 e de 08/11/2017, proc. 380/17.9JACBR.C1; Ac. da RL de 03/5/2016, proc. 73/16.4PFCSC-A.L1-5 e Ac. da RP de 20/11/2019, proc. n.º 54/19.6GDSTS-A.P1, todos acessíveis in www.dgsi.pt.

[11] Preceito legal que tem por epígrafe “Injunção para a apresentação ou concessão do acesso a dados” e que estatui no n.º 1 o seguinte: “Se no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados, armazenados num determinado sistema informático, a autoridade judiciária competente ordena a quem tenha a disponibilidade ou controlo desses dados que os comunique ao processo ou que permita o acesso aos mesmos, sob pena de punição por desobediência.”

[12] Neste sentido, vide, entre muitos outros, Acs. da RE de 30/09/2010, proc. 49/10.5JAFAR-A.E1, de 26/06/2012, proc. 342/11.0JAFAR.E1 e de 19/05/2015, proc. 54/15.5GCBNV-A.E1; Ac.s da RL de 22/06/2016, proc. 48/16.3PBCSC-A.L1-9 e de 03/5/2016, proc. 73/16.4PFCSC-A.L1-5; Ac.s da RC de 10/01/2018, proc. 388/17.4JACBR-A.C1 e de 08/11/2017, proc. 380/17.9JACBR.C1 e Ac. da RP de 11/02/2015, proc. 2063/14.2JAPRT-A.P1, todos acessíveis in www.dgsi.pt.

[13] Proferido no Proc. n.º 199/19.2GAFAL-A.E1, acessível no endereço www.dgsi.pt.

[14] Ac. RC de 10/1/2018, proc. 388/17.4JACBR-A.C1 e Ac. da RE de 19/05/2015, proc. 54/15.5GCBNV-A.E1, acessíveis em www.dgsi.pt

[15] Já citado Ac. da RE de 19/05/2015.