jurisprudência.pt

Tribunal da Relação de Guimarães
Processo nº 743/23.0JAVRL-A.G1

Relator: ISABEL CRISTINA GAIO FERREIRA DE CASTRO
Sessão: 23 Janeiro 2024
Número: RG
Votação: UNANIMIDADE
Meio Processual: RECURSO PENAL
Decisão: IMPROCEDENTE

METADADOS **DADOS DE BASE** **DADOS DE TRÁFEGO**

DADOS DE CONTEÚDO **DADOS DE LOCALIZAÇÃO CELULAR**

Sumário

I- Os dados da faturação detalhada e os dados da localização celular que fornecem a posição geográfica do equipamento móvel com base em atos de comunicação, na medida em que são tratados para permitir a transmissão das comunicações, são dados de tráfego respeitantes às telecomunicações e, portanto, encontram-se abrangidos pela proteção constitucional conferida ao sigilo das telecomunicações.
II- Tem sido entendimento maioritário que, tratando-se de dados de comunicações “conservadas” ou “preservadas”, não é possível aplicar o disposto no artigo 189º do Código de Processo Penal – a extensão do regime das escutas telefónicas – aos casos em que são aplicáveis as Leis n.ºs 32/2008 e 109/2009. Isto é, para a prova de comunicações preservadas ou conservadas 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, com as especificidades supra assinaladas, coadjuvado pelos artigos 3º a 11º da Lei nº 32/2008, se for caso de dados previstos nesta última.
O acórdão do Tribunal Constitucional n.º 268/22, de 19-04, veio declarar a inconstitucionalidade, com força obrigatória geral, de várias normativos da Lei n.º 32/2008, mais concretamente: da norma constante do artigo 4.º da Lei n.º 32/2008, de 17 de julho, conjugada com o artigo 6.º da mesma lei, por violação do disposto nos n.ºs 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo n.º 18.º, todos da Constituição; e da orma do

artigo 9.º da Lei n.º 32/2008, de 17 de julho, relativa à transmissão de dados armazenados às autoridades competentes para investigação, deteção e repressão de crimes graves, na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros, por violação do disposto no n.º 1 do artigo 35.º e do n.º 1 do artigo 20.º, em conjugação com o n.º 2 do artigo 18.º, todos da Constituição.
III- Em causa está a transmissão, por operadoras de serviços de telecomunicações, de dados conservados de tráfego e de localização celular emergentes da detenção e/ou utilização de aparelhos telefónicos, que, segundo o entendimento que sufragamos, é regulada e disciplinada especificamente pela Lei n.º 32/2008.
Contudo, nos presentes autos investigam-se factos suscetíveis de integrar a prática de um crime de incêndio, previsto e punível pelo artigo 274º, n.º 1, do Código Penal, com pena de prisão de 1 a 8 anos.
Ora, tal crime que não integra o catálogo de crimes que preenchem a definição de «crime grave» contemplada no artigo 2º, n.º 1, al. g), da Lei n.º 32/2008, complementada pelo esclarecimento constante do artigo 1º, alíneas i), j) e m) do Código Penal quanto ao que deve entender-se por «terrorismo», «criminalidade violenta» e «criminalidade altamente organizada».
Com efeito, a obtenção de prova de localização celular conservada apenas pode ser admitida quando está em causa crime grave de acordo com a apontada restrita definição, sendo este pressuposto essencial de aplicação da Lei n.º 32/2008.
Como tal, mostra-se inexoravelmente arredada a aplicabilidade da Lei n.º 32/2008 e prejudicada a apreciação dos restantes pressupostos de que depende – nomeadamente a qualidade [processual] da pessoa a que se referem os dados cuja transmissão é pretendida, conforme exige o n.º 3 do artigo 9º [designadamente, o suspeito, previsto na al. a)] e, bem assim, a questão dos efeitos decorrentes da declaração de inconstitucionalidade de alguns dos seus dipositivos nos sobreditos termos.
IV- De igual modo é de excluir a aplicabilidade do regime de extensão previsto nos artigos 189º, n.º 2, e 187º do Código de Processo Penal, porquanto é pedida a obtenção de dados passados conservados, e não de dados futuros ou em tempo real, circunstância que, só por si, perfilhando-se o entendimento supra explanado, a afasta de modo incontornável.
Ainda que assim se não entendesse, pese embora esteja em causa crime incluído no catálogo de crimes elencados no artigo 187º, n.º 1 [mais concretamente, previsto na alínea a) – crimes puníveis com pena de prisão

superior, no seu máximo, a 3 anos], já o mesmo não se verificava quanto ao catálogo de visados discriminados no n.º 4 do mesmo preceito, mormente pessoa com a qualidade processual de suspeito ou arguido [al. a)].
Com efeito, no inquérito ainda nem sequer há suspeitos. O artigo 1º, al. e), do Código de Processo Penal define «suspeito» como sendo "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". Ora, como assertivamente se sustentou na decisão alvo de recurso, tem sido amplamente defendido pela jurisprudência dos Tribunais superiores que se os dados de localização celular que se pretendem obter não têm como alvo um suspeito, mas antes um universo de pessoas não identificadas e unidas apenas pelo simples facto de estarem num dado local num dado momento, não é admissível, pois, além de não respeitar os princípios da proporcionalidade e da adequação, não permitem o enquadramento no conceito jurídico-penal de "suspeito".

Texto Integral

Acordam, em conferência, os Juízes da Secção Penal do Tribunal da Relação de Guimarães:

I. - RELATÓRIO

1. - No processo n.º 743/23...., no Juízo Local Criminal de Vila Real - Juiz ..., do Tribunal Judicial da Comarca de Vila Real, em 24.10.2023 foi proferido ***despacho judicial*** que indeferiu o requerimento do Ministério Público para que se «ordene às operadoras de telecomunicações "EMP01.../EMP02...", EMP03..., "EMP04..." a remessa aos presentes autos, em suporte digital e formato "excel", dos eventos de rede referentes aos códigos de antena indicados a fls. 09 (com a identificação dos titulares dos nºs de telemóvel aí accionados e respectivos IMEIS's e moradas), em virtude dos mesmos terem sido preservados e serem fundamentais para a descoberta da verdade, no período compreendido entre as 17h30 até às 18h30 do dia 28-08-2023.»

2. - Não se conformando com tal decisão, veio o **Ministério Público** interpor recurso, apresentando a respetiva motivação, que finaliza mediante as seguintes conclusões [transcrição[1]]:

«1. Na situação em concreto, tratando-se de dados de tráfego e estando em

causa factos subsumíveis a crime de catálogo do artigo 187°, será sempre o regime do artigo 189.° n.° 2 do Código Processo Penal o aplicável, e não a Lei 32/2008 de 17 de julho;
2. O artigo 189°, n.° 2 do Código Processo Penal não foi revogado pela Lei 32/2008 de 17 de julho, quer de forma expressa, tácita ou sistemática, mantendo-se plenamente em vigor
3. Os dados de tráfego que se pretende obter são conservados por um período de 6 meses (contados, no caso concreto, desde ../../2022) por força dos artigos 6°, n.° 2 da Lei n.° 41/2004 e 10.º da Lei n.° 23/96;
4. A declaração de inconstitucionalidade do Tribunal Constitucional proferida no âmbito do Acórdão do TC n.° 268/2022 não abrangeu este nicho normativo, nem questionou a vigência da Lei n°41/2004;
5. Assim, seria sempre de deferir a obtenção dos dados de tráfego nos termos do art° 189°. n.° 2 do Código Processo Penal (regime aplicável aos autos) e porque esses dados são conservados por força da Lei n.° 41/2004, não revestindo qualquer meio ilícito de obtenção de prova;
6. A Mm.a Juiz do Tribunal de Instrução violou, assim, o disposto nos artigos 125°, 126º, 187º, 189.° e 262°, todos do Código de Processo Penal, e artigos 6°, n.° 2 da Lei n,° 41/2004 e 10.° da Lei n.° 23/96.
7. Os autos indiciam a prática de incêndio florestal, p. e p. nos termos do art.° 274°, n°1 do Código Penal, punido com pena de prisão de 1 a 8 anos, e que, assim, nos termos do artigo 187°, n.° 1, alínea a) do Código de Processo Penal que admitem a realização de intercepções telefónicas;
8. A questão da indispensabilidade da utilização deste meio de prova não pode ser posta em causa, pois trata-se do único modo de obtenção de prova da eventual identificação dos suspeitos e determinação exacta da sua localização :90 local da prática dos factos.
9. Os dados de tráfego e de localização celular só podem ter como visados as pessoas enumeradas no n.° 4 do artigo 187.° do Código de Processo Penal ex vi do n.° 2 do artigo 189.° do mesmo diploma legal: suspeito ou arguido; 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 vítima de crime, mediante o respectivo consentimento efectivo ou presumido:
10. Suspeito é “toda a pessoa relativamente à qual exista indício de que cometeu ou se prepara para cometer um crime, ou nele participa ou se prepara para participar (artigo 1°, alínea e) do Código de Processo Penal);
11. A lei não exige que o suspeito seja pessoa determinada ou identificada. Basta que estejamos perante uma pessoa, um ser humano perante o qual há indícios da prática de um crime (Neste sentido Acórdão da Relação de Lisboa

de 7.11.2007 - Processo n.° 8860/2007-3);
12. In casu, dúvidas não restam que ocorreu crime graves de incêndio florestal, bem planeado e executado, perpetrados por indivíduo(s). Apenas não sabemos a sua identidade.
13. A Mm.ª Juiz de Instrução Criminal interpretou erradamente o conceito de "suspeito", ao exigir que se tenha em vista pessoa concreta.
14. Não exige a lei que se tenha em vista pessoa concreta, na medida em que a autorização judicial requerida refere-se a pessoas concretas e determináveis, sendo os seus traços comuns, para além do facto de terem ocupado, um local em concreto (abrangidos pelas BTS elencadas), no dia dos factos.
15. Não se pretende a obtenção dos vastos elementos detectados pelas BTS mas apenas os números identificados, para que seja efectuada análise das coincidências existentes
16. Com efeito, a diligência probatória requerida pretendia precisamente esse duplo objectivo de localização e identificação. O indeferimento pela Mmª Juiz de Instrução Criminal vai contra as próprias finalidades da investigação, nos termos do disposto no artigo 262°, n° 1, do Código de Processo Penal.
17. A noção de suspeito adoptada pela Mm.ª Juiz de Instrução Criminal não tendo correspondência na lei significa uma limitação excessiva do normativo, levando no seu limite, à ineficácia do meio de prova em causa em todos os casos em que o agente do crime não surge cabalmente identificado (p. ex. constar dos autos a sua identificação civil ou apenas um nome).
18. Não podendo recorrer a este meio de prova toda a investigação é colocada em causa, uma vez que não se afiguram outros meios de prova pelos quais se consiga obter o duplo objectivo de identificação e localização do(s) autor(es) do crime em causa.
Pelo exposto, deve a decisão recorrida ser revogada e substituída por outra que determine o fornecimento de tais informações: apurar, junto dos diversos operadores de comunicações móveis a identificação dos números e aparelhos de telemóveis activados, no período que decorreu as 17h30 até às 18h30 do dia 28-08-2023, nas antenas e células indicadas pela P.J. a fls. 15, conforme disposto no artigo 187° do Código de Processo Penal, fazendo-se, desta forma, JUSTIÇA.»

3. - Neste Tribunal da Relação, a **Ex.ma Procuradora-Geral Adjunta** emitiu fundamentado parecer no sentido de que o recurso não deverá obter provimento.

4. - Colhidos os vistos e realizada a conferência, em consonância com o

estatuído no artigo 419º, n.º 3, al. c), do Código de Processo Penal, cumpre apreciar e decidir.

*

II. – FUNDAMENTAÇÃO

1. - DELIMITAÇÃO DO OBJETO DO RECURSO
Decorre do preceituado no artigo 412º, n.º 1 do Código de Processo Penal que o poder de cognição do tribunal de recurso é delimitado pelas conclusões – deduzidas por artigos –, já que é nelas que o recorrente sintetiza as razões – expostas na motivação – da sua discordância com a decisão recorrida.
Contudo, o tribunal de recurso está, ainda, obrigado a decidir todas as questões de conhecimento oficioso, como é o caso das nulidades insanáveis que afetem o recorrente, nos termos dos artigos 379º, n.º 2, e 410º, n.º 3, do Código de Processo Penal, e dos vícios previstos no artigo 410º, n.º 2, do mesmo diploma, que obstam à apreciação do mérito do recurso, mesmo que este se encontre limitado à matéria de direito [cfr. Acórdão do Plenário das Secções do STJ n.º 7/95, de 19.10.1995, e Acórdão de Uniformização de Jurisprudência n.º 10/2005, de 20.10.2005[2]].
O objeto do recurso e os limites dos poderes de apreciação e decisão do Tribunal Superior são, assim, definidos e delimitados pelas referidas questões, umas, suscitadas pelo recorrente, e, outras, de conhecimento oficioso[3].

Assim, no caso concreto, atentas as conclusões formuladas pelo recorrente, e não se vislumbrando quaisquer (outros) vícios de conhecimento oficioso, a questão a decidir circunscreve-se à ***(in)admissibilidade da transmissão de dados conservados de tráfego e de localização celular.***

2. - INCIDÊNCIAS PROCESSUAIS RELEVANTES [para a apreciação da enunciada questão]:

2.1 - No âmbito do processo [743/23....] de que foi extraída a certidão para instruir o presente recurso, o Ministério Público formulou o seguinte requerimento:
«(…)
Os presentes autos têm por objecto factos que podem preencher o crime de incêndio florestal, p. e p. nos termos do art.º 274º, nº1 do Cod. Penal.
Não existem testemunhas dos factos.
Foram realizadas, até ao momento, todas as diligências possíveis, com o respeito dos princípios da legalidade e da proporcionalidade, bem como da

compressão dos direitos, liberdades e garantias constitucionais.
Assim, e na esteira do sugerido pela Policia Judiciária, torna-se imprescindível para o êxito e prosseguimento da investigação apurar, junto dos diversos operadores de comunicações móveis a identificação dos números e aparelhos de telemóveis activados, no período que decorreu entre as 17h30 até às 18h30 do dia 28-08-2023, nas antenas e células indicadas pela P.J. a fls. 09.
Desta forma, nos termos do art.º 26º, nº1, 34º e 35º, nº 4 da Constituição da República Portuguesa, é proibido o acesso, por terceiros, à imagem, à palavra, à reserva da intimidade da vida privada e familiar, ao domicílio, à correspondência e outros meios de comunicação privada e ao acesso a dados pessoais de terceiros, salvo em casos excepcionais previsto na lei, pelo que há que obter a autorização necessária.
O interesse da realização da justiça, cometida aos Tribunais, onde no âmbito penal o Ministério Público investiga por imperativo legal, é, no caso vertente, superior aos interesse legais acima indicados, justifica a realização das diligências sugeridas pela P.J..
Não há outra forma possível para o êxito e prosseguimento das investigações senão a obtenção das referidas autorizações.
Face ao objecto dos autos e por se tratar de elementos relevantes para a prova a produzir nos autos e, bem assim, para a descoberta da verdade material dos factos, P., nos termos dos artºs. 135º, 182º, 187, nº1, al. a), nº 4, 188º, 189º, nº2, 268º, nº1, al. f) e 269º, nº1, al. e), todos do C.P.P., se determine a quebra do sigilo das telecomunicações, relativamente às operadoras de redes móveis "EMP01…/EMP02…", "EMP04…" e EMP03… e, em consequência:
Se ordene às operadoras de telecomunicações "EMP01…/EMP02…", EMP03…, "EMP04…" a remessa aos presentes autos, em suporte digital e formato "excel", dos eventos de rede referentes aos códigos de antena indicados a fls. 09 (com a identificação dos titulares dos nºs de telemóvel aí accionados e respectivos IMEIS's e moradas), em virtude dos mesmos terem sido preservados e serem fundamentais para a descoberta da verdade, no período compreendido entre as 17h30 até às 18h30 do dia 28-08-2023.
Remeta os autos ao Ex.mo J.I.C., para apreciação e decisão.
(…)».

2.2 - Sobre tal requerimento recaiu o seguinte **despacho**, **objeto do recurso**:
"Nos presentes autos de inquérito, veio o Ministério Público promover se dispense as operadoras de telecomunicações móveis "EMP01…/EMP02…", EMP03…, "EMP04…" do dever de sigilo das telecomunicações e que se ordene a remessa aos autos de informação sobre os eventos de rede registados nas células e períodos especificados em anexo ao relatório tático de inspeção

judiciária levado a cabo pelo OPC.
Cumpre apreciar e decidir.
O fornecimento dos referidos dados insere-se no acesso a dados de tráfego e de conteúdo, no âmbito do artigo 2.º, n.º 1, al. a) da Lei n.º 32/2008, de 17 de julho.
Estamos ainda no âmbito do regime da interceção e gravação de conversações ou comunicações telefónicas, nos termos dos artigos 187.º, n.º 1 e 189.º, ambos do Código de Processo Penal.
Em conformidade com estas disposições legais, a interceção e a gravação de conversações ou comunicações telefónicas, bem como a obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações, só podem ser ordenadas ou autorizadas por despacho do juiz, em prol de particulares necessidades de investigação e repressão criminal, relativamente apenas a crimes do catálogo, quando, através de um cuidado juízo de ponderação dos interesses em causa, se conclua que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter.
Acresce o disposto no artigo 3.º, n.º 2 da Lei n.º 32/2008, 17 de julho, nos termos da qual "[a] transmissão dos dados às autoridades competentes só pode ser ordenada ou autorizada por despacho fundamentado do juiz, nos termos do artigo 9.º".
Explana o artigo 9.º, n.º 1 da Lei n.º 32/2008, 17 de julho que "[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, deteção e repressão de crimes graves.". Por sua vez, tal autorização só pode ser requerida pelo Ministério Público ou pela autoridade de polícia criminal competente (cf. n.º 2 do mesmo preceito), sendo que se entende por crimes graves, "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 de títulos equiparados a moeda, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima" [cf. alínea g) do n.º 1 do artigo 2.º da referida Lei e artigo 1.º, alínea l) do Código de Processo Penal].
Já o n.º 3 do mesmo preceito legal, estabelece que:

“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.”(sublinhado nosso).
Ou seja, temos que o legislador não prescindiu do requisito quanto à identidade dos visados, conforme resulta de tal preceito, bem como do teor do artigo 187.º, n.º 4 do Código de Processo Penal. Na verdade, tais preceitos legais determinam que só pode ser autorizada a transmissão de dados relativos à localização celular, em relação a suspeitos ou arguidos, a pessoa que sirva de intermediário ou à vítima.
A este propósito, veja-se o sumário do acórdão do Tribunal da Relação de Coimbra, de 08.11.2017 (proferido no processo n.º 380/17.9JACBR.C1, disponível em www.dgsi.pt), onde se refere o seguinte:
“I - Os valores constitucionais da descoberta da verdade material e da realização da justiça, mesmo em matéria criminal, estão sujeitos aos limites impostos pela dignidade e pelos direitos fundamentais das pessoas e que processualmente se traduzem nas proibições de prova, em relação às quais o artigo 32.º, n.º 8, da CRP, estabelece, quanto à questão que agora nos ocupa, que são nulas todas as provas obtidas mediante abusiva intromissão nas telecomunicações.
II - A obtenção de dados de tráfego e de localização como aqueles que o Ministério Público pretende só pode ocorrer em relação às pessoas referidas no artigo 9.º, n.º 3, da Lei 32/2008, de 17-07, e no n.º 4 do artigo 187.º do CPP, 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 respectivo consentimento, efectivo ou presumido.
III - É também pressuposto 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, detecção e repressão de crimes graves.
IV - Exige-se ainda que a decisão judicial de transmitir os dados respeite 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.
V - Não é permitido que se aceda a dados de tráfego e de localização de um conjunto indeterminado de pessoas que efectuaram comunicações, accionado

células de antenas de comunicações, na expectativa de, entre elas, descortinar quem possa ter praticado o ilícito investigado.
VI - Pretende-se, pois, obter dados de tráfego e de localização, desejavelmente de suspeitos, mas seguramente de muitos "não suspeitos".
VII - O que não é permitido pela salvaguarda do sigilo das telecomunicações, consubstanciada nos apertados limites estabelecidos na Lei n.º 32/2008 e nas exigências constitucionais de adequação, necessidade e proporcionalidade." (sublinhado nosso).
No mesmo sentido, veja-se o acórdão do mesmo Tribunal, datado de 10.01.2018, (proferido no processo n.º 388/17.4JACBR-A.C1, também disponível em www.dgsi.pt), segundo o qual "[n]o caso dos autos, não há arguidos e não há suspeitos (…). Assim, o levantamento do sigilo das comunicações, para obtenção e junção aos autos dos dados sobre a localização celular e de registos da realização de conversações ou comunicações, visando o universo de todas as pessoas não determinadas, que acionaram os telemóveis nas duas zonas e nos períodos indicados, não pode ser deferido. O dano causado à privacidade de um elevado número indeterminado de pessoas, afetadas num direito fundamental, nos termos requeridos é demasiadamente grave e não pode ser ultrapassado, sacrificando o seu direito fundamental da privacidade e inviolabilidade nas telecomunicações em prol da investigação" (sublinhado nosso).
Feito este enquadramento legal, voltemos a nossa atenção para o caso em apreço.
Nos presentes autos investiga-se a prática de um crime de incêndio florestal, p. e p. pelo artigo 274.º, n.º 1, do Código Penal, que é punido com pena de prisão de um a oito anos, pelo que se constata, desde logo, que tal crime não é passível de se subsumir ao previsto nos artigos 2.º, n.º 1, alínea g) e 9.º, n.º 1 da Lei nº 32/2008, de 17 de julho.
Mas mesmo que assim não se entendesse, o que não é o caso, o certo é que, no caso em apreço, e conforme resulta do teor do exposto pelo Ministério Público, das diligências efetuadas até momento não foi possível apurar a identidade do(s) autor(es) dos factos em investigação ou, sequer, de qualquer suspeito.
Acrescentou o Ministério Público que, "O interesse da realização da justiça, cometida aos Tribunais, onde no âmbito penal o Ministério Público investiga por imperativo legal, é, no caso vertente, superior aos interesse legais acima indicados, justifica a realização das diligências sugeridas pela P.J..
Não há outra forma possível para o êxito e prosseguimento das investigações senão a obtenção das referidas autorizações.".
De facto, com a diligência promovida, pretende-se lograr a identificação de

suspeitos pela prática dos factos em investigação e não, como a lei exige, incidir sobre dados de tráfego e de localização relativos a suspeitos concretos.
Dito de outro modo, o que é pretendido é que se aceda a dados de tráfego e de localização de um conjunto indeterminado de pessoas que efetuaram comunicações, acionando células de antenas de telecomunicações, na esperança de, entre todas, descortinar quem possa ter praticado o crime investigado.
Ora, a pretensão do Ministério Público vai necessariamente abranger um leque muito alargado de cidadãos que não possuem o estatuto jurídico processual de "suspeito" e, como tal, entende-se que não se verifica o requisito previsto nos sobreditos preceitos legais.
É certo que a exigência de individualização do suspeito enquanto interveniente processual, designadamente para efeitos da alínea a) do n.º 3 e do artigo 9.º da Lei n.º 32/2008, de 17 de Julho, não se confunde com a sua identificação completa, mas não dispensa a existência de dados factuais tendentes a essa identificação, com base nos quais possa individualizar-se uma pessoa determinada.
O artigo 1.º, alínea e) do Código de Processo Penal define "suspeito" como sendo 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.
In casu, não há, de facto, arguidos, mas também inexiste qualquer elemento concreto que permita considerar como identificável qualquer suspeito e, bem assim, o(s) seu(s) número(s) de telemóvel.
O pedido de obtenção de dados quanto à localização celular abrange, aliás, um número indeterminado de pessoas que se desconhece em absoluto que tenham qualquer relação com o objeto deste processo, sendo que em caso de autorização, estar-se-ia a permitir a recolha de informações relativamente a pessoas inocentes, na simples esperança de que entre elas se apanhar um suspeito.
Aliás, veja-se que o Ministério Público requereu a identificação de todos os dados de tráfego, o que implica que o leque de visados integre todos aqueles que efetuaram comunicação telefónica nas áreas mencionadas e em período próximo do momento da prática do crime, fazendo ativar a correspondente antena, sendo estes critérios manifestamente insuficientes para satisfazer as exigências mínimas de densificação factual do conceito de "suspeito".
Como defendido por Paulo Pinto de Albuquerque, in "Comentário do Código de Processo Penal", 2.ª Edição, p. 509, "a existência de um catálogo de alvos obsta à determinação de escutas telefónicas em processo contra incertos. O legislador pretendeu que a autorização judicial tivesse por referência as

conversações mantidas por pessoas concretas, ainda que não seja conhecida a sua identidade civil. São, portanto, inadmissíveis as escutas determinadas a grupos de pessoas cujo único traço comum é o ocuparem habitualmente ou esporadicamente um determinado espaço físico".
Também Gomes Canotilho e Vital Moreira in "Constituição da República Portuguesa Anotada", 4.ª Edição, Volume I, p. 543, defenderam que "[n]o que respeita à lei restritiva, esta não poderá legitimar escutas telefónicas (…) para a investigação de quaisquer crimes, devendo limitarse a crimes particularmente graves (…), nem estender ilimitadamente o universo de pessoas suspeitas à escuta (alargamento das escutas a terceiros que não têm qualquer relação com os factos sujeitos a investigação)".
Defende-se, na linha do sufragado no Acórdão do Tribunal Constitucional n.º403/2015, que o acesso aos dados de tráfego pode constituir uma ingerência gravosa na vida privada das pessoas, já que permitem aceder a informações relativas a todas as chamadas efetuadas, incluindo as chamadas para as linhas de serviço de emergência, SOS e similares, ao número de chamadas, aos números de telefone chamados, à hora e início e duração de cada uma delas, à posição geográfica e direção da deslocação que o utilizador efetuou durante a realização de uma determinada chamada.
Ora, tem sido amplamente defendido pela jurisprudência dos Tribunais superiores que se os dados de localização celular que se pretendem obter não têm como alvo um suspeito, mas um conjunto de pessoas não identificadas e unidas apenas pelo simples facto de estarem num dado local num dado momento não é admissível, pois, além de não respeitar os princípios da proporcionalidade e da adequação, não permitem o enquadramento no conceito jurídico-penal de "suspeito".
Neste sentido, vejam-se, entre outros, os Acórdãos do Tribunal da Relação de Évora de 23/09/2010, 18/10/2011, 26/06/2012, 19/05/201, do Tribunal da Relação do Porto de 11/02/2015, do Tribunal da Relação de Lisboa de 22/06/2016, de 03/05/2016 de 07/03/2017 e do Tribunal da Relação de Coimbra de 08/11/2017, todos disponíveis em www.dgsi.pt.
Nestes termos, entende-se que a diligência promovida, para além de ferir os ditames legais supra expostos, apresenta-se violadora do princípio da proporcionalidade, quer na sua dimensão da adequação, quer na sua dimensão da proporcionalidade em sentido estrito (artigo 18.º da Constituição da República Portuguesa), pelo que entende-se que ainda que possa revestir alguma utilidade para a descoberta da verdade material nestes autos, pela sua amplitude, comporta uma devassa incomportável e intolerável à reserva da vida privada de todas as pessoas que, desconectadas destes autos, ativaram as células mencionadas nos autos, com os seus dispositivos móveis.

Tudo sem olvidar que, no caso, nem sequer é permitido o recurso a tais dados para a investigação do crime em causa e, ainda, que nem há a certeza de que os autores fizeram uso de telemóvel, na prática do crime sob investigação.
O argumento da gravidade do crime não pode servir, claro está, para tornear quer os ditames legais imperativos, quer o princípio da proporcionalidade constitucionalmente garantido.
Face a todo o exposto, indefere-se o promovido.
Devolva os autos ao Ministério Público.»

3. - APRECIAÇÃO DO RECURSO

3.1 - O despacho recorrido indeferiu a pretensão formulada pelo Ministério Público visando a **obtenção de dados de comunicações**.
Conforme assinalado pelo Ministério Público, encontram-se simultaneamente em vigor quatro diplomas legais que regulam a complexa arquitetura normativa da obtenção de dados em posse de fornecedores de serviços de comunicações, a saber:
1. O **Código de Processo Penal** (*maxime*, os artigos 187º a 190º);
2. A **Lei n.º 41/2004**, de 18 de agosto (Lei da Proteção de Dados Pessoais e Privacidade) – transpõe para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao **tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas**;
3. A **Lei n.º 32/2008**, de 17 de julho – 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**;
4. A **Lei n.º 109/2009**, de 15 de setembro (Lei do Cibercrime) – transpõe para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a **ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa**.
Esta proliferação legislativa foi determinada pela crescente e rápida evolução tecnológica no âmbito das comunicações que se tem registado nas últimas décadas, com ampla projeção, quotidianamente, nas relações interpessoais e institucionais, nos planos pessoal e profissional.
A progressiva passagem da era analógica para a era digital implica, necessariamente, proporcional aumento de registo de dados inerentes à generalizada informatização das mais diversas vertentes da vida em sociedade

à escala mundial.
Tal realidade tem óbvios reflexos em direitos fundamentais dos cidadãos num estado de direito democrático, nomeadamente o direito à privacidade e reserva da vida privada e familiar, o direito à inviolabilidade dos meios de comunicação privada e o direito à autodeterminação informativa, com assento constitucional [artigos 26º, n.º 1, 34º e 35º da Constituição da República Portuguesa], cuja compressão deve obedecer ao princípio basilar da necessidade, adequação e proporcionalidade [artigo 18º, n.º 2, do mesmo diploma], competindo, em primeira linha, ao legislador ordinário assegurar esses pressupostos ao legislar sobre a matéria.
Analisemos, pois, ainda que perfuntoriamente, os sobreditos instrumentos legislativos.

A **Lei n.º 41/2004** apenas regula os direitos dos utilizadores no tratamento de dados pessoais e a proteção da sua privacidade face aos prestadores de serviços de comunicações eletrónicas – *"aplica-se ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas, nomeadamente nas redes públicas de comunicações que sirvam de suporte a dispositivos de recolha de dados e de identificação, especificando e complementando as disposições da Lei n.º 67/98, de 26 de outubro (Lei da Proteção de Dados Pessoais)"*[artigo 1º, n.º 2].
O artigo 2º, n.º 1, define:
«*Dados de tráfego*» como *quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma* [al. d)];
«*Dados de localização*» como *quaisquer dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público* [al. d)]; e
«Serviços de valor acrescentado» como *sendo todos aqueles que requeiram o tratamento de dados de tráfego ou de dados de localização que não sejam dados de tráfego, para além do necessário à transmissão de uma comunicação ou à faturação da mesma.*
Estatui o artigo 4º, n.º 1, que as empresas que oferecem redes ou serviços de comunicações eletrónicas devem garantir a inviolabilidade das comunicações e respetivos dados de tráfego.

O artigo 5º, sob a epígrafe *armazenamento e acesso à informação*, dispõe:

"1 - O armazenamento de informações e a possibilidade de acesso à informação armazenada no equipamento terminal de um assinante ou utilizador apenas são permitidos se estes tiverem dado o seu consentimento prévio, com base em informações claras e completas nos termos da Lei de Proteção de Dados Pessoais, nomeadamente quanto aos objetivos do processamento.
2 - O disposto no presente artigo e no artigo anterior não impede o armazenamento técnico ou o acesso:
a) Que tenha como única finalidade transmitir uma comunicação através de uma rede de comunicações eletrónicas;
b) Estritamente necessário ao fornecedor para fornecer um serviço da sociedade de informação solicitado expressamente pelo assinante ou utilizador."
O artigo 6º estipula como princípio geral que os ***dados de tráfego*** devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos de transmissão da comunicação.
E o n.º 1 do artigo 7º impõe que *"Nos casos em que sejam processados* ***dados de localização****, para além dos dados de tráfego, relativos a assinantes ou utilizadores das redes públicas de comunicações ou de serviços de comunicações eletrónicas acessíveis ao público,* ***o tratamento destes dados é permitido apenas se os mesmos forem tornados anónimos***", regulando os restantes números do preceito o circunstancialismo excecional em que é permitido o registo, tratamento e disponibilização de tal tipo de dados, nomeadamente às organizações com competência legal para receber ou tratar comunicações de emergência, para efeitos de resposta a essas comunicações [cfr. n.º 2].
Em conformidade com a Diretiva n.º 2002/58/CB, a Lei n.º 41/2004 considera os dados de localização que fornecem a posição geográfica do equipamento terminal como dados de tráfego apenas na medida em que sejam estritamente tratados pela rede móvel para permitir a transmissão de comunicações, ficando fora desta classificação os dados de localização que são mais precisos do que o necessário para a transmissão das comunicações e que são utilizados para a prestação de serviços de valor acrescentado, tais como serviços que prestam aos condutores informações e orientações individualizadas sobre o tráfego [artigos 2º, alíneas d), e) e f), 6º e 7º].
Aqui chegados, importa, portanto, concluir que os dados da faturação detalhada e os dados da localização celular que fornecem a posição geográfica do equipamento móvel com base em atos de comunicação, na medida em que são tratados para permitir a transmissão das comunicações, são dados de tráfego respeitantes às telecomunicações e, portanto, encontram-se

abrangidos pela proteção constitucional conferida ao sigilo das telecomunicações[4].
Este diploma afasta expressamente do seu âmbito de aplicação a prevenção, investigação e repressão de infrações penais, as quais são definidas em legislação especial, como se refere nos n.ºs 4 e 5 do artigo 1º:
*"4. As **exceções à aplicação da presente lei** que se mostrem estritamente necessárias para a proteção de atividades relacionadas com a segurança pública, a defesa, a segurança do Estado e a **prevenção, investigação e repressão de infrações penais são definidas em legislação especial**.*
5 - Nas situações previstas no número anterior, as empresas que oferecem serviços de comunicações eletrónicas acessíveis ao público devem estabelecer procedimentos internos que permitam responder aos pedidos de acesso a dados pessoais dos utilizadores apresentados pelas autoridades judiciárias competentes, em conformidade com a referida legislação especial.
Esclarece, ainda, no artigo 6º, n.º 7, que *"[o] disposto nos números anteriores não prejudica o direito de os tribunais e as demais autoridades competentes obterem informações relativas aos **dados de tráfego**, nos termos da legislação aplicável, **com vista à resolução de litígios**, em especial daqueles relativos a interligações ou à faturação"*.
Ademais, ao contrário dos demais diplomas, como melhor se verá, a disponibilização de dados não tem como pressuposto que esteja em causa a investigação de qualquer crime e, muito menos, um específico catálogo de crimes.
Donde se infere que o campo de aplicação da Lei n.º 41/2004 se circunscreve à relação contratual, não sendo lícito dela lançar mão para efeito de investigação criminal.

Por seu lado, a **Lei n.º 32/2008** visa acautelar a conservação de dados essenciais à investigação e instrução criminal.
Segundo o artigo 1º, n.º 1, *"regula a conservação e a transmissão dos **dados de tráfego e de localização** relativos a pessoas singulares e a pessoas coletivas, bem como dos **dados conexos** necessários **para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves** por parte das autoridades competentes"*, estabelecendo o n.º 2 que *"[a] conservação de dados que revelem o conteúdo das comunicações é proibida, **sem prejuízo do disposto na Lei n.º 41/2004, de 18 de Agosto, e na legislação processual penal relativamente à interceção e gravação de comunicações**."*
O artigo 2º, n.º 1, define, além do mais, o que deve entender-se como **«*dados*»** – *"os dados de tráfego e os dados de localização, bem como os dados conexos*

necessários para identificar o assinante ou o utilizador" [al. a)] – e por ***"crime grave"*** – "*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 de títulos equiparados a moeda, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima*" [al. b)].

O artigo 3º dispõe sobre a finalidade do tratamento, preceituando o n.º 1 que "*[a] **conservação e a transmissão dos dados** têm por **finalidade exclusiva a investigação, deteção e repressão de crimes graves por parte das autoridades competentes***", acrescentando o n.º 2 que "*[a] transmissão dos dados às autoridades competentes só pode ser ordenada ou autorizada por despacho fundamentado do juiz, nos termos do artigo 9.º*".

O artigo 4º discrimina as "*categorias dos dados a conservar*" e o artigo 6º estabelece o "*período de conservação*" [1 (um) ano].

E o artigo 9º regula os termos em que pode ocorrer a "***transmissão dos dados***":

"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, deteção 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 respetivo consentimento, efetivo 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 proteção do segredo profissional, nos termos legalmente previstos."

Em suma, a Lei n.º 32/2008 criou e definiu um regime processual penal

especial relativamente aos dados que têm que ser conservados para fins de investigação, deteção e repressão de ***crimes graves***.
O legislador visou, por imposição de regulamentação europeia (transposição da Diretiva 2006/24/CE), regular e limitar o modo de conservação e acesso, quanto ao período temporal e quanto ao fundamento, de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.
Esta Diretiva surgiu num contexto específico, na sequência de ataques terroristas a Londres, motivando que o Conselho da Europa, na sua Declaração de 13/07/2015, tenha reafirmado «a necessidade de aprovar o mais rapidamente possível medidas comuns relativas à conservação de dados de telecomunicações». A Diretiva surge na esteira da consideração «da importância dos dados de tráfego e dos dados de localização para a investigação, deteção e repressão de infrações penais» e, por isso, da necessidade de «garantir a nível europeu a conservação durante um determinado período dos dados gerados ou tratados, no contexto da oferta de comunicações, pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações».
O objetivo primacial da Diretiva traduzia-se na «harmonização das obrigações que incumbem aos fornecedores de conservarem determinados dados e assegurarem que estes sejam disponibilizados para efeitos de investigação, deteção e repressão de crimes graves tal como definidos no direito nacional de cada Estado-Membro» e que as estipulações da Diretiva teriam presente a conformidade com o princípio da proporcionalidade e, consequentemente, não excederiam o necessário para atingir aqueles objetivos e respeitariam «os direitos fundamentais e os princípios consagrados nomeadamente na Carta dos Direitos Fundamentais da União Europeia», visando assegurar «que sejam plenamente respeitados os direitos fundamentais dos cidadãos em matéria de respeito pela privacidade e pelas comunicações e de proteção dos dados pessoais».
Ora, o legislador português poderia perfeitamente ter definido como “crimes graves”, para efeito da Diretiva, aqueles que integram o catálogo já constante do n.º 1 do artigo 187º do Código de Processo Penal, fazendo-os coincidir, o que levaria a que, quanto ao âmbito, nada se alterasse relativamente à previsão da geral do n.º 2 do artigo 189º do mesmo código.
Todavia, não foi essa a opção do legislador, que expressamente optou por definir os “crimes graves” na alínea g) do n.º 1 do artigo 2º da Lei n.º 32/2008, reduzindo substancialmente o catálogo de crimes relativamente àquele, constante do n.º 1 do artigo 187º do Código de Processo Penal, assim reforçando a especialidade daquela Lei e a restritividade do seu campo de

aplicação.
Porém, à luz das regras europeias, exigir-se-ia até maior restrição no que toca ao acesso a dados de tráfego, comunicação e localização do que aquela que a Lei n.º 32/2008 trouxe relativamente ao regime do artigo 189º, n.º 2, do Código de Processo Penal, como se depreende do facto de a aludida Diretiva ter sido, entretanto, julgada inválida pelo Acórdão do Tribunal de Justiça da União Europeia (Grande Secção), de 08 de Abril de 2014, precisamente por não assegurar a proporcionalidade na restrição dos direitos ao respeito pela vida privada e familiar e à proteção de dados pessoais, consagrados nos artigos 7º e 8º da Carta dos Direitos Fundamentais da União Europeia, consistindo, numa das vertentes, essa falta de proporcionalidade em determinar-se a conservação de todos os dados de tráfego, mesmo sem indícios de que o visado estaria ligado, ainda que de modo indireto ou longínquo, com crimes graves, o que viria a ser reconhecido, entre nós, no acórdão do Tribunal Constitucional n.º 268/2022, que declarou a inconstitucionalidade de algumas das normas da Lei n.º 32/2008, como *infra* se detalhará[5].

Ulteriormente, foi aprovada a **Lei n.º 109/2009**, que *"estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da* ***recolha de prova em suporte eletrónico*** *(...)"* [artigo 1º], ou seja, criou mecanismos processuais visando, especificamente, garantir e ***regular o modo de obtenção*** da ***prova digital***.
Em termos materiais ou substantivos, consagra novos tipos penais e outras normas conexas (artigos 3º a 10º) e, do ponto de vista processual ou adjetivo, estabelece um regime processual próprio (artigos 11º a 19º).
O referido regime processual desdobra-se, na realidade, em dois – um, previsto nos artigos 11º a 17º; outro, regulado nos artigos 18 e 19º.

O primeiro [**artigos 11º a 17º**] corresponde ao regime processual geral de aquisição de prova por **recolha de dados "*conservados*" nos crimes informáticos,** no que tange aos crimes que, nos termos das alíneas do n.º 1 do artigo 11º, "*estão previstos na própria lei*" [al. a)], "*são ou foram cometidos por meio de um sistema informático*" [al. b)] ou "*em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico*" [al. c)], ***desde que não esteja em causa a interceção de comunicações*****, excluindo, por conseguinte, a aplicabilidade do disposto nos artigos 187º a 190º do Código de Processo Penal.** Os artigos 12º a 17º referem-se à *preservação expedita, revelação expedita, injunção para apresentação ou concessão do*

acesso a dados, pesquisa de dados, apreensão de dados e apreensão de correio eletrónico e registos de comunicações de natureza semelhante, sendo que os dados podem ser de ***base*** e de ***tráfego***.

O segundo [**artigos 18º e 19º**] corresponde ao regime aplicável se estiver em causa a ***interceção de comunicações*** relativamente *aos crimes nela previstos* [al. a) do n.º 1 do artigo 18º] e *aos cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal* [al. b)]. O n.º 4 do artigo 18º estabelece que *"[e]m tudo o que não for contrariado pelo presente artigo, à interceção e registo de transmissões de dados informáticos* ***é aplicável o regime da interceção e gravação de conversações ou comunicações telefónicas, constante dos artigos 187.º, 188.º e 190.º do Código de Processo Penal****"*. A previsão dos artigos 18º e 19º abrange os ***dados de tráfego*** e os ***dados de conteúdo***.
O elemento distintivo essencial entre os dois sobreditos regimes processuais é, assim, a natureza da intervenção:
- No caso dos artigos 11º a 17º está em causa a **pesquisa, apreensão e transmissão** de dados de ***base*** e de ***tráfego*** e de ***conteúdo de correio eletrónico*** pretéritos, que estão **armazenados**;
- No caso do artigo 18º trata-se de **intercetar, em tempo real**, dados de ***tráfego*** e de ***conteúdo***, ou seja, de comunicações **que estão a ocorrer**.

Como se vê, o objeto da **Lei n.º 32/2008** e da **Lei n.º 109/2009** é parcialmente coincidente, pois ambas regulam dados guardados – *dados conservados* no primeiro caso; *dados preservados* no segundo caso.
Contudo, a Lei n.º 109/2009 assume um carácter geral no seu âmbito de aplicação, não distinguindo dados arquivados pela sua natureza, abrangendo, por conseguinte, todos eles.
Já a Lei n.º 32/2008 restringe os dados a submeter ao seu regime aos elencados no seu artigo 4º, n.º 1 ["*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*"], explicitando os números 2 a 7 do mesmo preceito em que consistem os dados necessários referidos em

cada uma das mencionadas alíneas daquele n.º 1.
O **regime processual da Lei n.º 32/2008 apresenta-se**, assim, no que concerne aos dados "conservados" que especificamente regula, **como um regime especial relativamente ao capítulo processual penal geral que consta dos artigos 11º a 19º da Lei n.º 109/2009, já que esta, mesmo quando se refere a interceção de comunicações, tem por objeto comunicações eletrónicas,** e não comunicações telefónicas. Ademais, o n.º 2 do artigo 11º estatui expressamente que *"[a]s disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008/ de 17 de julho"*.
Nessa medida, como os dados previstos no n.º 1 do artigo 4º da Lei n.º 32/2008 dizem respeito a comunicações telefónicas, mas ambas as leis os equiparam a dados "conservados ou "preservados", o regime processual com tutela reforçada daquela lei deveria manter-se para esses dados, prevalecendo a sua aplicação, desde que verificados os demais pressupostos, nomeadamente o preenchimento do crime de catálogo de âmbito mais restrito ali definido.

Com decorrência do que vimos expondo, há quem entenda que se mostram tacitamente revogados alguns segmentos do regime consagrado no Código de Processo Penal, especialmente nos artigos **187º a 190º**. Neste sentido, afirma João Conde Correia que «*primeiro a Lei n.º 32/2008 e depois a Lei n.º 109/2009 revogaram, tacitamente, parcelas importantes do regime consagrado no artigo 189º do Código de Processo Penal, reduzindo muito o seu alargado âmbito de aplicação inicial*" e *"em suma, a legislação contida no Código de Processo Penal foi, no essencial, ultrapassada pelas Leis n.ºs 32/2008 e 109/2009*»[6]. Por seu lado, entre outros, Paulo Pinto Albuquerque [7] e Pedro Verdelho[8] entendem que «o artigo 18º da Lei n.º 109/2009 não revogou o artigo 189º do Código de Processo Penal nem as 23 disposições processuais da Lei n.º 32/2008».
Mas, mesmo para quem perfilha o primeiro entendimento, continua, porém, em vigor o disposto no artigo **189º** do Código de Processo Penal, com as seguintes especialidades:
- O n.º 1, quando estabelece que *"[o] disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, […], e à interceção das comunicações entre presentes"*, com exceção, portanto, do segmento [designadamente correio eletrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital].
- O n.º 2, ao determinar que *"[a] obtenção e junção aos autos de dados sobre a*

localização celular só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo", reporta-se a **"dados sobre a localização celular" obtidos em tempo real**.

Destarte, tem sido entendimento maioritário que, tratando-se de dados de comunicações "conservadas" ou "preservadas", não é possível aplicar o disposto no artigo 189º do Código de Processo Penal – a extensão do regime das escutas telefónicas – aos casos em que são aplicáveis as Leis n.ºs 32/2008 e 109/2009. Isto é, para a prova de ***comunicações preservadas ou conservadas 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, com as especificidades *supra* assinaladas, coadjuvado pelos artigos 3º a 11º da Lei nº 32/2008, se for caso de dados previstos nesta última. Fundamental é, além do mais, ter presente que o acesso a *dados conservados* não é o mesmo que uma *interceção de dados*[9].
Predominava, assim, o entendimento de que a obtenção de dados conservados por operadoras de telecomunicações que se enquadrassem no elenco do artigo 4º da Lei n.º 32/2008 só poderiam ser acedidos nos termos admitidos por tal diploma, não podendo recorrer-se a outros expedientes, como sejam a invocação do disposto no artigo 189º, n.º 2, do Código de Processo Penal ou na Lei do Cibercrime.
O acórdão do Tribunal da Relação de Évora de 20.01.2015, que aqui seguimos de perto, efetua uma síntese impressiva desta temática no respetivo sumário, que ora transcrevemos:
«1. O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão às «telecomunicações eletrónicas», «crimes informáticos» e «recolha de prova eletrónica (informática)» desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra.
2. Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável à **recolha de prova por «localização celular conservada**» - uma forma de «recolha de prova eletrónica - desde a entrada em vigor da **Lei 32/2008**, de 17-07.
3. Para a **prova eletrónica 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 eletrónica.
Isto porquanto existe um segundo catálogo na Lei n.º 109/2009, o do artigo 18º, n.º 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime - o dos artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187º, 188º e 190º do C.P.P. e sob condição de não contrariarem e Lei 109/2009.
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.º 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 eletrónico.
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 interceção de comunicações eletrónicas, em tempo real, de dados de tráfego e de conteúdo associados a comunicações específicas transmitidas através de um sistema informático***.
7. Assim, o Capítulo III da Lei 109/2009, relativo ás disposições processuais, deve ser encarado como um «escondido Capítulo V («Da prova eletrónica»), do Título III («Meios de obtenção de prova») do Livro III («Da prova») do Código de Processo Penal» (Dá Mesquita).
8. Tratando-se de obter **prova por «localização celular conservada**», isto é, **a obtenção dos dados previstos no artigo 4º, n.º 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.º 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.º 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.º 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 **objeto 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 exceção do correio eletrónico, 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.º 1 da Lei nº 32/2008 ou seja, dados conservados em geral;
- **vigente** para todos os dados que estejam especificamente previstos no artigo 4º, n.º 1 da Lei nº 32/2008, isto é, para os dados conservados relativos á localização celular. Só para este último caso ganha relevo o conceito de «crime grave».
14. Antes da entrada em vigor das Leis 32/2008 e 109/2009 podia afirmar-se que havia duas formas «processualmente úteis» de usar a localização celular. Uma delas a medida cautelar de polícia prevista no artigo 252º-A do C.P.P. e a outra o meio de obtenção de prova previsto no **artigo 189º, n.º 2 do mesmo código, que se mantém em vigor para a localização celular em tempo real**.
15. Agora coexistem três realidades distintas através do acrescento da **obtenção de dados de localização celular «conservados» por via da Lei nº 32/2008**.
16. Os requisitos do n.º 3 do artigo 9º da Lei 32/2008 mostram-se de verificação alternativa. O conceito de «suspeito» dele constante exige «determinabilidade» e não «determinação».

17. A previsão do artigo 252º-A do Código de Processo Penal é claramente uma previsão de carácter excecional para situações de carácter excecional.»
E o acórdão do Tribunal da Relação de Coimbra de 12.10.2022 sintetizou a posição da jurisprudência e da doutrina nesta matéria, nos seguintes moldes:
«Tem sido unânime o entendimento de que (cfr. Acórdão desta Relação no Pº 380/17.9JACBR.C1, acompanhando a posição assumida nos Acórdãos da Relação de Lisboa de 22-06-2016 (processo n.º 48/16.3PBCSC-A.L1-9), 07-03-2017 (processo n.º 1585/16.5PBCSC-A.L1-5), da Relação de Évora de 25-10-2016 (processo n.º 223/16.0GBLLE.E1) e, mais recentemente, nos Acórdãos da Relação do Porto de 20-11-2019 (processo n.º 54/19.6GDSTS-A.P1) e 04-12-2019 (processo n.º 463/18.8PASTS-A.P1), da Relação de Évora de 14-07-2020 (processo n.º 9/20.8GAMTL-A.E1) e da Relação de Guimarães de 03-02-2022 (processo n.º 57/21.0GAMCD-A.G1), que o **regime estabelecido pela Lei n.º 32/2008**, de 17 de Julho, **aplica-se à obtenção dos dados relativos a comunicações já ocorridas e que se encontram preservados ou conservados, não sendo de aplicar o CPP neste jaez.**
Tratando-se, pois, de obter prova por "localização celular conservada", isto é, relativa aos dados previstos no artigo 4.º, n.º 1 da Lei n.º 32/2008, de 17 de Julho, o regime processual aplicável assume especialidade nos artigos 3.º e 9.º deste diploma, regime que, sendo especial, se sobrepõe ao de carácter geral instituído pelos artigos 12.º a 17.º da Lei n.º 109/2009, de 15 de Setembro – Lei do Cibercrime –, a qual, de resto, expressamente ressalva, no artigo 11.º, n.º 2, que as suas disposições processuais não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho.
Já o artigo 189.º, n.º 2 do CPP, com a extensão do regime das escutas telefónicas nele consagrada, remetendo para os requisitos de admissibilidade fixados no artigo 187.º, n.ºs 1 e 4 do mesmo diploma, **tem em vista os dados recolhidos em tempo real**.
Para além da jurisprudência acima referida, é também nesse sentido o que se anota em António Henriques Gaspar et al., Código de Processo Penal Comentado (anotação de Santos Cabral ao artigo 189.º), 2.ª ed., Almedina, 2016, pág.786, e António Gama et al., Comentário Judiciário do Código de Processo Penal, tomo II (anotação de Tiago Caiado Milheiro ao artigo 189.º), Almedina, 2019, págs.828 a 835).
Também o recente acórdão do STJ datado de 18 de Maio de 2022 (Pº 618/16.0SMPRT-B.S1) assim opina:
«Perante a diversidade de meios de prova vêm a doutrina e a jurisprudência assinalando que, em termos de unidade do sistema jurídico, se impõe a necessidade de harmonização entre os regimes dos artigos 187º e 189º do CPP e o regime da Lei n.º 32/2008, de 17/7, donde resulta que o daquele se

aplica à interceção de comunicações, obtida em tempo real, a decorrer, e interceção da comunicação entre presentes, enquanto o desta tem como âmbito de aplicação a obtenção de dados que concernem a comunicações relativas ao passado, ou seja, conservadas ou armazenadas em arquivo, como se extrai até do consagrado no seu artigo 1º, n.º 1.
(…)
Por isso, seja conversação ou comunicação e o que lhe é conexo, necessariamente, a fonte telefónica ou informática, caberá nas normas dos artigos 187º e 189º do CPP. Já se o que interessa são comunicações passadas, localizadas no tempo e no espaço, chama-se à colação a Lei n.º 32/2008, de 17 de Julho».
Damos o nosso assentimento a esta tese.»
Também o acórdão do Tribunal da Relação de Lisboa de 07.03.2017 refere que «(…) o regime dos artigos 187º a 189º, do CPP, aplica-se aos "dados sobre a localização celular", obtidos em tempo real e interceção das comunicações entre presentes, enquanto o consagrado na Lei nº 32/2008, de 17/07, tem como âmbito de aplicação os dados que concernem a comunicações relativas ao passado, ou seja, arquivadas (…)».
No acórdão do Supremo Tribunal de Justiça de 06.09.2022 também se afirma que «Os arts. 187 a 189, do CPP, regulam o recurso aos dados relativos a conversações ou comunicações telefónicas em tempo real, enquanto o acesso aos dados conservados pelas operadoras por conversações ou comunicações telefónicas passadas é regulado pela Lei nº32/2008, de 17 Julho; o nº 1, do art.187 citado, delimita o objeto dessa regulação como "a interceção e a gravação de conversações ou comunicações telefónicas", o que representa comunicações a ocorrer, conversações ou comunicações telefónicas em tempo real. Já se o que interessa processualmente são comunicações passadas, localizadas no tempo e no espaço, chama-se à colação a Lei nº 32/2008, de 17 de Julho».
E no acórdão do Tribunal da Relação do Porto, de 15.03.2023, sinaliza-se que «Os regimes do Código de Processo Penal e da Lei 32/2008 têm campos de aplicação diversos, dizendo o do primeiro respeito à captura dos dados relativos a comunicações a realizar no futuro enquanto o da segunda diz respeito a dados relativos a comunicações ocorridas no passado, a dados arquivados».
Em sentido divergente, claramente minoritário, vejam-se, a título exemplificativo, os acórdãos:
- Do Tribunal da Relação de Lisboa, de 22.02.2023, em que se sustenta que «O n.º 2 do artigo 189º do Cód. Proc. Penal, não se reporta à obtenção de "dados dinâmicos", ou seja, que estejam a ser transmitidos em tempo real, por

oposição a “dados preservados ou armazenados”;
- Do Tribunal da Relação do Porto, de 29.03.2023, em que assim se discorre a este respeito:
«A verdadeira extensão do regime de intercepção e gravação de conversações e comunicações (escutas telefónicas) decorrente dos arts. 187.º e 188.º do CPPenal centra-se no n.º 1 do art.189.º do mesmo diploma legal, relativamente às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone e às comunicações entre presentes, respeitando o seu n.º 2 a dados de tráfego e localização celular já existentes, ou seja, dados conservados, e não aos produzidos em tempo real.
Daí se mencionar a obtenção e junção aos autos e não a intercepção desses dados. E também por isso não se mencionam os procedimentos de controlo previstos no antecedente art. 188.º, destinados à intercepção de comunicações, e se preveja a autorização judicial em qualquer fase do processo. Em fase de julgamento pode fazer sentido a obtenção de dados de tráfego e localização celular conservados, mas já não faz sentido a realização de intercepção desses dados em tempo real, pois a prova do julgamento respeita a factos pretéritos, os descritos na acusação. E como também invoca Rui Cardoso [ob cit.], caso aquele n.º 2 do art. 189.º do CPPenal respeitasse à intercepção de comunicações, seria obvia a ineficácia da medida em fases em que o processo não se encontra já em segredo de justiça.
A obtenção e junção aos processos de natureza criminal de dados de tráfego e de localização celular estava, e está, apenas limitada pela exigência de despacho judicial a determinar ou autorizar essas acções, que estão circunscritas aos crimes de catálogo do n.º 1 do art. 187.º do CPPenal e relativamente às pessoas referidas no n.º 4 deste preceito.
Assim, entre a Lei 48/2007, de 29-08 e a Lei 32/2008, de 17-07, o fundamento para conservar dados de comunicação residia na Lei 41/2004, de 18-08, encontrando-se a base legal para a respectiva obtenção e junção aos autos no âmbito do processo penal no art. 189.º, n.º 2, do CPPenal.»

Apesar da progressiva convergência da jurisprudência quanto à problemática da harmonização dos diplomas vigentes em matéria de obtenção de prova digital nos moldes que vimos descrevendo, a situação estava longe de ser pacífica.
Ocorre que o **acórdão do Tribunal Constitucional n.º 268/22**, de 19-04 [10], veio declarar a inconstitucionalidade, com força obrigatória geral, de várias normativos da Lei n.º 32/2008, mais concretamente:
- Da norma constante do **artigo 4.º** da Lei n.º 32/2008, de 17 de julho, conjugada com o **artigo 6.º** da mesma lei, por violação do disposto nos n.ºs 1

e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo n.º 18.º, todos da Constituição; e
- Da norma do **artigo 9.º da Lei n.º 32/2008, de 17 de julho**, relativa à transmissão de dados armazenados às autoridades competentes para investigação, deteção e repressão de crimes graves, **na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros,** por violação do disposto no n.º 1 do artigo 35.º e do n.º 1 do artigo 20.º, em conjugação com o n.º 2 do artigo 18.º, todos da Constituição.
Tal declaração de inconstitucionalidade teve subjacente o entendimento de que as sobreditas normas da Lei n.º 32/2008 permitiam uma lesão desproporcionada à reserva da intimidade e da vida privada dos cidadãos[11].
O aludido acórdão do Tribunal Constitucional relançou e, até, agudizou, a discussão em torno desta temática, tendo em perspetiva, agora, além do mais, as repercussões da predita declaração de inconstitucionalidade de normativos fundamentais da Lei n.º 32/2008.
Com efeito, perante a referida declaração de inconstitucionalidade tem surgido uma miríade de decisões dos tribunais superiores sustentando entendimentos díspares, por vezes, até, no seio do mesmo tribunal. Assim, passamos a transcrever os sumários de algumas dessas decisões, optando-se por fazê-lo na íntegra para melhor perceção das matérias e questões abordadas, tratadas e decididas e respetivo contexto:
- Acórdão do Tribunal da Relação de **Coimbra** de 12.10.2022:
«I - «Metadados» são dados referentes ao tráfego das comunicações eletrónicas e de localização, bem como os dados conexos necessários para identificar o assinante e/ou utilizador, permitindo determinar todos os dados atinentes àquela forma de comunicabilidade, com exceção do seu teor ou conteúdo, onde se incluem as informações de localização, de identificação de fonte e destino, data, hora, duração da comunicação, tipo de comunicação e o equipamento utilizado.
II – Os serviços de telecomunicações compreendem, fundamentalmente, os dados de base, os dados de tráfego e os dados de conteúdo.
III – Os dados de base são os dados respeitantes à conexão à rede, ou seja, são os dados através dos quais o utilizador da rede de telecomunicações tem acesso à ligação.
IV – Os dados de tráfego correspondem aos dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede.

V – Por último, os dados de conteúdo são os dados alusivos ao conteúdo da comunicação ou da mensagem.
VI – Os dados de localização, inseridos no âmbito dos dados de tráfego, são os dados tratados numa rede de comunicações eletrónicas que indicam a posição geográfica do equipamento terminal de um assistente ou de qualquer utilizador de um serviço de comunicações eletrónicas acessíveis ao público.
VII– Só cabem dentro dos dados de localização os autênticos dados de comunicação ou de tráfego, i.e., aqueles que se reportam a comunicações efetivamente realizadas ou tentadas/falhadas entre pessoas.
VIII - O regime estabelecido pela Lei n.º 32/2008, de 17 de Julho, aplica-se à obtenção de dados correspondentes a comunicações já ocorridas e que se encontram preservados ou conservados.
IX – Tratando-se de obter prova por "localização celular conservada", isto é, concernente aos dados previstos no artigo 4.º, n.º 1, da Lei n.º 32/2008, o regime processual aplicável assume especialidade nos artigos 3.º e 9.º deste diploma, regime que, sendo especial, se sobrepõe ao de carácter geral instituído pelos artigos 12.º a 17.º da Lei n.º 109/2009, de 15 de Setembro – Lei do Cibercrime –, a qual, de resto, expressamente ressalva, no artigo 11.º, n.º 2, que as suas disposições processuais não prejudicam o regime do outro corpo de normas referido.
X – Já o artigo 189.º, n.º 2, do CPP, com a extensão do regime das escutas telefónicas nele consagrada, remetendo para os requisitos de admissibilidade fixados no artigo 187.º, n.ºs 1 e 4 do mesmo diploma, tem em vista os dados recolhidos em tempo real.
XI – Por sua vez, a aplicação da Lei 41/2004, de 18 de Agosto, limita-se à proteção contratual, no contexto das relações estabelecidas entre as empresas fornecedoras de serviços de comunicações eletrónicas e os seus clientes, não sendo lícito recorrer a ela para efeitos de investigação criminal.
XII – Mesmo a considerar-se aplicável este diploma, à luz do artigo 6.º, n.º 2, ele não permitiria o pedido de dados de localização.
XIII – A declaração de inconstitucionalidade, com força obrigatória geral, das normas a que se reporta o recente Acórdão n.º 268/2022 do Tribunal Constitucional, tendo por base a consideração de que as mesmas permitiam lesão desproporcionada da reserva da intimidade e da vida privada dos cidadãos, veda o acesso aos dados não permitidos com recurso à Lei 32/2008; de outro modo, a declaração de inconstitucionalidade permitiria o efeito contrário àquele que definiu.
IVX – Não existindo qualquer identidade formal ou material entre a previsão legal do artigo 2.º, n.º 1, alínea a), da Lei n.º 32/2008 e o catálogo de crimes delineado no artigo 187.º, n.º 1 e 189.º, do CPP – com a "virtual" exceção da

alínea b) do n.º 1 do artigo 187.º –, não há revogação do segundo pelo primeiro dos dois regimes.
XV – Se assim é, não se tem de aplicar, por repristinação, nenhuma norma do CPP.
XVI – "Caída" a Lei 32/2008, e na impossibilidade de aplicação do CPP e da Lei 41/2004, recorrer, na questão da localização celular, às normas da Lei 109/2009 seria seguir um caminho espúrio, face à enunciada declaração de inconstitucionalidade e aos fundamentos que a determinaram.
XVII – O que significa que no caso específico de obtenção por localização celular conservada, isto é, a obtenção dos dados previstos no artigo 4.º, n.º 1, da Lei 32/2008, o regime processual aplicável assume especialidade nos artigos 3.º e 9.º deste diploma (para estes casos ganhando relevo o conceito de «crime grave», já que nos termos do artigo 3.º, n.º 1, ainda do mesmo compêndio legislativo, a obtenção de prova da localização celular conservada só é prevista para crimes que caibam nesse conceito) - desaparecendo a especialidade, não é consentido recorrer à generalidade e permitir localização celular para além desses crimes é defraudar o espírito do legislador.
XVIII – A faturação detalhada, integrando também dados de tráfego relativos às comunicações efetuadas – pelo menos, informações atinentes a todas as chamadas realizadas num determinado período, números de telefone chamados, data da chamada, hora de início e duração de cada comunicação –, inviabiliza a aplicação da norma do artigo 14.º, n.º 4, da Lei 109/2009, não sendo também de aplicar o preceito contido no artigo 18.º, apenas destinado a interceções em tempo real, a exemplo das normas do CPP para que remete, anotando-se ainda que, no caso dos autos, o prazo de três meses, previsto no artigo 12.º, n.º 3, já se extinguiu.»
Este acórdão contém voto de vencida da 1.ª adjunta, que, em síntese, sustenta o seguinte:
«Os artigos 1º, nº 4 e 6º nº 7, da Lei 41/2004, afastam expressamente do seu âmbito de aplicação a conservação de dados para fins de prevenção, investigação e repressão de infracções penais, as quais são definidas em legislação especial, só se aplicando à relação contratual.
O mesmo não sucede com a transmissão dos dados de localização e de tráfego legitimamente conservados às autoridades competentes, quando solicitados ao abrigo dos artigos 11º, 14º e 18º, da Lei do Cibercrime, para efeitos de investigação criminal que é legitima e conforme os princípios constitucionais de proporcionalidade, nas vertentes de proibição do excesso e proibição da insuficiência e do principio da proibição da alienação do fim.
A Lei do Cibercrime contém normas especiais relativamente à Lei geral nº 41/2004, que não se excluem, antes se complementam, no que respeita à

obtenção dos dados para fins criminais.
A Lei 41/2007 não enferma de nenhum dos vícios apontados à Lei 32/2008 no Acórdão do Tribunal Constitucional nº 268/2022, não tendo sido, sequer, objecto de apreciação.
A base de dados armazenados pela Lei 41/2004, não se destina à investigação criminal, como sucedia na Lei 32/2008, pelo que a declaração de inconstitucionalidade não impede a conservação dos dados para as finalidades previstas da Lei n. 41/2004, nem os posteriores acesso e utilização dos mesmos na investigação criminal.
Note-se, aliás, que, antes da entrada em vigor da Lei 32/2008, da reforma do Código de Processo Penal e a da Lei 109/2009, a jurisprudência admitia a obtenção dos dados de tráfego, que já então eram conservados à luz da Lei 41/2004, junto dos operadores de comunicações eletrónicas (cf., entre outros, os Acórdãos do Tribunal desta Relação de Coimbra de 17 de maio de 2006 e de 15 de novembro de 2006; do Tribunal da Relação de Guimarães de 10 de janeiro de 2005 e do Tribunal da Relação de Évora de 26 de junho de 2007, em www.dgsi.pt)
Igual posição foi assumida no Parecer do Conselho Consultivo da Procuradoria Geral da República, P000792008, publicado no Jornal Oficial em 2 de outubro de 2009, acessível em www.dgsi.pt.
No caso vertente, estando em causa a investigação de um crime (de incêndio) não abrangido pelo catálogo de crimes enunciados no artigo 2º, n. º1, alínea g) da Lei 32/2008, com um suspeito devidamente identificado e revelando-se essencial à investigação obter informação sobre os dados de trafego e de localização, concederia provimento ao recurso do Ministério Público.»

- Acórdão do Tribunal da Relação de **Coimbra** de 23.11.2022:
«I – A facturação detalhada referente às comunicações telefónicas integra o conceito de dados de tráfego.
II – O regime dos artigos 187.º a 189.º do CPP mantém a sua aplicação relativamente a escutas telefónicas, nomeadamente quanto à intercepção e à gravação de conversações ou comunicações telefónicas, quando verificados os requisitos previstos no n.º 1 do primeiro dos dois artigos referidos e relativamente aos crimes aí previstos.
III – O regime de extensão contido no artigo 189.º do CPP continua a ter a aplicação prática prevista no artigo 18.º da Lei n.º 109/2009, de 15-09 (“Lei do Cibercrime”).
IV – A obtenção de prova electrónica preservada ou conservada em sistemas informáticos está actualmente submetida ao regime previsto nos artigos 11.º a 19.º da Lei n.º 109/2009».

- Acórdão do Tribunal da Relação de **Coimbra** de 27.09.2023:
«I – Os dados de base são os que respeitam ao acesso à rede e permitem identificar o utilizador do equipamento (endereços de protocolos de IP, identidade civil do titular, números de telefone e endereços de correio eletrónico), e os dados de tráfego são os que revelam circunstâncias das comunicações, como a localização dos intervenientes na comunicação, duração, data, hora das comunicações interpessoais, mas também os que não pressupõem uma comunicação interpessoal.
II – No acórdão n.º 268/2022, de 19 de Abril, o Tribunal Constitucional declarou, com força obrigatória geral, violar o princípio constitucional da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada, ao sigilo nas comunicações, ao livre desenvolvimento da personalidade, à autodeterminação informativa e à tutela jurisdicional efetiva a recolha, o registo, conservação e acesso de dados pessoais, de tráfego e localização em relação a todos os assinantes e utilizadores registados nas empresas fornecedoras de serviços de comunicações eletrónicas, de modo generalizado e indiferenciado e em relação a todos os meios de comunicação eletrónica, durante um e para fins criminais, nos termos previstos nos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de Julho.
III – Idêntica censura mereceu a ausência de notificação ao visado de que os seus dados tinham sido acedidos, devido ao entendimento de que o direito à autodeterminação informativa e a uma tutela jurisdicional efetiva ficariam comprimidos de forma desproporcionada.
IV – O Tribunal Constitucional entende que a conservação dos dados de base, enquanto medida restritiva dos direitos à reserva da intimidade da vida privada e à autodeterminação informativa, respeita o princípio da proporcionalidade, uma vez que apenas identificam os utilizadores do meio de comunicação e não pressupõem a análise de qualquer comunicação.
V – No acórdão n.º 268/2022, de 19 de Abril, o Tribunal Constitucional não fiscalizou, nem censurou outras normas, para além das dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de Julho, nem outros diplomas legais, não tendo, por isso, a declaração de inconstitucionalidade dele emanada a virtualidade de abranger toda e qualquer prova obtida por meios digitais.
VI – O Tribunal Constitucional não entendeu estarem feridas de inconstitucionalidade as normas do C.P.P. que preveem a possibilidade de obter e juntar aos autos dados sobre a localização celular ou registos de realização de conversações ou comunicações quanto a crimes previstos no n.º 1 do artigo 187.º, nem afastou a possibilidade de conservação de dados ao abrigo de outros diplomas, por exemplo para fins contratuais, de que é

exemplo a Lei n.º 41/2004, de 18 de Agosto, que prevê a conservação de dados de tráfego por um período de 6 meses.
VII – São válidas as provas obtidas a partir de dados guardados pelas operadoras respeitando os limites impostos legalmente pelas leis que se mantêm em vigor e que continuam a prever a possibilidade de obtenção, guarda e transmissão de tais dados.
VIII – Informações da Ascendi, de onde se retire a hora e local de passagem de determinados veículos em autoestradas nacionais, informações da Via Verde, de onde se retire a existência ou inexistência de registos relativamente a determinadas viaturas, e da Brisa, dando conta de uma cessão de posição contratual num contrato de concessão outorgado pelo Estado e do não tratamento de dados solicitados, informações bancárias, aditamentos a autos de notícia elaborados na sequência de observação directa de agentes da autoridade, não colidem com a declaração de inconstitucionalidade em causa, porque não são dados funcionais necessários ao estabelecimento de uma comunicação, nem são abarcadas pelas considerações que fundamentaram o juízo de inconstitucionalidade.
(…)».

- Acórdão do Tribunal da Relação do **Porto** de 29.03.2023:
«A declaração de inconstitucionalidade com força obrigatória geral do artigo 4.º, conjugado com os artigos 6.º e 9.º, todos da Lei n.º 32/2008, de 17 de julho, não impede a possibilidade de se autorizar a obtenção de dados de tráfego ou de localização celular conservados no âmbito da Lei n.º 41/2008, de 18 de agosto, com fundamento no artigo 189.º, n.º 2, do Código de processo Penal.»
- Acórdãos do Tribunal da Relação do **Porto** de 18.01.2023 e de 01.02.2023:
«I – Os fundamentos de inconstitucionalidade declarada, com força obrigatória geral, no ac TC n.º 268/2022, de 19.04, não têm aplicação na interceção de dados de tráfego, incluída localização celular, em tempo real durante a investigação.
II – A interceção de dados de tráfego, como a faturação detalhada, onde constem as chamadas efetuadas e recebidas (trace-back), as localizações celulares e a identificação dos números que os contactem e as comunicações em roaming, quando obtidas em tempo real, durante a investigação, em relação a suspeitos ou arguidos (nº 4, al.a) do art.187º, do CPP), não implica uma ingerência desproporcional nos direitos fundamentais ao respeito pela vida privada e familiar e à proteção de dados pessoais previstos nos art.ºs 7.º e 8.º da C.D.F.U.E., bem assim nos nºs 1 e 4 do art.35.º e do n.º 1 do art.26.º, da C.R.P.

III – À semelhança dos dados de conteúdo (escutas telefónicas), a interceção de dados de tráfego, incluídas localizações celulares, em tempo real, durante a investigação, pressupõe a interceção ou monitorização dos mesmos, à semelhança das escutas telefónicas, e não o recurso a base de dados de conservação ou armazenamento das operadoras relativas a todos os assinantes e utilizadores registados, situação, única, a que se refere o ac TC 268/2022 e a Lei nº32/2008, de 17 de julho.
IV – Permitir o acesso e valoração no processo penal de metadados obtidos e tratados para efeitos de faturação entre cliente e operadora é o mesmo que consentir na sua utilização para uma finalidade diferente daquela para a qual foram conservados, defraudando o âmbito de regulamentação prevista na Lei 41/2004, de 18 de agosto, para acudir à investigação criminal.
V – Relativamente aos dados de tráfego, incluídas localizações celulares, em tempo real, o regime de extensão contido no artigo 189.º, nº2, continua a ter a aplicação aos crimes de catálogo previsto no art.187º, nº1, ambos do Código Processo Penal. Nesse caso, também o regime especial do art.18º, nº1 e 3, da Lei n.º 109/2009, de 05.09 (Lei do Cibercrime) continua a ter a aplicação aos crimes de catálogo previstos nesse normativo.
VI – O arguido ou suspeito, cujos dados de trafego e dados de localização virão a ser intercetados, beneficia das garantias de controlo estabelecidas para as escutas telefónicas nos art.s 187º e 188º, do CPP, aqui aplicáveis mutatis mutandi, não havendo razão para impor à interceção de dados de tráfego, em tempo real, uma comunicação que é dispensada na interceção de dados de conteúdo (escutas telefónicas), a pretexto do direito à autodeterminação informativa e tutela jurisdicional efetiva previstos no n.º 1 do art.35.º e do n.º 1 do art.20.º, da C.R.P..»
- Acórdão do Tribunal da Relação do **Porto** de 18.01.2023:
«I – Com a entrada em vigor da Lei n.º 32/2008, de 17.07, ficou, no que concerne aos dados conservados, revogado o regime processual penal previsto nos art.ºs 187.º a 189.º do CPP.
II - O regime dos art.ºs 187.º a 189.º do CPP não é aplicável aos dados abrangidos pela Lei n.º 32/2008, a tal não obstando a declaração de inconstitucionalidade, com força obrigatória geral, das normas constantes dos art.ºs 4.º, 6.º e 9.º da referida Lei.
III - Ainda que assim não fosse, permitir o acesso aos dados de trafego e aos dados de localização com base naquelas disposições afrontaria claramente o direito europeu e a interpretação que dele faz a jurisprudência do TJUE, materializando uma agressão mais intensa e desproporcional dos direitos fundamentais à intimidade da vida privada e à proteção de dados pessoais previstos nos art.ºs 7.º e 8.º da Carta dos Direitos Fundamentais da União

Europeia (CDFUE) do que a Diretiva n.º 2006/24/CE, entretanto declarada inválida.
IV - Com efeito, o regime dos art.ºs 187.º e 189.º do CPP nem sequer obedece às imposições da Diretiva, contrariamente ao que veio a suceder com a Lei n.º 32/2008, que, inclusivamente, até foi além do que era imposto no que concerne a normas que garantem a segurança dos dados conservados e critérios disciplinadores do acesso aos dados armazenados.»
- Acórdão do Tribunal da Relação do **Porto** de 07.12.2022:
«I – Tendo o acórdão do Tribunal Constitucional declarado a inconstitucionalidade, com força obrigatória geral, dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de julho (Lei relativa à conservação de dados gerados ou tratados no contexto de oferta de serviços de comunicações eletrónicas), não podemos tentar tornear esse acórdão, "deixando entrar pela janela" aquilo a que ele "fechou a porta"; ou seja, não podemos recorrer a outras normas para obter o mesmo efeito que resultaria da aplicação das normas declaradas inconstitucionais sem que essas outras normas contenham aquelas garantias que faltam a estas e que levaram a essa declaração de inconstitucionalidade.
II – Não é, por isso, legalmente possível recorrer para esse efeito aos regimes dos artigos 187.º e 189.º do Código de Processo Penal (relativo às comunicações em tempo real, não à conservação de dados de comunicações pretéritas), da Lei n.º 4172008, de 18 de agosto (relativo à proteção contratual no contexto das relações entre empresas fornecedoras de serviços de comunicações eletrónicas e seus clientes, campo distinto do da investigação criminal) e da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime).
III – Não podem os tribunais substituir-se ao legislador suprindo omissões de onde resultam graves inconvenientes para a investigação criminal.»
- Acórdão do Tribunal da Relação do **Porto** de 29.03.2023:
«A declaração de inconstitucionalidade com força obrigatória geral do artigo 4.º, conjugado com os artigos 6.º e 9.º, todos da Lei n.º 32/2008, de 17 de julho, não impede a possibilidade de se autorizar a obtenção de dados de tráfego ou de localização celular conservados no âmbito da Lei n.º 41/2008, de 18 de agosto, com fundamento no artigo 189.º, n.º 2, do Código de processo Penal.»
- Acórdão do Tribunal da Relação do **Porto** de 24.05.2023:
«I - A declaração de inconstitucionalidade do Acórdão do Tribunal Constitucional n.º 268/2022 respeita apenas a dados - de tráfego e de localização - previamente conservados/armazenados, à conservação generalizada e indiferenciada dos dados de tráfego e não a dados de tráfego em tempo real; por isso, a declaração de inconstitucionalidade não afeta os dados de tráfego gerados concomitantemente aos dados de conteúdo

(interceção de conversações ou comunicações telefónicas), posto que, uns e outros, se mostram obtidos em tempo real.
II - A obtenção e transmissão dos dados de tráfego e de localização, em tempo real, neles se incluindo o registo de chamadas efetuadas e recebidas, faturação detalhada e respetiva localização celular, conexos com as comunicações intercetadas, não implica uma ingerência desproporcional nos direitos fundamentais ao respeito pela vida privada e familiar e à proteção de dados pessoais previstos nos art.ºs 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (CDFUE); isto porque, à semelhança dos dados de conteúdo (escutas telefónicas), a interceção de dados de tráfego em tempo real não abrangeria, de forma generalizada, todos os assinantes e utilizadores registados, mas apenas os suspeitos ou arguidos investigados, não estando, também por esse motivo, abrangidos pela declaração de inconstitucionalidade do Acórdão do Tribunal Constitucional n.º 268/2022.»

- Acórdão do Tribunal da Relação de **Lisboa** de 22.02.2023:
«O disposto no art. 9° da Lei 32/2008 só foi declarado inconstitucional, com força obrigatória geral (relativa à transmissão de dados armazenados às autoridades competentes para investigação, deteção e repressão de crimes graves), na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros.
–O referido art. 9°, no seu conteúdo não foi declarado inconstitucional desde que o visado seja notificado de que os dados conservados foram acedidos pelas autoridades de investigação criminal.
–A norma do art. 4º da Lei 32/2008 foi declarada inconstitucional com força obrigatória geral quando conjugada com o art. 6° da mesma Lei, ou seja, o que é inconstitucional é a obrigação para os fornecedores de serviços (de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações) conservarem os dados previstos no art. 4° pelo período de um ano a contar da data da conclusão da comunicação.
–A possibilidade de transmissão de dados de tráfego no âmbito de processo criminal não está prevista apenas na Lei 32/2008 de 17.07.
Não só o art. 189°, n° 2 do Cód. Proc. Penal, mas também o art. 14° da Lei 109/2009 de 15.09 (Lei do Cibercrime) permitem essa possibilidade.
–A investigação criminal no que se refere à obtenção, nomeadamente, de dados de tráfego, não está limitada à previsão da citada Lei 32/2008;
–O n° 2 do art. 189° do Cód. Proc. Penal, não se reporta à obtenção de "dados dinâmicos", ou seja, que estejam a ser transmitidos em tempo real, por

oposição a dados “preservados ou armazenados”».
- Acórdão do Tribunal da Relação de **Lisboa** de 26.01.2023:
«I - Nos termos dos artigos 187.º a 189.º do CPP é lícita, entre outras, a utilização dos dados de localização celular desde que a sua guarda e entrega resulte de despacho do juiz, no âmbito de uma investigação criminal, apenas se podendo utilizar como prova aqueles que forem registados e entregues após tal decisão, uma vez que este regime em nada foi beliscado pela publicação da Lei n.º 32/2008, de 17/06, nem pela sua declaração de inconstitucionalidade proferida no Acórdão do TC n.º 268/2022, de 19/04.
II - O regime dos artigos 187.º a 189.º do CPP foi alargado e estendido por esta Lei 32/2008, de 17/06, tendo agora, com a declaração de inconstitucionalidade, ficado reduzido à sua inicial dimensão.
III - A Lei 32/2008 referida não procedeu à revogação daquele regime, pois isso teria impedido, durante a sua vigência, a aplicação do art.º 189.º, n.º 2, do CPP aos outros crimes referidos no art.º 187.º não abrangidos pela definição de crimes graves de tal Lei, sendo certo que tal se não verificou.
IV - O art.º 189.º, n.º 2, foi incluído no Código de Processo Penal pela Lei n.º 48/2007, de 29/08, para, precisamente, regular os termos em que estes dados poderiam ser requisitados e juntos ao processo, pois alguns de tais dados (metadados) já eram guardados temporariamente pelas operadoras para efeitos designadamente de faturação dos serviços prestado.
V - Os dados de localização celular que sejam remetidos a um processo e que provenham de operações de conservação prévia (ao referido despacho) dos mesmos, estão abrangidos pela declaração de inconstitucionalidade do Acórdão do TC n.º 268/2022, de 19/04, pelo que constituem prova proibida, ainda que na data da sua conservação já estivesse pendente processo contra a pessoa em relação à qual os dados são solicitados.
VI - Assim, a aludida imposição de armazenamento extenso, universal e indiscriminado foi objeto de declaração de inconstitucionalidade. Todavia, não foi julgado inconstitucional armazenar dados, desde que tal operação respeite a restante legislação em vigor.
VII - Em relação aos dados relativos a registos de realização de conversações ou comunicações, poderão os mesmos resultar da prolação de decisão a esse respeito ou ser obtidos, mediante idêntica decisão, a partir dos registos efetuados nos termos e para os efeitos do art.º 6.º da Lei n.º 41/2004, de 18/08, os quais terão sempre o limite temporal previsto no n.º 3 deste artigo, uma vez que a decisão do TC não se pronunciou expressamente sobre esta questão; a mencionada Lei n.º 41/2004 contém um regime extremamente restritivo em relação aos dados sobre localização, constante do seu artigo 7.º, o que, só por si, constituiu uma das justificações para o regime estabelecido

pela Lei n.º 32/2008, de 17/06, que impôs a sua guarda por um ano.
VIII - O artigo 189.º, n.º 2, do CPP, prevê expressamente a possibilidade de obtenção de localizações celulares quanto aos crimes previstos no art.º 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo (incluindo, portanto, a alínea b – intermediário).
IX - Independentemente da qualificação como intermediário ou suspeito de determinada pessoa, o n.º 2 do art.º 189.º do CPP não procede a qualquer distinção neste campo, afirmando perentoriamente que o seu regime é aplicável "(…) em relação às pessoas referidas no n.º 4 do mesmo artigo", onde se incluem os intermediários.
X - Sendo proferida decisão para cujo teor contribuiu prova proibida prevista no art.º 126.º, n.º 3, do CPP, ocorre nulidade, que apenas é sanável mediante consentimento do visado.
XI - Caso falte tal consentimento, a nulidade deve considerar-se insanável. A situação assim criada cai assim sob a alçada do disposto no art.º 410.º, n.º 3, do CPP, e tem como consequência a anulação da decisão e a sua repetição pelo mesmo tribunal, mas desta feita sem a ponderação da prova proibida.»

- Acórdão do Tribunal da Relação de **Évora** de 28.03.2023:
«O art. 189.º, n.º 2, do Código de Processo Penal permite aceder a dados de tráfego, neste caso, dados sobre a localização celular ou de registos da realização de conversações ou comunicações e, por maioria de razão [in eo quod plus est, sempre inest et minus (no que é mais está sempre compreendido o que é menos)], a dados de base relacionados, neste caso, com a identificação dos titulares dos cartões de telemóvel [nos quais, como salienta o acórdão do TC 268/2022, «o grau de agressão ao direito à intimidade da vida privada (…) é menos gravoso do que os demais metadados elencados no artigo 4.º da Lei n.º 32/2008, de 17 de Julho (pois apenas identificam o utilizador do meio de comunicação em causa)»], aos quais o MP sempre poderia aceder por via do disposto no art. 14.º, n.ºs 1 e 4, al. b), da Lei 109/2009, de 15.09 (Lei do Cibercrime), quando se investiguem os crimes previstos no n.º 1 do artigo 187.º, nomeadamente, crimes puníveis com pena de prisão superior, no seu máximo, a 3 anos.
Tratando-se de elementos de identificação constantes dos contratos celebrados com os operadores e/ou ligados ao reconhecimento da posse de equipamentos móveis, os respetivos registo e fornecimento à autoridade judiciária competente não importam desproporcionalidade ou desadequação face ao fim em vista, nem a afetação do direito fundamental à autodeterminação informativa.
Nem demanda tal acesso, sem relação com qualquer comunicação efetuada,

notificação específica ulterior, assemelhando-se, do ponto de vista da natureza e do regime, à obtenção, em processo penal, de outros dados pessoais, mormente, de identificação.
Destarte, os ditos elementos probatórios recolhidos mostram-se válidos, não integrando prova proibida e suficientes para alicerçarem o pedido de autorização das buscas domiciliárias, nos termos dos artigos 174º, nºs 1 e 2 e 177, do CPP.»

- Acórdão do Tribunal da Relação de **Guimarães** de 02.05.2023:
«I- A Lei nº 32/2008, de 17.07, que transpôs para a ordem jurídica interna a Diretiva n.º 2006/24/CE, de 15 de março, que alterou a Diretiva n.º 2002/58/CE, de 12 de Junho, regula a conservação e a transmissão dos dados de tráfego e de localização de comunicações eletrónicas relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes.
II- A Diretiva 2006/24/CE, visou (face às grandes divergências de leis nacionais que criavam sérias dificuldades práticas e de funcionamento do mercado interno) estabelecer normas de harmonização, no espaço da União Europeia, de conservação de dados de tráfego e dados de localização, bem como dados conexos necessários para identificar o assinante ou o utilizador registado, que são normas de tratamento dos dados pelos fornecedores de comunicações para determinada finalidade, mas não regulou, nem podia regular, a atividade das autoridades públicas (órgãos de polícia criminal, Ministério Público, juízes e tribunais) com competência para assegurar a realização daquela finalidade.
III- Importa distinguir a atividade de conservação de dados de tráfego e de localização da atividade de acesso a esses dados, as quais constituem ingerências distintas em matéria de direitos fundamentais, como é o caso do direito à privacidade.
IV- O regime de acesso a dados pessoais pelas autoridades competentes, para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais encontra-se previsto na Lei n.º 59/2019, de 08.08 (Lei de Proteção de Dados Pessoais), que transpôs a Diretiva (UE) 2016/680.
V- O acesso, no âmbito do processo penal, a dados conservados na posse de fornecedores de serviços de comunicações encontra-se previsto nos artigos 187.º a 189.º e 269.º, n.º 1, al. e), do CPP e na Lei n° 109/2009, de 15 de setembro (Lei do Cibercrime).

VI- Nesta conformidade, por se situarem em planos distintos, a Lei nº 32/2008, de 17.07, não revogou, nem podia ter revogado os artigos 187º a 189 do CPP.
VII- O legislador, na Lei nº 32/2008, de 17.07, excedeu-se na transposição da Diretiva 2006/24/CE , legislando não apenas sobre a conservação e a transmissão de dados, mas também sobre o acesso a esses dados para prova em processo penal (cfr. artigo 9º, declarado inconstitucional pelo Ac. TC nº 268/2022). Ora, tal alteração deveria ter sido efetuada no local próprio, ou seja, no Código de Processo Penal, o que não sucedeu, mantendo-se inalterada a redação dos artigos 187º, nº 1 e 189º, nº 2. Em resultado disso passou a existir um catálogo de crimes para cuja prova desses dados poderiam ser utilizados, ou seja, os crimes graves previstos no artigo 2º, nº 1 al. g), que é diferente do catálogo previsto para as interceções do nº 1 do artigo 187º do CPP.
VIII- O artigo 189º, nº 2 do CPP, que não foi revogado pela Lei nº 32/2008, de 17.07, constitui, pois, a norma fundamento para acesso aos dados tráfego e de localização conservados para prova dos crimes previsto no nº 1 do artigo 187º do CPP que não integram o conceito de crimes graves do artigo 2º, nº 1 al. g) da referida lei.
IX- Mas ainda que assim não fosse, atualmente face à declaração de inconstitucionalidade com força obrigatória geral do artigo 9º da Lei nº 323/2008, de 17.07, por força do Ac. TC nº 268/2022, tendo em conta o preceituado no artigo 282º da CRP, o nº 2 do artigo 189º do CPP sempre seria de considerar-se repristinado. O que quer dizer que atualmente este preceito legal sempre constituiria a única norma que permite o acesso a dados de tráfego e de localização conservados relativamente aos crimes indicados no nº 1 do artigo 187º do CPP.
X- O acórdão do Tribunal Constitucional nº 268/2022 manteve intocado o referido regime acesso a dados conservados pelas autoridades com vista à investigação de determinados crimes, designadamente os referidos artigos 187º a 189º do CPP e a aludida Lei nº 109/209 (Lei do Cibercrime).
XI- Mas, declarada a inconstitucionalidade com força obrigatória geral da Lei nº 32/2008, com o sentido que ficou assinalado, e tendo anteriormente sido declarada invalidade a Diretiva 2006/24/CE (Acórdão de 08.04.2014, Digital Rights Ireland) subsiste a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12.06, transposta pela Lei nº 41/2004, de 18.08.
XII- A Lei 41/2004, de 18.08, grosso modo, impõe aos fornecedores de serviços de comunicações eletrónicas a obrigação de conservarem os dados de tráfegos e de localização para efeitos de faturação pelo prazo de 6 meses contados de cada comunicação.
XIII- Não se destinando, segundo esta lei, os dados conservados para efeitos

de prova em processo penal, nada obsta a que eles possam ser utilizados para esse efeito.»
- Acórdão do Tribunal da Relação de **Guimarães** de 17.10.2023:
«1. Tal como a Directiva 2006/24/CE não revogou a Directiva 2002/58/CE – excepto no aditamento do n.º 1-A ao art. 15.º desta última –, a Lei n.º 32/2008 não revogou a Lei n.º 41/2004 no plano da mera conservação dos dados e passou a coexistir com a mesma, ainda que com diferentes âmbitos de aplicação, nomeadamente no que respeita ao catálogo de crimes relevantes e ao prazo de conservação dos dados.
2. Do mesmo modo, no plano do acesso aos dados conservados, impõe-se entender que o art. 9.º da Lei n.º 32/2008 não revogou totalmente o art. 189.º, n.º 2, do CPP, sem prejuízo da respectiva e exclusiva derrogação na parte relativa aos dados conservados e à extensão do catálogo de crimes relevantes
3. A inconstitucionalidade com força obrigatória geral declarada no Acórdão do Tribunal Constitucional n.º 268/2022, afectou o regime jurídico nacional de conservação e de transmissão de dados gerados pelas comunicações electrónicas.
4. Com esta declaração de inconstitucionalidade com eficácia ex tunc, passou a ser inequívoco que os operadores de comunicações móveis já não podem conservar ou transmitir dados ao abrigo dos artigos 4.º a 6.º, e bem assim, do art. 9.º da Lei n.º 32/2008.
5. Afastada a aplicação da Lei n.º 32/2008, a conservação de dados de localização pelos operadores de comunicações móveis e a respectiva transmissão à autoridade judicial fica integralmente sujeita ao já acima analisado regime previsto no art. 189.º, n.º 2, do Código de Processo Penal (redaçcão da Lei n.º 48/2007), e na Lei n.º 41/2004, de 18 de Agosto, maxime artigos 1.º, n.ºs 2, 4 e 5, art. 2.º, n.º 1, al. e), 5.º, 6.º, n.ºs 2 e 3, e 7.º (redacção da Lei n.º 46/2012), incluindo a remissão aqui operada para o prazo de prescrição de seis meses do direito ao recebimento do preço dos serviços prestados, previsto no art. 10.º, n.º 1, da Lei 23/96, de 26 de Julho (redacção da Lei n.º 24/2008).
6. Em virtude do efeito repristinatório previsto no n.º 1 do art. 282.º da Constituição, a declaração de inconstitucionalidade em apreço não pode deixar de afectar a aludida derrogação tácita do art. 189.º, n.º 2, do Código de Processo Penal (na redaçcão da Lei n.º 48/2007) operada pelo art. 9.º da Lei n.º 32/2008 e, consequentemente, a norma do art. 189.º, n.º 2, do Código de Processo Penal, regressa à sua amplitude anterior à entrada em vigor da Lei n.º 32/2008.
7. Assim, por um lado, a obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou

comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz quanto a crimes previstos no art. 1.º do art. 187.º do CPP e em relação a pessoas referidas no n.º 4 do mesmo artigo (art. 189.º, n.º 2, do CPP).
8. Por outro lado, os operadores de comunicações móveis só podem tratar e transmitir estes dados durante o prazo de seis meses após a prestação do serviço e devem responder aos pedidos de acesso a dados pessoais dos utilizadores apresentados pelas autoridades judiciárias competentes, nomeadamente ao abrigo do referido art. 189.º, n.º 2, do CPP, e da Lei n.º 41/2004.»
A diversidade das soluções jurisprudenciais ilustrada nas precedentes transcrições é bem demonstrativa da dimensão do problema que se coloca e da premência de se produzirem instrumentos legislativos que se harmonizem entre si e ponham cobro a tanta incerteza e insegurança jurídica, com incontornáveis reflexos negativos na imagem dos tribunais, que administram a justiça em nome do povo, e na confiança que este deposita naqueles.

3.2 - Efetuado o enquadramento do complexo quadro normativo e jurisprudencial em que nos movemos e tendo em perspetiva as considerações expendidas, importa atentar no caso concreto objeto do recurso.
O Ministério Público requereu, ao abrigo do disposto nos artigos 135º, 182º, 187, nº 1, al. a), nº 4, 188º, 189º, nº 2, 268º, nº 1, al. f), e 269º, nº 1, al. e), todos do Código de Processo Penal, que fossem dispensadas as operadoras de telecomunicações móveis "EMP01…/EMP02…", EMP03… e "EMP04…" do dever de sigilo e ordenada «a remessa aos presentes autos, em suporte digital e formato "excel", dos eventos de rede referentes aos códigos de antena indicados a fls. 09 (com a identificação dos titulares dos nºs de telemóvel aí acionados e respetivos IMEIS's e moradas), em virtude dos mesmos terem sido preservados e serem fundamentais para a descoberta da verdade, no período compreendido entre as 17h30 até às 18h30 do dia 28-08-2023.»
Mediante o despacho recorrido foi indeferida tal pretensão, por se entender, em suma, que estamos no domínio de acesso a dados de tráfego e de conteúdo, no âmbito do artigo 2º, n.º 1, al. a), da Lei n.º 32/2008 e, ainda, do regime da interceção e gravação de conversações ou comunicações telefónicas, nos termos dos artigos 187º, n.º 1, e 189º, ambos do Código Penal, que o crime investigado não corresponde a nenhum dos previstos nos artigos 2º, n.º 1, al. g), e 9º, n.º 1, da Lei n.º 32/2008 e, por outro lado, que se pretende que se aceda a dados de tráfego e de localização de um conjunto indeterminado de pessoas que efetuaram comunicações, acionando células de antenas de telecomunicações, e não de *suspeito*, como exigem o artigo 9º, n.º

3, al. a), da Lei n.º 32/2008 e o artigo 187º, n.º 4, al. a), do Código de Processo Penal.
Vejamos.
Em causa está a transmissão, por operadoras de serviços de telecomunicações, de dados conservados de tráfego e de localização celular emergentes da detenção e/ou utilização de aparelhos telefónicos, que, segundo o entendimento que sufragamos, é regulada e disciplinada especificamente pela Lei n.º 32/2008, nos moldes a que antes aludimos.
Contudo, nos presentes autos investigam-se factos suscetíveis de integrar a prática de um crime de incêndio, previsto e punível pelo artigo 274º, n.º 1, do Código Penal, com pena de prisão de 1 a 8 anos.
Ora, tal crime que não integra o catálogo de crimes que preenchem a definição de «crime grave» contemplada no artigo 2º, n.º 1, al. g), da Lei n.º 32/2008, complementada pelo esclarecimento constante do artigo 1º, alíneas i), j) e m) do Código Penal quanto ao que deve entender-se por «terrorismo», «criminalidade violenta» e «criminalidade altamente organizada».
Com efeito, a obtenção de prova de localização celular conservada apenas pode ser admitida quando está em causa *crime grave* de acordo com a apontada restrita definição, sendo este pressuposto essencial de aplicação da Lei n.º 32/2008.
Como tal, mostra-se inexoravelmente arredada a aplicabilidade da Lei n.º 32/2008 e prejudicada a apreciação dos restantes pressupostos de que depende – nomeadamente a qualidade [processual] da pessoa a que se referem os dados cuja transmissão é pretendida, conforme exige o n.º 3 do artigo 9º [designadamente, o suspeito, previsto na al. a)] e, bem assim, a questão dos efeitos decorrentes da declaração de inconstitucionalidade de alguns dos seus dipositivos nos sobreditos termos.
De igual modo é de excluir a aplicabilidade do regime de extensão previsto nos artigos 189º, n.º 2, e 187º do Código de Processo Penal, porquanto é pedida a obtenção de dados passados conservados, e não de dados futuros ou em tempo real, circunstância que, só por si, perfilhando-se o entendimento *supra* explanado, a afasta de modo incontornável. Ainda que assim se não entendesse, pese embora esteja em causa crime incluído no catálogo de crimes elencados no artigo 187º, n.º 1 [mais concretamente, previsto na alínea a) – crimes puníveis com pena de prisão superior, no seu máximo, a 3 anos], já o mesmo não se verificava quanto ao catálogo de visados discriminados no n.º 4 do mesmo preceito, mormente pessoa com a qualidade processual de *suspeito* ou *arguido* [al. a)]. Com efeito, no inquérito ainda nem sequer há suspeitos. O artigo 1º, al. e), do Código de Processo Penal define «suspeito» como sendo *"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". Ora, como assertivamente se sustentou na decisão alvo de recurso, tem sido amplamente defendido pela jurisprudência dos Tribunais superiores que se os dados de localização celular que se pretendem obter não têm como alvo um suspeito, mas antes um universo de pessoas não identificadas e unidas apenas pelo simples facto de estarem num dado local num dado momento, não é admissível, pois, além de não respeitar os princípios da proporcionalidade e da adequação, não permitem o enquadramento no conceito jurídico-penal de "suspeito". Para além dos acórdãos ali citados, podem ver-se, ainda, outros, entre os quais os indicados [12] pela Ex.ma Procuradora-Geral Adjunta no seu parecer:
- Acórdão do Tribunal da Relação de Évora de 08.11.2011:
«Para o efeito da autorização de uma escuta telefónica ou, para o que nos interessa, da junção ao processo dos elementos a eu se refere o n.º 2 do art.º 189.º do CPP não é exigível que o " suspeito" seja uma pessoa identificada no processo, nomeadamente, através do seu nome, mas é necessário, pelo menos, que se trate de uma pessoa "concretizada" por meio do conhecimento de um mínimo de características que permita individualizá-lo relativamente às demais, pois, a não ser assim, ficaria desprovido de objecto o juízo de indiciação associado à evocada categoria de pessoas. Ora, no caso presente, são desconhecidas quaisquer características individualizadoras das pessoas que tenham praticado os factos sob investigação».
- Acórdão do Tribunal da Relação do Porto de 11.02.2015:
«I - A localização celular revela a localização de um detentor de telemóvel ou outro equipamento móvel, dando a conhecer o percurso que está a fazer ou fez e a sua mobilidade.
II – A obtenção de dados de localização celular afronta o direito á inviolabilidade das telecomunicações.
III – O principio da inviolabilidade dos meios de comunicação privada, vg. das telecomunicações, tem de recuar quando está em causa o direito fundamental de respeito pela
dignidade humana e o livre desenvolvimento da personalidade faz emergir as necessidades da justiça criminal.
IV – O artº 189º CPP torna extensivo o regime das escutas telefónicas à obtenção de dados sobre a localização celular.
V – O suspeito de um crime não tem de ser completamente identificado ou individualizado bastando que seja pessoa determinável ou identificável.
VI – Se os dados de localização celular que se pretendem obter não têm como alvo um suspeito, mas um conjunto de pessoas não identificadas e unidas apenas pelo simples facto de estarem num dado local num dado momento não

é admissível a obtenção de dados de localização celular relativos a um número indeterminado de pessoas.»
Nessa confluência, a Ex.ma Procuradora-Geral Adjunta emitiu parecer no sentido de que o recurso interposto pela Ex.ma Magistrada do Ministério Público em primeira instância não deverá obter provimento.
Outrossim, é de afastar a aplicação da Lei n.º 41/2004 a que o Ministério Público alude no recurso [cfr. conclusões 3 a 6], uma vez que, como vimos anteriormente, aquela se destina essencialmente a regular as relações entre as empresas fornecedoras de serviços de comunicações eletrónicas e os seus clientes, não sendo lícito lançar mão da mesma para efeito de investigação criminal [cfr. artigo 1º, n.ºs 4 e 5 e 6º, n.º 7], além de que os dados de localização apenas são processados excecionalmente e disponibilizados em situações muito restritas, nomeadamente para efeito de resposta a pedidos de emergência, nos termos do artigo 7º.
Finalmente, não é possível recorrer ao regime processual penal previsto na Lei n.º 109/2009 porquanto estão em causa dados resultantes de comunicações telefónicas – que integram a especial previsão da Lei n.º 32/2008 –, e não de comunicações eletrónicas, como antes assinalámos. Ainda que assim não se entendesse, o crime em investigação nos autos também não corresponde a nenhum dos que estão previstos no artigo 11º, n.º 1, da Lei n.º 109/2009, que é pressuposto do seu funcionamento.
Ante o exposto, improcede a pretensão recursiva do Ministério Público, sendo de manter o despacho recorrido.
*
III. – DISPOSITIVO

Nos termos e pelos fundamentos *supra* expostos, acordam os Juízes do Tribunal da Relação de Guimarães em julgar improcedente o recurso interposto pelo Ministério Público e confirmar o despacho recorrido.
*
Não é devida tributação.
*
*
(Elaborado pela relatora, e revisto e assinado eletronicamente pelos signatários – artigo 94º, n.ºs 2 e 3, do Código de Processo Penal)
Guimarães, 23 de janeiro de 2024

Isabel Gaio Ferreira de Castro[Relatora]
Fátima Furtado[1.ª Adjunta]
Anabela Varizo Martins (voto a decisão) [2.ª Adjunta]

[1] Todas as transcrições a seguir efetuadas estão em conformidade com o texto original, ressalvando-se, nalguns casos, a alteração da formatação do texto, da responsabilidade da relatora.
[2] Publicados no Diário da República, I.ª Série - A, de 19.10.1995 e 28.12.1995, respetivamente.
[3] *Vide* Germano Marques da Silva, Direito Processual Penal Português, vol. 3, Universidade Católica Editora, 2015, pág. 335; Simas Santos e Leal-Henriques, Recursos Penais, 8.ª ed., Rei dos Livros, 2011, pág. 113; Paulo Pinto de Albuquerque, Comentário do Código de Processo Penal, à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem, 4ª edição atualizada, Universidade Católica Editora, 2011, págs. 1059-1061
[4] Cfr. Código de Processo Penal Comentado, Henriques Gaspar e outros, 4.ª edição revista, pág. 774
[5] Neste sentido, cfr. o acórdão do Tribunal da Relação de Coimbra de 12.10.2022, disponível para consulta no sítio da internet http://www.dgsi.pt, tal como todos os demais acórdãos que, doravante, sejam referidos sem expressa menção de fonte de acesso.
[6] "Prova digital: as leis que temos e a lei que deveríamos ter", *in* Revista do Ministério Público, ano 35 (2014), n.º 139, págs. 36 e 37.
[7] *In* Comentário do Código de Processo Penal, 2.ª Edição, pág. 509
[8] *In* Técnica no Novo Código de Processo Penal. Exame, perícias e prova digital, Revista do CEJ, 1.º Semestre 2008, n.º 9, pág. 166
[9] Rui Cardoso, «A conservação e a utilização probatória de metadados de comunicações electrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – o que nasce torto…», consultável em R.M.P. – Revista do Ministério Público n.º 172, meses de outubro – dezembro, pg.41 " Seja o fundamento de acesso o artigo 189.º, n.º 2, do CPP, o artigo 9.º da Lei 32/2008 ou o artigo 14.º da LCC (hipóteses que analisaremos de seguida), nunca se trata de uma intercepção (a dados em transmissão), mas sim de acesso a dados de comunicações pretéritas (já armazenados). A intercepção, seja ela de comunicações telefónicas, de transmissão de dados informáticos ou ainda por outro meios técnicos, podendo incluir os respectivos metadados, é sempre para comunicações que estão a ocorrer, para dados que estão em transmissão, ou seja, em tempo real, e, por isso, necessariamente posteriores ao despacho que as autoriza/ordena".
[10] Publicado no Diário da República, Série I, de 03.06.2022, págs. 18-81

[11] Em outubro de 2023, a Assembleia da República aprovou alterações às referidas normas (Decreto n.º 91/XV da Assembleia da República, publicado no Diário da Assembleia da República n.º 26, II Série A, de 26 de outubro de 2023) com o intuito de conformar tais normas com a Lei Fundamental.
Entre as alterações propostas, com a assinalada finalidade, restringiu-se a conservação dos dados por parte dos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações ao território de Portugal ou de outro Estado-Membro da União Europeia e, portanto, em cujas jurisdições são assegurados níveis de proteção dos dados materialmente equivalentes àqueles que decorrem da Constituição e procedeu a uma densificação do período de conservação dos dados previsto no artigo 6.º, com o estabelecimento de regras diferenciadas em relação às diferentes categorias de dados em causa.
Assim, para os dados de base prevê-se a conservação de um ano e para os dados de tráfego e de localização o período de três meses a contar da data da conclusão da comunicação, considerando-se esse período prorrogado até seis meses, salvo se o seu titular se tiver oposto perante as referidas entidades à prorrogação dessa conservação.
Os prazos de conservação podem ser prorrogados por períodos de três meses até ao limite máximo de um ano, mediante autorização judicial fundada na sua necessidade para as finalidades referidas, requerida pelo Procurador-Geral da República.
Não obstante as alterações introduzidas pelo legislador, o Tribunal Constitucional, através do recente Acórdão n.º 800/2023, de 04 de dezembro, reprovou as alterações propostas no que tange aos dados de tráfego e de localização, considerando, em essência, que, apesar da redução do prazo de conservação, se mantinham ultrapassados os limites da proporcionalidade no que respeita ao respetivo âmbito subjetivo (ou seja, continua a ser geral e indiferenciada, e não seletiva, por não se dirigir, de forma direta, objetiva e não discriminatória, a pessoas que tenham uma relação com os objetivos da ação penal, antes continuando a atingir sujeitos relativamente aos quais não há qualquer suspeita de atividade criminosa), restringindo-se os direitos fundamentais à reserva da intimidade da vida privada e à autodeterminação informativa.
[12] Disponíveis para consulta em http://www.dgsi.pt