

Tribunal da Relação de Coimbra
Processo nº 116/24.8GAPCV-A.C1

Relator: FÁTIMA SANCHES

Sessão: 28 Maio 2025

Votação: MAIORIA COM * VOT VENC

Meio Processual: RECURSO CRIMINAL

Decisão: REVOGADA

PROTECÇÃO DE DADOS PESSOAIS

DADOS DE TRÁFEGO/LOCALIZAÇÃO

DADOS CONSERVADOS PARA EFEITOS DE FATURAÇÃO

ADMISSIBILIDADE DA UTILIZAÇÃO PROBATÓRIA DOS DADOS DE TRÁFEGO/LOCALIZAÇÃO CONSERVADOS

PRAZO DE CONSERVAÇÃO - SEIS MESES

Sumário

1 - A Lei nº 58/2019 (Lei de proteção de dados pessoais) no seu artigo 23º, nº 2, não impede a transmissão de dados pessoais entre entidades públicas para finalidades diversas das determinadas na recolha. E ainda que assim não fosse, o certo é que não tem de haver previsão expressa para que todos os meios de prova possam ser utilizados no processo penal, atento o princípio da legalidade e liberdade da prova consagrado no artigo 125.º do Código de Processo Penal, que estabelece serem admissíveis as provas que não forem proibidas por lei.

2 - Quanto aos dados de tráfego/localização, a ponderação à luz dos princípios da necessidade e da proporcionalidade está feita pelo legislador no artigo 189.º, n.º 2 do Código de Processo Penal, e igualmente se impõe ao aplicador por força direta do artigo 18.º, n.º 2, da CRP, devendo notar-se o Tribunal Constitucional não apreciou a questão da admissibilidade de utilização no processo penal dos dados conservados para efeitos de faturação.

3 - Não há, pois, qualquer omissão legislativa que, em consequência, seja óbice constitucional à conservação dos dados feita ao abrigo da Lei 41/2004,

não podendo esse argumento ser utilizado para recusar o acesso a esses dados para prova em processo penal com fundamento no artigo 189.º, n.º 2, do Código de Processo Penal, como o faz o despacho recorrido.

4 - É legalmente admissível a utilização probatória dos dados de tráfego/localização conservados, ao abrigo da Lei 41/2004, de 18.08, com o limite quanto ao prazo de conservação, que é de seis meses - artigo 6º, nºs 2 e 7 e artigo 10º da Lei nº 23/96, de 26.07.

5 - A declaração de inconstitucionalidade com força obrigatória geral - Acórdão do T.C. nº 268/2022 - do artigo 4º, conjugado com os artigos 6º e 9º da Lei nº 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 41/2008, de 18/8, com fundamento no artigo 189º, nº 2, do Código de Processo Penal (ou seja, quanto a crimes previstos no número 1 do artigo 187º e em relação às pessoas referidas no nº4 do mesmo artigo), preceito legal esse que não se reporta à interceção e gravação desses dados em tempo real, pois que estas já se encontram previstas nos artigos 187º e 188º do CPP e versam sobre dados de conteúdo, de tráfego e de localização.

6 - O nº 2 do artigo 189º do CPP inclui assim na sua previsão apenas o acesso a dados conservados ou armazenados (dados de tráfego e de localização).

Texto Integral

Acordam os Juízes da 4ª Secção Criminal do Tribunal da Relação de Coimbra:

I. RELATÓRIO

1. No Inquérito com o NUIPC116/24.8GAPCV, que corre termos no Tribunal Judicial da Comarca de Coimbra, no Juízo de Instrução Criminal de Coimbra, foi proferido despacho em 16-12-2024 com o seguinte teor (transcrição):

«Versam os presentes autos de inquérito a investigação da prática de factos consubstanciadores do crime de *perturbação da vida privada*, previsto e punido pelo art.º 190.º, n.º 2, do Código Penal, com **pena de prisão até 1 ano ou com pena de multa até 240 dias**.

Sob a epígrafe “intercepção de comunicações” dispõe o art.º 18.º da Lei 109/2009, de 15/09 (“Lei do Cibercrime”):

“1 - É admissível o recurso à interceptação de comunicações em processos relativos a crimes:

a) Previstos na presente lei; ou

b) Cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no artigo 187.º do Código de Processo Penal.

2 - A interceptação e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, 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, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público.

3 - A interceptação pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar apenas a recolha e registo de dados de tráfego, devendo o despacho referido no número anterior especificar o respectivo âmbito, de acordo com as necessidades concretas da investigação.

4 - Em tudo o que não for contrariado pelo presente artigo, à interceptação e registo de transmissões de dados informáticos é aplicável o regime da interceptação e gravação de conversações ou comunicações telefónicas constantes dos artigos 187.º, 188.º e 190.º do Código de Processo Penal”.

Dispõe o art.º 187.º, n.º 1, do Cód. de Processo Penal que “a interceptação e a gravação de conversações ou comunicações telefónicas só podem ser ordenadas ou autorizadas, por despacho do juiz... 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... quanto a crimes [...] puníveis com pena de prisão superior, no seu máximo, a 3 anos”.

Ademais, em conformidade com o n.º 4, do mesmo art.º, “a interceptação e a gravação previstas nos números anteriores só podem ser autorizadas, independentemente da titularidade do meio de comunicação utilizado, contra:

a) Suspeito ou arguido;

b) 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) Vítima de crime, mediante o respectivo consentimento, efectivo ou presumido”.

Neste conspecto, o art.º 9.º da Lei 32/2008, de 17/07 (diploma que transpõe para a ordem jurídica interna a Directiva 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 electrónicas publicamente disponíveis ou de redes públicas de comunicações), nos seus n.ºs 1 a 4, preceitua: “1 - A transmissão dos dados referentes às categorias previstas no artigo 4.º [\[1\]](#) só pode ser autorizada, por despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, detecção e repressão de crimes graves.

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

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

a) Ao suspeito ou arguido;

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

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

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

Sucedee, todavia, que o Ac. do TC 268/2022, de 19/04, decidiu: “a) Declarar a inconstitucionalidade, com força obrigatória geral, 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 números 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;

b) Declarar a inconstitucionalidade, com força obrigatória geral, 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”.

Quanto aos efeitos da declaração de inconstitucionalidade prescreve o art.º 282.º da Constituição da República Portuguesa: “1. A declaração de inconstitucionalidade ou de ilegalidade com força obrigatória geral produz efeitos desde a entrada em vigor da norma declarada inconstitucional ou ilegal e determina a reprimenda das normas que ela, eventualmente, haja revogado.

2. Tratando-se, porém, de inconstitucionalidade ou de ilegalidade por infracção de norma constitucional ou legal posterior, a declaração só produz efeitos desde a entrada em vigor desta última.

3. Ficam ressalvados os casos julgados, salvo decisão em contrário do Tribunal Constitucional quando a norma respeitar a matéria penal, disciplinar ou de ilícito de mera ordenação social e for de conteúdo menos favorável ao arguido.

4. Quando a segurança jurídica, razões de equidade ou interesse público de excepcional relevo, que deverá ser fundamentado, o exigirem, poderá o Tribunal Constitucional fixar os efeitos da inconstitucionalidade ou da ilegalidade com alcance mais restritivo do que o previsto nos n.ºs 1 e 2”.

Assim, eliminados da ordem jurídica, por feridos de inconstitucionalidade, os art.ºs 4.º e 9.º da Lei 32/2008, de 17/07, foi repriminado, integralmente, o regime que resultava do art.º 189.º do Cód. de Processo Penal, com referência aos precedentes art.ºs 187.º e 188.º, sem embargo das normas da Lei do Cibercrime, cujas não foram afectadas pela declaração de inconstitucionalidade.

Neste conspecto, dispõe o art.º 189.º do Cód. de Processo Penal: “1 - O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à interceptação das comunicações entre presentes.

2 - 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 n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo”.

Contudo, as normas dos art.ºs 4.º e 9.º da Lei 32/2008, de 17/07, vieram a ser alteradas pela Lei 18/2024, de 05/02, passando a ter a seguinte redacção:

“Artigo 4.º

Categorias de dados a conservar

1 - Os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar, nos termos previstos na presente lei, em Portugal ou no território de outro Estado-Membro da União Europeia, as seguintes categorias de dados:

a) Dados necessários para encontrar e identificar a fonte de uma comunicação;

b) Dados necessários para encontrar e identificar o destino de uma comunicação;

c) Dados necessários para identificar a data, a hora e a duração de uma comunicação;

d) Dados necessários para identificar o tipo de comunicação;

e) Dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento;

f) Dados necessários para identificar a localização do equipamento de comunicação móvel.

2 - Para os efeitos do disposto na alínea a) do número anterior, os dados necessários para encontrar e identificar a fonte de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel:

i) O número de telefone de origem;

ii) O nome e endereço do assinante ou do utilizador registado;

b) No que diz respeito ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet:

i) Os códigos de identificação atribuídos ao utilizador;

ii) O código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública;

iii) O nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador ou o número de telefone estavam atribuídos no momento da comunicação.

3 - Para os efeitos do disposto na alínea b) do n.º 1, os dados necessários para encontrar e identificar o destino de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel:

i) Os números marcados e, em casos que envolvam serviços suplementares, como o reencaminhamento ou a transferência de chamadas, o número ou números para onde a chamada foi reencaminhada;

ii) O nome e o endereço do assinante, ou do utilizador registado;

b) No que diz respeito ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet:

i) O código de identificação do utilizador ou o número de telefone do destinatário pretendido, ou de uma comunicação telefónica através da Internet;

ii) Os nomes e os endereços dos subscritores, ou dos utilizadores registados, e o código de identificação de utilizador do destinatário pretendido da comunicação.

4 - Para os efeitos do disposto na alínea c) do n.º 1, os dados necessários para identificar a data, a hora e a duração de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, a data e a hora do início e do fim da comunicação;

b) No que diz respeito ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet:

i) A data e a hora do início (log in) e do fim (log off) da ligação ao serviço de acesso à Internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à Internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado;

ii) A data e a hora do início e do fim da ligação ao serviço de correio eletrónico através da Internet ou de comunicações através da Internet, com base em determinado fuso horário.

5 - Para os efeitos do disposto na alínea d) do n.º 1, os dados necessários para identificar o tipo de comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, o serviço telefónico utilizado;

b) No que diz respeito ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet, o serviço de Internet utilizado.

6 - Para os efeitos do disposto na alínea e) do n.º 1, os dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento, são os seguintes:

a) No que diz respeito às comunicações telefónicas na rede fixa, os números de telefone de origem e de destino;

b) No que diz respeito às comunicações telefónicas na rede móvel:

i) Os números de telefone de origem e de destino;

ii) A Identidade Internacional de Assinante Móvel (International Mobile Subscriber Identity, ou IMSI) de quem telefona;

iii) A Identidade Internacional do Equipamento Móvel (International Mobile Equipment Identity, ou IMEI) de quem telefona;

iv) A IMSI do destinatário do telefonema;

v) A IMEI do destinatário do telefonema;

vi) No caso dos serviços pré-pagos de carácter anónimo, a data e a hora da ativação inicial do serviço e o identificador da célula a partir da qual o serviço foi ativado;

c) No que diz respeito ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet:

i) O número de telefone que solicita o acesso por linha telefónica;

ii) A linha de assinante digital (digital subscriber line, ou DSL), ou qualquer outro identificador terminal do autor da comunicação.

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

a) O identificador da célula no início da comunicação;

b) Os dados que identifiquem a situação geográfica das células, tomando como referência os respetivos identificadores de célula durante o período em que se procede à conservação de dados”;

Art.º 9.º: “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.

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.

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

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

7 - Sem prejuízo do disposto no número seguinte, o despacho que autoriza a transmissão dos dados referentes às categorias previstas no n.º 1 do artigo 4.º é notificado ao titular dos dados no prazo máximo de 10 dias a contar da sua prolação.

8 - Se, em inquérito, o Ministério Público considerar que a notificação referida no número anterior comporta risco de pôr em causa a investigação, dificultar a descoberta da verdade ou criar perigo para a vida, para a integridade física ou psíquica ou para a liberdade dos participantes processuais, das vítimas do crime ou de outras pessoas devidamente identificadas, pode solicitar ao juiz de instrução criminal que proteja a notificação, a qual é realizada logo que a razão do protelamento deixar de existir ou, o mais tardar, no prazo máximo de 10 dias a contar da data em que for proferido despacho de encerramento desta fase processual.

9 - A transmissão dos dados referentes às categorias previstas no n.º 1 do artigo 4.º a autoridades de outros Estados só pode ocorrer no âmbito da cooperação judiciária internacional em matéria penal, de acordo com as regras fixadas na respetiva lei e desde que esses Estados garantam o mesmo nível de proteção de dados pessoais vigente no território da União Europeia”.

Crimes graves são, nos termos da al. g) do n.º 1 do art.º 2.º da Lei 32/2008, de 17/07, “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”, sendo “‘Terrorismo’ as condutas que integram os crimes de infrações terroristas, infrações relacionadas com um grupo terrorista, infrações relacionadas com atividades terroristas e financiamento do terrorismo” e “‘Criminalidade violenta’ as condutas que dolosamente se dirigirem contra a vida, a integridade física, a liberdade pessoal, a liberdade e autodeterminação sexual ou a autoridade pública e forem puníveis com pena de prisão de máximo igual ou superior a 5 anos” (als. i) e j) do art.º 1.º do Cód. de Processo Penal).

Posto isto, para que se autorize uma *compressão dos direitos fundamentais à palavra e à reserva da intimidade da vida privada*, constitucionalmente garantidos nos art.ºs 26.º, n.º 1, e 34.º, n.ºs 1 e 4, da Constituição da República Portuguesa, é essencial *despacho do juiz de instrução*, a quem incumbe, na fase de inquérito, em suma, apreciar e decidir as questões atinentes a direitos fundamentais dos cidadãos (cfr. art.º 269.º, n.º 1, al. e), do Cód. de Processo Penal).

Ora, se é certo que os dados pretendidos obter respeitam a suspeito dos crimes sob investigação (cfr. art.ºs 187.º, n.º 4, al. a), 189.º, n.ºs 1 e 2, do Cód. de Processo Penal, e 9.º, n.º 3, al. a), da Lei 32/2008, de 17/07), não menos certo é que o crime indiciado está excluído do catálogo do art.º 9.º, n.º 1, da Lei 32/2008, de 17/07, não se tratando de crime grave, máxime, não obstante a moldura penal, não se integrando na criminalidade violenta ou na criminalidade altamente organizada, nem em qualquer dos outros crimes definidos como graves sob a al. g) do n.º 1 do art.º 2.º da Lei 32/2008, de 17/07.

Saliente-se que o regime do Cód. de Processo Penal, por extensão contemplada no art.º 189.º (e onde caberia o crime sob investigação), não respeita a comunicações passadas, mas a comunicações futuras.

Não será, portanto, possível, à luz do vigente regime, a obtenção das informações pretendidas obter pelo Ministério Público.

Pelo exposto, indefiro a obtenção das informações pretendidas.

Devolvam-se os autos aos serviços do Ministério Público.»

2. Inconformado com a decisão, interpôs recurso o Ministério Público.

Na sequência das respetivas alegações termina apresentando as seguintes conclusões (transcrição):

«I. Os presentes autos iniciaram-se com a denúncia apresentada por AA contra BB, dando conta, entre o período compreendido entre Maio a Julho de 2024 recebeu vários telefonemas desta última, a várias horas do dia, para o seu número de telefone fixo (...60), nas quais a insulta com as seguintes expressões: “... ó desgraçada ... vem-me trazer o que me roubaste ... vem-me trazer o ouro, as libras e os lençóis que me roubaste ...!”.

II. São, pois, investigados factos susceptíveis, em abstracto, de configurar, entre outros, a prática de um crime de perturbação da vida privada, previsto e punível pelo artigo 190.º, nº2 do Código Penal, crime esse cometido por meio telefónico.

III. Torna-se imperativo confirmar a identidade do(s) autor(es) de tais telefonemas, e elencá-los, designadamente os realizados no período entre Maio e Julho de 2024, (sem prejuízo do prazo máximo de 6 meses para conservação dos dados), para a ofendida, titular do telefone fixo com o nº ...60.

IV. “A Lei nº 32/2008, de 17.07, que transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, de 15 de Março, que alterou a Directiva n.º 2002/58/CE, de 12 de Junho, regula a conservação e a transmissão dos dados de tráfego e de localização de comunicações electrónicas relativos a pessoas singulares e a pessoas colectivas, 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.

V. 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.

VI. 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.

VII. 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 transpõe a Diretiva (UE) 2016/680.

VIII. 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.º 109/2009, de 15 de setembro (Lei do Cibercrime).

IX. Nesta conformidade, por se situarem em planos distintos, a Lei n.º 32/2008, de 17.07, não revogou, nem podia ter revogado os artigos 187º a 189 do CPP.

X. O legislador, na Lei n.º 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.

XI. 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.

XII. 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.

XIII. 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).

XIV. Mas, declarada a inconstitucionalidade com força obrigatória geral da Lei nº 32/2008, com o sentido que ficou assinalado, e tendo anteriormente sido declarada invalidez a Diretiva 2006/24/CE (Acórdão de 08.04.2014, Digital RightsIreland) subsiste a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12.06, transposta pela Lei nº 41/2004, de 18.08.

XV. 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.

XVI. 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.- cfr. Acórdão do Tribunal da Relação de Guimarães, de 02.05.2023, tirado no processo n.º 12/23.6 PBGMR-A.G, disponível em www.dgsi.pt.

XVII. As diligências promovidas são indispensáveis para a descoberta da verdade material dos factos e de quem são os seus autores e, a impossibilidade de obtenção dos dados cujo acesso ora se promove, impede a investigação, detecção e repressão de crimes e um aumento do sentimento de impunidade dos autores e de insegurança da comunidade.

XVIII. O despacho recorrido violou o disposto nos artigos 187.º e 189.º, n.º 2 e 167.º ambos do Código de Processo Penal, artigo 6.º da Lei nº 41/2004 de 18.08 (concretamente o artigo 6.º, nº7) e 14.º, nº3 da Lei nº 109/2009, de 15.09.

Termos em que se requer que o presente recurso seja julgado procedente e que, em consequência de tal decisão, seja o despacho a quo revogado na sua plenitude e, em sua substituição, seja proferido novo despacho que dê

cumprimento integral às normas legais invocadas e, consequentemente, substituído por outro que defira o requerido pelo Ministério Público, nos termos do disposto nas disposições conjugadas dos artigos 187º, nº 1 al. e), 189º, n.º2, 269º, nº 1 al. e) e 167º, do CPP, artigos 11º, nº 1 al. c) e 14º, nº4 da Lei 109/2009, de 15.09, artigo 6º, nºs 2 e 7 da Lei nº 41/2004, de 18.08 e artigo 10º da Lei nº 23/96, de 26.07.»

3. Neste Tribunal da Relação, a **Exma. Procuradora-geral Adjunta**, emitiu parecer, no sentido de que o recurso deve proceder, acompanhando a motivação e conclusões constantes do recurso e acrescentando à jurisprudência ali citada a referência ao acórdão do Tribunal da Relação de Coimbra de 27-09-2023, processo nº13/20.6PEVIS.C1

4. Não foi apresentada resposta a esse parecer e, efetuado exame preliminar e colhidos os vistos, o processo foi presente à conferência, por o recurso dever ser aí julgado, de harmonia com o preceituado no artigo 419º, n.º 3, alínea b) do Código de Processo Penal.

II. FUNDAMENTAÇÃO

1. DELIMITAÇÃO DO OBJETO DO RECURSO

Segundo jurisprudência pacífica, sem prejuízo das questões de conhecimento oficioso - como seja a deteção de vícios decisórios ao nível da matéria de facto resultantes da simples leitura do texto da decisão recorrida, por si só ou conjugada com as regras da experiência comum, referidos no artigo 410º, n.º 2, do Código de Processo Penal^[2], e a verificação de nulidades que não devam considerar-se sanadas, nos termos dos artigos 379º, n.º 2, e 410º, n.º 3, do mesmo código - é pelas conclusões que o recorrente extrai da motivação, onde sintetiza os fundamentos de discordância com o decidido e resume as razões do pedido (artigo 412º, n.º 1, do referido diploma), que se delimita o objeto do recurso e se fixam os limites do conhecimento do mesmo pelo tribunal superior.

Atentas as conclusões formuladas pelo Recorrente, a questão a decidir é a de saber se o despacho recorrido, que indeferiu um pedido do Ministério Público de obtenção do registo detalhado de comunicações telefónicas estando em causa a investigação de crime de perturbação da vida privada, violou o

disposto nos artigos 187.º e 189.º, n.º 2 e 167.º ambos do Código de Processo Penal, artigo 6.º da Lei nº 41/2004 de 18.08 (concretamente o artigo 6.º, nº7) e 14.º, nº3 da Lei nº 109/2009, de 15.09.

2. DA DECISÃO RECORRIDA.

Importa ter em conta os seguintes dados do processo:

- Com data de 09-07-2024 foi lavrado auto de notícia dando conta da denúncia por parte de AA de factos suscetíveis de integrar a prática, nomeadamente, de crimes de ofensa à integridade física, injúrias e ameaças.

- Datado de 29-07-2004 encontra-se nos autos auto de inquirição da denunciante onde consta que a mesma disse, além do mais, que nos últimos 2 a 3 meses, cerca de 2 ou 3 vezes por semana, a denunciada lhe telefona para o seu telefone fixo com o nº...60, injuriando-a e perturbando-a de dia e de noite.

- Datado de 10-12-2024 e com a referência 95844790, deu entrada requerimento formulado pelo Ministério Público com o seguinte teor (transcrição):

«Nos presentes investiga-se a prática de factos que são suscetíveis de configurar, em abstrato, a prática de um crime de perturbação da vida privada, p. e p. pelo artigo 190.º, n.º 2 do C.P.

Em síntese, do auto de inquirição de AA de fls. 14, dá-se conta de que “nos últimos 2 a 3 meses, por 2 a 3 vezes por semana”, a denunciada BB efectua chamadas telefónicas para o número de telefone fixo da ofendida (...60), durante o dia, noite e mesmo de madrugada, encontrando-se a ofendida a dormir, e insulta-a com as seguintes expressões: “... ó desgraçada ... vem-me trazer o que me roubaste ... vem-me trazer o ouro, as libras e os lençóis que me roubaste ...!”.

Por requerimento de 05.12.2024, a ofendida informou que o seu número de telefone fixo é telemóvel é ...60, onde recebeu as referidas chamadas, e que se encontra associado à operadora “MEO/ALTICE”.

Neste sentido, revela-se fundamental o acesso aos registos detalhados de comunicações, nomeadamente chamadas recebidas pelo número ...60, pertencente à denunciante, no período compreendido entre 01.05.2024 a 31.07.2024, por forma a identificar o número de origem das chamadas recebidas para

Ora, nos termos do artigo 269.º, n.º 1, alínea c) do C.P.P., durante o inquérito, compete exclusivamente ao juiz de instrução ordenar ou autorizar a interceção gravação ou registo de conversações ou comunicações, nos termos dos artigos 187.º e 190.º do C.P.P.

O artigo 187.º do C.P.P. estabelece as condições de admissibilidade da interceção e da gravação de conversações ou comunicações telefónicas e o artigo 190.º, do mesmo Código, prevê a extensão do regime a comunicações efetuadas por meio técnico diferente do telefone.

Ora, a garantia do sigilo das comunicações abrange não apenas o conteúdo das comunicações, mas o próprio "tráfego" como tal (espécie, hora, duração, intensidade de utilização). Nesses casos, as restrições a tal confidencialidade estão autorizadas apenas em processo criminal e estão igualmente sob reserva de lei, só podendo ser decididas por um juiz.

Salvo melhor entendimento, cremos que o direito à reserva da vida privada dos visados deve ceder perante os interesses manifestos e inequívocos da investigação nestes autos, uma vez que a informação decorrente da faturação detalhada vai permitir aferir da eventual prática pela denunciada de um crime de perturbação da vida privada. Entendemos, assim, que se encontra perfeitamente justificado o acesso a tais informações, porquanto revelam-se essenciais para o apuramento da verdade dos factos denunciados nos presentes autos.

Face a todo o exposto, ao abrigo do disposto nos artigos 187.º, n.º 1, alínea e), e n.º 4, alínea a), 188.º, 189.º, n.º 2, e 269.º, n.º1, alínea e), todos do Código de Processo Penal, apresente os autos ao(à) Mmo(a) Juiz de Instrução, a quem se promove se oficie a operadora "MEO", solicitando o envio:

- dos registos detalhados de comunicações (chamadas) recebidas pelo número ...60, pertencente à denunciante, no período compreendido entre 01.05.2024 e 31.07.2024.»

- Sobre este requerimento recaiu o despacho recorrido a acima transcrito.

3. APRECIÇÃO DO RECURSO.

Cabe, antes de mais delimitar o campo em que se insere o requerimento de que foi objeto o despacho recorrido.

Com efeito, trata-se de requerimento para obtenção dos registos das chamadas recebidas por um número de telefone fixo, pertencente à denunciante de crime de perturbação da vida privada, num determinado período.

Por outro lado, o requerimento foi feito ao abrigo do disposto nos artigos 187.º, n.º 1, alínea e), e n.º 4, alínea a), 188.º, 189.º, n.º 2, e 269.º, n.º1, alínea e), todos do Código de Processo Penal.

Cumpre, pois, ter presente o teor de tal regime legal.

Artigo 187º nº1 alínea e) e nº4 alínea a):

1 - A intercepção e a gravação de conversações ou comunicações telefónicas só podem ser autorizadas durante o inquérito, 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, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público, quanto a crimes:

e) De injúria, de ameaça, de coacção, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone;

4 - A intercepção e a gravação previstas nos números anteriores só podem ser autorizadas, independentemente da titularidade do meio de comunicação utilizado, contra:

a) Suspeito ou arguido;

Artigo 189º nº2:

2 - 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 n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo.

Não se situa a questão a decidir, portanto, no campo da intercepção de comunicações pretéritas, presentes ou futuras, mas apenas no da obtenção do registo de chamadas recebidas por um determinado número de telefone num determinado período.

Estamos no domínio daquilo que se denomina de dados de tráfego (metadados).

O despacho recorrido funda-se num concreto entendimento sobre a decisão do Tribunal Constitucional constante do Acórdão nº 268/2022, de 19/04/2022, publicado no DR, 1ª Série, de 03/06/2022, pags. 18 e ss.

Neste acórdão nº 268/2022, o Tribunal Constitucional decidiu:

“a) Declarar a inconstitucionalidade, com força obrigatória geral, 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 18.º, todos da Constituição;

b) Declarar a inconstitucionalidade, com força obrigatória geral, 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.”

A lei nº 32/2008, de 17.07^[3], 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, sendo certo que os metadados ali em causa são apenas e só os dados de base/tráfego, que não pressupõem qualquer análise de comunicações.

O Tribunal de Justiça da União Europeia (TJUE), através do Acórdão de 8 de abril de 2014, declarou a invalidade da referida Diretiva. A decisão do TJUE fundamentou-se na violação do princípio da proporcionalidade pela restrição que a Diretiva operaria dos direitos ao respeito pela vida privada e familiar e à proteção de dados pessoais, consagrados nos artigos 7.º e 8.º da Carta; e embora decidindo que as normas inerentes à imposição do dever de conservação de dados de tráfego e de localização gerados no contexto de comunicações eletrónicas e do dever da sua transmissão às autoridades competentes para efeitos de investigação, deteção e repressão de crimes graves - eram, em si mesmas, medidas legítimas e adequadas ao fim visado - acabou por concluir que as mesmas violavam o princípio da proporcionalidade, na sua dimensão da necessidade.

A Lei nº 32/2008, de 17.07, 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 (art. 1º, nº 1).

Volvendo ao polémico acórdão do Tribunal Constitucional, foi a recolha, 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 ano, que pela abrangência subjetiva (que pode atingir qualquer cidadão e não só os suspeitos de crimes) e temporal (um ano) o Tribunal Constitucional entendeu 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.

Nesta medida, por força da decisão do Tribunal Constitucional deixaram de existir na ordem jurídica as normas constantes dos artigos 4º, 6º e 9º (este na dimensão apontada no acórdão) da Lei 32/2008 de 17 de julho, que determinava para os fornecedores de serviços de comunicações eletrónicas, publicamente disponíveis, a obrigação de conservação para fins criminais, por um ano, dos dados gerados ou tratados no âmbito dos serviços de comunicações eletrónicas. Nada mais do que isso.

Como referido no mesmo acórdão nº 268/2022 os dados referidos no artigo 4.º não abrangem o conteúdo das comunicações, dizendo respeito somente às suas circunstâncias – razão pela qual são usualmente designados por metadados (ou dados sobre dados) – cf. Acórdãos n.ºs 403/2015 e 420/2017 – sendo que, o juízo de inconstitucionalidade se coloca, assim, apenas e só em relação aos dados de base e de tráfego.

Para além disso, o aludido juízo de inconstitucionalidade apenas se reporta a dados do passado, armazenados – já não assim quando obtidos em tempo real – na medida em que – tendo presente os fundamentos do ac. do TC supra referido – só nessa hipótese se colocam as questões de (des)proporcionalidade na restrição dos direitos constitucionalmente protegidos da reserva da intimidade da vida privada e do direito ao conhecimento do armazenamento de dados pessoais e do fim a que se destinam (ainda que tenham sido acedidos legitimamente por terceiros).

Como se decidiu no acórdão deste Tribunal da Relação de Coimbra de 27.09.2023^[4]:

“O Tribunal Constitucional não entendeu estarem feridas de inconstitucionalidade as normas do CPP 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 nº 1 do artigo 187º (onde se incluem crimes puníveis com pena de prisão superior, no seu máximo, a 3 anos)^[5], nem o TC afastou a possibilidade de conservação de dados ao abrigo de outros diplomas, por exemplo para fins contratuais, de que é exemplo a Lei 41/2004 de 18.08, que prevê a conservação de dados de tráfego, por um período de 6 meses.

Ora, se o CPP prevê a possibilidade de obtenção de dados relativos a conversações e comunicações telefónicas, se eles existirem validamente conservados no âmbito de outros diplomas em vigor, (v.g. artigo 14 da Lei 109/2009), nada impede que as autoridades a eles acedam ainda que observando as condições técnicas e de segurança exigidas pelo SAPDOC (Sistema de acesso ou pedido de dados às operadoras de comunicação), e Portaria 469/2009 de 06.05, alterada pelas portarias 915/2009 de 08.08 e 694/2010 de 16.08, quando estão em causa valores como a segurança, a legalidade democrática e o exercício da ação penal no combate à criminalidade. De igual modo, se há dados que podem ser guardados, por exemplo, para fins contratuais, por exemplo, de faturação, nada impede que possam ser utilizados para fins de investigação criminal, tanto mais quanto a Lei 41/2004 o admite (art. 6 n.º 7) e no âmbito do processo criminal ao arguido são obrigatoriamente transmitidos (artigo 141º, nº 4 e) do CPP) os elementos do processo que indiciam os factos imputados, sempre que a sua comunicação não ponha em causa a investigação, não dificulte a descoberta da verdade nem crie perigo para a vida, a integridade física ou psíquica ou a liberdade dos participantes processuais ou das vítimas de crime.”

Também nós cremos que o Tribunal Constitucional não vedou o acesso, no âmbito do processo penal, a dados conservados na posse de operadoras de serviços de comunicações, que está previsto nos artigos 187º a 189º, na alínea e) do artigo 269º do Código de Processo Penal e na Lei do Cibercrime.

Noutra perspetiva, as operadoras de comunicações não ficaram impedidas de conservar dados de tráfego dos seus clientes, v.g. para fins de faturação, como ocorre com a Lei 41/2004 de 18.08 - que transpõe a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho e que, contrariamente à Diretiva 2006/24/CE (transposta pela Lei 32/2008 de 17.07) se mantém válida - pelo prazo de 6 meses.^[6]

Pertinente nos surge atentar, também, na observação de Rui Cardoso^[7], que partilhamos, no sentido de que, com a declaração de inconstitucionalidade com força obrigatória geral da norma do artigo 9.º da Lei 32/2008, a norma do n.º 2 do artigo 189.º do Código de Processo Penal foi repristinada na sua plenitude, ao abrigo do disposto no n.º 1 do artigo 282.º da Constituição da República Portuguesa.

Gomes Canotilho e Vital Moreira, citados no artigo mencionado supra, afirmam, a propósito do artigo 282º da Constituição da República Portuguesa que: *“A declaração de inconstitucionalidade (ou de ilegalidade) tem efeito repristinatório (nº 1, in fine), determinando a reentrada em vigor de normas eventualmente revogadas pela norma declarada inconstitucional (ou ilegal). Trata-se de um efeito direto da inconstitucionalidade (ou da ilegalidade), pois, sendo a norma inválida desde a origem, é inválida desde logo a revogação de normas anteriores que ela tenha efetuado.”*

Alinhamos, pois, no entendimento de que, após a prolação do acórdão do Tribunal Constitucional nº268/2022, o artigo 189.º, n.º 2, do Código de Processo Penal constitui fundamento normativo para obtenção de dados de tráfego/localização e que a Lei nº 41/2004 (artigos 6º e 7º) constitui o fundamento legal para a sua conservação.

Poderá objetar-se que a Lei nº 41/2004 de 18.08 não prevê a notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal.

Com efeito, é dado adquirido que esta lei respeita à conservação de dados e nela não se contempla ou regula o acesso aos mesmos.

Porém, não é menos certo que o Tribunal Constitucional se debruçou sobre a falta de notificação apenas quanto ao artigo 9º da Lei 32/2009, de 17.07, que constituía uma norma de acesso a dados, pelo que a questão, salvo melhor entendimento, não se colocará relativamente à Lei nº 41/2004.

Nesta medida, estando os dados conservados pelo período de seis meses após o fim de cada comunicação, podem ser obtidos para efeitos de prova em processo penal, ao abrigo do disposto no artigo 189.º, n.º 2, do Código de Processo Penal, ficando assim cumprida a exigência de previsão legal para a restrição de direitos fundamentais, imposta pelo artigo 18.º, n.º 2, da Constituição da República Portuguesa.

Ao contrário do que vem sustentado no despacho recorrido, cremos ter explicitado supra que o nº2 do artigo 189º do Código de Processo Penal, não se limita à obtenção de “dados dinâmicos”, ou seja, que estejam a ser transmitidos em tempo real, por oposição a dados “preservados ou armazenados”^[8].

De igual modo, no acórdão do Tribunal da Relação do Porto de 29.03.2023^[9], se decidiu que: *“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.”*

Conforme refere Rui Cardoso^[10]: *“Os metadados são prova documental/digital. No caso dos conservados ao abrigo da Lei 41/2004 são documentos que existem independentemente do processo penal – não há qualquer especial meio que seja necessário prever para a sua obtenção. Poderiam ser obtidos por busca, por pesquisa e apreensão de dados informáticos, por injunção (ordem), cabendo à lei determinar que meios podem ser utilizados, o que, quanto à injunção, está feito no art. 189.º n.º 2 do CPP”.*

Mesmo que a Lei 41/2004 não previsse – o que não sucede – a possibilidade de utilização probatória desses dados em processo penal, os mesmos poderiam ser obtidos e utilizados, desde que não existisse qualquer crime na sua conservação.

A norma fundamento para tal está no Código do Processo Penal.

Por seu lado, a Lei nº 58/2019 (Lei de proteção de dados pessoais) no seu artigo 23º, nº 2, não impede a transmissão de dados pessoais entre entidades públicas para finalidades diversas das determinadas na recolha. E ainda que assim não fosse, o certo é que não tem de haver previsão expressa para que todos os meios de prova possam ser utilizados no processo penal, atento o princípio da legalidade e liberdade da prova consagrado no artigo 125.º do Código de Processo Penal, que estabelece serem admissíveis as provas que não forem proibidas por lei.

Quanto aos dados de tráfego/localização, a ponderação à luz dos princípios da necessidade e da proporcionalidade está feita pelo legislador no artigo 189.º, n.º 2 do Código de Processo Penal, e igualmente se impõe ao aplicador por

força direta do artigo 18.º, n.º 2, da CRP, devendo notar-se o Tribunal Constitucional não apreciou a questão da admissibilidade de utilização no processo penal dos dados conservados para efeitos de faturação.

Concluindo dir-se-á que não há, pois, qualquer omissão legislativa que, em consequência, seja óbice constitucional à conservação dos dados feita ao abrigo da Lei 41/2004, não podendo esse argumento ser utilizado para recusar o acesso a esses dados para prova em processo penal com fundamento no artigo 189.º, n.º 2, do Código de Processo Penal, como o faz o despacho recorrido.

De tudo quanto se expôs, resulta a admissibilidade legal de utilização probatória dos dados de tráfego/localização conservados, ao abrigo da Lei 41/2004, de 18.08, com o limite quanto ao prazo de conservação, que é de seis meses, cf. artigo 6º, nºs 2 e 7 e artigo 10º da Lei nº 23/96, de 26.07,

A declaração de inconstitucionalidade com força obrigatória geral do artigo 4º, conjugado com os artigos 6º e 9º a Lei nº32/2008, 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 41/2008, de 18/8, com fundamento no artigo 189º, nº2, do Código de Processo Penal (ou seja, quanto a crimes previstos no número 1 do artigo 187º e em relação às pessoas referidas no nº4 do mesmo artigo), preceito legal esse que não se reporta à interceção e gravação desses dados em tempo real, pois que estas já se encontram previstas nos artigos 187º e 188º do CPP e versam sobre dados de conteúdo, de tráfego e de localização.

O citado nº2 do artigo 189º do CPP inclui assim na sua previsão apenas o acesso a dados conservados ou armazenados (dados de tráfego e de localização).

Neste sentido, ou pelo menos, referindo-se à questão em causa adotando esta perspetiva, vejam-se as seguintes recentes decisões, todas disponíveis em www.dgsi.pt:

- Do Supremo Tribunal de Justiça, os acórdãos de 31-01-2024 (processo nº170/11.2TAOLH-E.S1, relator Lopes da Mota); de 03-11-2022 (processo nº19/20.5JBLSB.L1.S1, relator, António Gama) e de 13-09-2023 (processo nº83/15.9PJLRS-O.S1, relator Maria do carmo Silva Dias).

- Do Tribunal da Relação de Coimbra, os acórdãos de 01-06-2022 (processo nº152/21.6GGCBBR-A.C1, relator, Alcina Ribeiro; de 24-04-2024 (processo nº515/21.7T9GRD.C1, relator, Maria Alexandra Guiné;

- Do Tribunal da Relação de Guimarães, o acórdão de 03-10-2023 (processo nº241/20.4JAVRL.G1, relator, António Teixeira) e de 17-10-2023 (processo nº308/19.1JAVRL.G1, relator, Paulo Almeida Cunha);

- Do Tribunal da Relação de Évora de 28-06-2023 (processo nº2010/21.5JFLSB-A.E1, relator, Laura Goulart Maurício);

- Do Tribunal da Relação de Lisboa os acórdãos de 04-06-2024 (processo nº41/24.2JBLSB-A.L1.5, relator Maria José Machado) e de 26-04-2023, (da mesma relatora, processo nº685/21.4JGLSB.L1-5)

Não se ignoram, nem se desmerecem, naturalmente, as posições contrárias, indicando-se, a título de exemplo a seguinte Jurisprudência, disponível para consulta em www.dgsi.pt:

- Do Tribunal da Relação de Évora os acórdãos de 05-03-2024 (processo nº355/22.6JGLSB.E1, relator Fátima Bernardes); de 12-09-2023 (processo nº950/10.6PCSTB.E2, relator, Nuno Garcia); de 28-02-2023 (processo nº661/17.1TELSB.E1); de 25-10-2022 (processo nº52/18.7GBSLV.E1, relator Gomes de Sousa) e de 09-05-2023 (processo nº275/22.4GCSTB-A.E1, relator, Beatriz Marques Borges);

- Do Tribunal da Relação de Lisboa de 25-10-2022 (processo nº50/22.6JBLSB-A.L1-5, relator, Mafalda Sequinho dos Santos);

- Do Tribunal da Relação de Guimarães, os acórdãos de 23-01-2024 (processo nº743/23.0JAVRL-A.G1, relator, Isabel Cristina Gaio Ferreira de castro) e de 19-03-2024 (processo nº204/23.8GBCHV-A.G1, relator, Fátima Furtado);

- Do Tribunal da Relação do Porto o acórdão de 07-12-2022 (processo nº5011/22.2JAPRT-A.P1, relator, Pedro Vaz Pato).

Com efeito, o teor do acórdão do Tribunal Constitucional propicia a disparidade das leituras em causa pela sua aparente abrangência. Por outro lado, a sobreposição de regimes legais relativamente a estas matérias também não ajuda à clareza das questões que se colocam, nem se nos afigura que a Lei n.º 18/2024, de 05 de fevereiro venha a lograr tal desiderato quando passe a produzir efeitos.

Trata-se de matérias surgidas com as recentes e rapidíssimas inovações a que assistimos no âmbito das possibilidades oferecidas pelas novas comunicações, que conhecem uma rapidez evolutiva que, naturalmente, a Lei não consegue acompanhar.

Todo este panorama de novas formas de comunicação coloca um grande número de possibilidades à prática de ilícitos, com a consequente dificuldade para a sua investigação, não podendo, porém, no afã de perseguir todo um novo modo de delinquir, associado ao cibercrime, atropelar-se os direitos fundamentais dos cidadãos avultando aqui os da privacidade, intimidade, autodeterminação.

Tudo se reconduz, no nosso modesto entender, e refletindo, pensamos, o entendimento do Tribunal Constitucional, à necessidade de observar, na compatibilização entre a salvaguarda dos direitos das vítimas de crimes graves e os mecanismos de perseguição e punição desses mesmos crimes, os princípios da proporcionalidade e da necessidade das medidas de intromissão nas comunicações.

A leitura que fazemos, assente na Jurisprudência e Doutrina citadas, em nosso modesto entender, compatibiliza aqueles interesses em conflito e, parece-nos, interpreta de forma adequada o sentido da declaração de inconstitucionalidade em causa.

Ora, no caso dos autos, estão em causa dados de tráfego - registo de chamadas recebidas num determinado número de telefone fixo, pertencente à vítima - delimitados no tempo, essenciais à investigação de crime previsto no artigo 187º nº1 alínea e) do Código de Processo Penal, a ordenar por despacho do Juiz de Instrução.

Assim sendo, nada obsta ao deferimento do requerido, posto que respeitadas as regras de conservação dos mesmos dados nos termos do regime legal descrito supra.

Por tudo quanto vem exposto, julga-se procedente o recurso interposto pelo Ministério Público, revogando-se o despacho recorrido, o qual deverá ser substituído por outro que, com atualidade, em face do mencionado prazo de 6 meses, defira ao requerido, caso nisso ainda mantenha interesse o Ministério Público.

III. DISPOSITIVO

Nos termos e pelos fundamentos expostos, acordam os Juízes da 4ª Secção do Tribunal da Relação de Coimbra em julgar procedente o recurso interposto pelo **Ministério Público** e, consequentemente, revogar o despacho recorrido que deve ser substituído por outro nos termos determinados supra.

Sem tributação.

(Texto elaborado pela relatora e revisto pelos seus signatários - artigo 94º, n.º 2, do CPP)

Coimbra, 28-05-2025

Os Juízes Desembargadores

Fátima Sanches (relatora)

Capitolina Fernandes Rosa (2ª Adjunta)

(data certificada pelo sistema informático e assinaturas eletrónicas qualificadas certificadas)

Voto de vencido

Vencida na medida em que sufrago entendimento diverso, conforme supra assinalado nos termos do acórdão de 23-01-2024 (processo nº743/23.0JAVRL-A.G1), acessível em www.dgsi.pt de que fui relatora.

Isabel Gaio Ferreira de Castro (1ª Adjunta)

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

- a) Dados necessários para encontrar e identificar a fonte de uma comunicação;
- b) Dados necessários para encontrar e identificar o destino de uma comunicação;

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

2 - Para os efeitos do disposto na alínea a) do número anterior, os dados necessários para encontrar e identificar a fonte de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel:

- i) O número de telefone de origem;
- ii) O nome e endereço do assinante ou do utilizador registado;

b) No que diz respeito ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:

- i) Os códigos de identificação atribuídos ao utilizador;
- ii) O código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública;
- iii) O nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador ou o número de telefone estavam atribuídos no momento da comunicação.

3 - Para os efeitos do disposto na alínea b) do n.º 1, os dados necessários para encontrar e identificar o destino de uma comunicação são os seguintes:

a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel:

- i) Os números marcados e, em casos que envolvam serviços suplementares, como o reencaminhamento ou a transferência de chamadas, o número ou números para onde a chamada foi reencaminhada;
- ii) O nome e o endereço do assinante, ou do utilizador registado;

b) No que diz respeito ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:

- i) O código de identificação do utilizador ou o número de telefone do destinatário pretendido, ou de uma comunicação telefónica através da Internet;
- ii) Os nomes e os endereços dos subscritores, ou dos utilizadores registados, e o código de identificação de utilizador do destinatário pretendido da comunicação.

4 - Para os efeitos do disposto na alínea c) do n.º 1, os dados necessários para identificar a data, a hora e a duração de uma comunicação são os seguintes:

- a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, a data e a hora do início e do fim da comunicação;

b) No que diz respeito ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:

- i) A data e a hora do início (log in) e do fim (log off) da ligação ao serviço de acesso à Internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à Internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado;
- ii) A data e a hora do início e do fim da ligação ao serviço de correio electrónico através da Internet ou de comunicações através da Internet, com base em determinado fuso horário.

5 - Para os efeitos do disposto na alínea d) do n.º 1, os dados necessários para identificar o tipo de comunicação são os seguintes:

- a) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, o serviço telefónico utilizado;
- b) No que diz respeito ao correio electrónico através da Internet e às comunicações telefónicas através da Internet, o serviço de Internet utilizado.

6 - Para os efeitos do disposto na alínea e) do n.º 1, os dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento, são os seguintes:

- a) No que diz respeito às comunicações telefónicas na rede fixa, os números de telefone de origem e de destino;
- b) No que diz respeito às comunicações telefónicas na rede móvel:
 - i) Os números de telefone de origem e de destino;
 - ii) A Identidade Internacional de Assinante Móvel (International Mobile Subscriber Identity, ou IMSI) de quem telefona;
 - iii) A Identidade Internacional do Equipamento Móvel (International Mobile Equipment Identity, ou IMEI) de quem telefona;
 - iv) A IMSI do destinatário do telefonema;
 - v) A IMEI do destinatário do telefonema;
 - vi) No caso dos serviços pré-pagos de carácter anónimo, a data e a hora da activação inicial do serviço e o identificador da célula a partir da qual o serviço foi activado;
- c) No que diz respeito ao acesso à Internet, ao correio electrónico através da Internet e às comunicações telefónicas através da Internet:
 - i) O número de telefone que solicita o acesso por linha telefónica;
 - ii) A linha de assinante digital (digital subscriber line, ou DSL), ou qualquer outro identificador terminal do autor da comunicação.

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

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

[2] Neste sentido, vd. o acórdão de uniformização de jurisprudência n.º 7/95, proferido pelo Plenário das Secções Criminais do STJ em 19 de outubro de 1995, publicado no Diário da República, I Série - A, n.º 298, de 28 de dezembro de 1995, que fixou jurisprudência no sentido de que “É oficioso, pelo tribunal de recurso, o conhecimento dos vícios indicados no artigo 410º, nº 2, do Código de Processo Penal, mesmo que o recurso se encontre limitado à matéria de direito”.

[3] Cabe notar que, já após a prolação deste acórdão do Tribunal Constitucional, foi publicada a Lei n.º18/2024, de 05 de Fevereiro a qual, nos termos do seu artigo 1º alínea a) procedeu “a) À segunda alteração à Lei n.º 32/2008, de 17 de julho, que transpõe para a ordem jurídica interna a Diretiva 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, conformando-a com os Acórdãos do Tribunal Constitucional n.ºs 268/2022 e 800/2023;”

Tal lei entrou em vigor, nos termos do seu artigo 5º, no dia seguinte ao da sua publicação, ou seja, em 06-02-2024.

Porém, nos termos do disposto no artigo 18º da Lei n.º 32/2008, de 17 de julho, assim alterada, a mesma só produz efeitos 90 dias após a publicação da portaria a que se refere o n.º 3 do artigo 7.º, portaria que ainda não foi publicada.

Nesta medida, a referência a esta Lei por parte do Tribunal *a quo*, parece-nos, não é pertinente, devendo a apreciação da questão ater-se à redação da Lei n.º 32/2008, de 17 de julho, antes desta sua alteração.

[4] Prolatado no âmbito do Processo nº13/20.6PEVIS.C1, relatora: Maria Teresa Coimbra, disponível para consulta em www.dgsi.pt

[5] Como também, “*crimes de injúria, de ameaça, de coação, de devassa da vida privada e perturbação da paz e do sossego, quando cometidos através de telefone*”, nos termos do disposto no artigo 187º nº1 alínea e) do Código de Processo Penal, acrescentamos nós, tendo em conta o objeto do presente recurso.

[6] Nesse sentido, o acórdão do Tribunal da Relação de Guimarães de 02.05.2023, prolatado no âmbito do processo nº12/23.6PBGMR-A.G1, relator: Armando Azevedo disponível para consulta em www.dgsi.pt.

[7] In em “A conservação e a utilização probatória de metadados de comunicações eletrónicas após o Acórdão do Tribunal Constitucional n.º 268/20022 – o que nasce torto...” - Revista do Ministério Público n.º 172, pág. 59 e ss.,

[8] Neste sentido, o acórdão do Tribunal da Relação de Lisboa de 22.02.2023, prolatado no âmbito do processo n.º 495/22.1JAFUN-A.L1-5, relatora: Alda Tomé Casimiro, disponível para consulta em www.dgsi.pt.

[9] Prolatado no âmbito do processo n.º 47/22.6PEPRT-Z.P1, relatora: Maria Joana Grácio, disponível para consulta em www.dgsi.pt,

[10] In artigo supracitado, pág. 64
