A competência da Formação do Supremo Tribunal de Justiça nos termos da Lei n.º 32/2008, de 17 de julho ("Lei dos Metadados") e as normas processuais de acesso a dados conservados de tráfego e de localização

Tiago Caiado Milheiro,
Juiz de Direito

Resumo: O texto começa por fazer alguns considerandos sobre a competência do juiz de instrução criminal e da formação das secções criminais do Supremo Tribunal de Justiça no âmbito da Lei n.º 32/2008, de 17 de julho. Seguidamente procura delimitar o âmbito da Lei n.º 32/2008, de 17 de julho, abordando o antes e depois do Acórdão do Tribunal Constitucional n.º 268/2022, as tentativas de o legislador sanar as inconstitucionalidades e o resultado final. Termina analisando o âmbito diverso de aplicação do artigo 189.º do Código de Processo Penal, a diferença entre normas processuais penais de acesso e de conservação, e a importância atual do n.º 2 daquele preceito.

Palavras-chave: metadados, dados de tráfego, dados de localização.

I – A competência do juiz de instrução criminal e da formação das secções criminais do Supremo Tribunal de Justiça no âmbito da Lei n.º 32/2008, de 17 de julho. Considerações iniciais.

§ 1 A Lei n.º 18/2024, de 5 de fevereiro alterou o artigo 6.º da Lei n.º 32/2008, de 17 de julho e, de forma *inovatória*, veio atribuir competência a uma formação das secções criminais do Supremo Tribunal de Justiça no âmbito da Lei n.º 32/2008, de 17 de julho. A forma pouco clara como foi construída a norma é propícia a equívocos. Pretende-se, assim,

clarificar, de uma forma muito sintética, quais são as competências do juiz de instrução criminal e da formação das secções criminais do Supremo Tribunal de Justiça no âmbito da Lei n.º 32/2008, de 17 de julho, *separando as águas*. Para isso, é muito importante compreender qual o *objeto* da Lei n.º 32/2008, de 17 de julho e os *antecedentes* que culminaram com a Lei n.º 18/2024, de 5 de fevereiro. Depois, como veremos, será bem mais fácil chegar a uma conclusão.

II – O âmbito da Lei n.º 32/2008, de 17 de julho. As diferentes bases de conservação de dados de tráfego e de localização. A diversidade das fontes que justificam essa conservação e das finalidades.

§ 2 A Lei n.º 32/2008, de 17 de julho é um diploma que *disciplina* os termos em que os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações (*v.g.* Nos ou a Meo, mas existem muitos outros fornecedores registados em Portugal, podendo consultar-se a lista daqueles que estão em atividade no site da ANACOM), estão *obrigados* a conservar dados gerados por essas comunicações, mais concretamente dados tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dados conexos necessários para identificar o assinante ou o utilizador registado, com a *finalidade* de investigar, detetar e reprimir crimes graves.

§ 3 É uma lei *direcionada* para as empresas que fornecem serviços de comunicações telefónicas e de internet, impondo-lhes um *dever* de *conservação* de dados de tráfego e de localização *no presente* com uma finalidade específica de serem utilizados numa investigação criminal no *futuro*. De uma forma simplista, conserva-se no presente porque eventualmente poderá revelar-se *útil* para uma investigação criminal. Ou seja, a *conservação* de dados pelos fornecedores dos serviços telefónicos ou de internet ao abrigo desta lei não é feita *porque já foram considerados* pertinentes para um processo criminal que está em curso. Esse pedido de *acesso* da investigação criminal é *futuro, eventual e hipotético*. Aliás, na verdade, muitos dos dados conservados não serão sequer utilizados

num processo criminal. Pela simples razão, como é bom de ver, que apenas uma pequena percentagem dos utilizadores *cujos dados são conservados* cometem crimes graves. E é justamente *esses* que a lei pretende "apanhar" nas suas *malhas*, permitindo que quando esteja a ser investigados, se *acedam* a dados gerados no passado úteis para determinar se cometeu o crime.

§ 4 Acesso a dados conservados no *passado* que apenas no *futuro* se descobre serem relevantes para uma investigação criminal que *não* é privativo desta Lei n.º 32/2008, de 17 de julho. Imagine-se um indivíduo que circulando no seu veículo usa uma *app* de identificação de trajeto, passa na via verde, pára num posto de combustível onde é filmado, e ali levanta dinheiro. Nesse local existe um homicídio com fuga. Naturalmente que os dados de localização, dados bancários, dados de imagem, dados de faturação, embora possam ter sido conservados *ab initio* para fins *diversos* da investigação criminal (prestação de serviços, cobrança de portagens, atividade bancária, segurança de um estabelecimento), poderão vir a ser usados no *futuro* na investigação criminal *caso se verifiquem os pressupostos da norma processual de acesso* (sobre a noção e distinção com a norma processual de conservação v. § 16). A grande diferença é que *ab initio* a conservação ao abrigo da Lei n.º 32/2008, de 17 de julho, tem como *finalidade* a sua utilização numa investigação criminal. O que, diga-se, *também* não é novidade. A conservação de dados resultantes de sistemas de videovigilância, de impressões digitais após uma condenação ou de perfis de ADN, justifica-se com o propósito de auxiliar uma *investigação criminal* que deles venha a necessitar.

§ 5 Duas outras notas a reter. *Primus*, a conservação de dados de tráfego e de localização dos fornecedores de serviços de comunicações *para fins de investigação criminal* ao abrigo da Lei n.º 32/2008, de 17 de julho *não* se deve confundir com a conservação de dados de tráfego de localização para *outros* fins, por exemplo, para *fins de faturação ou de cobrança de serviços de valor acrescentado, nos termos da Lei n.º 41/2004, de 18 de agosto*. As bases de dados que resultam dessas conservações são autónomas, separadas e diferenciadas,

como exige a Lei n.º 32/2008, de 17 de julho. *Secundus*, a intervenção do juiz de instrução criminal a que alude o artigo 9.º da Lei n.º 32/2008, de 17 de julho, é para *decidir* da transmissão para uma investigação criminal de dados *previamente* conservados pelos fornecedores de serviço *nos termos da Lei n.º 32/2008, de 17 de julho*. *Só e apenas estes*. Caso os dados tenham sido conservados para fins comerciais ou contratuais *a norma a convocar terá de ser outra, nomeadamente o artigo 189.º do Código de Processo Penal.* Pela simples razão, *reitera-se*, que a Lei n.º 32/2008, de 17 de julho, *somente* se refere aos dados conservados em servidores das empresas de comunicações com a *expressa finalidade de uma futura investigação criminal*. E essa diferenciação e autonomização implica uma *separação* na conservação de dados mesmo que implique uma *duplicação*. Simplificando, os *mesmos* dados de registo de uma conversa telefónica ou por internet – número de telefone ou IP de origem e destino, tempo da conversação, hora – poderão ser conservados por uma empresa de comunicações nos termos da Lei n.º 41/2004, de 18 de agosto e/ou Lei n.º 32/2008, de 17 de julho. Mas a *conservação* dos mesmos dados é em *duplicado*, devendo constar de base de dados *distintas e autonomizadas.* Desde logo porque os critérios de acesso são *diferentes.*

III – O antes e depois do Acórdão do Tribunal Constitucional n.º 268/2022

§ 6 *Antes* da prolação do Acórdão n.º 268/2022, as empresas fornecedoras de comunicações telefónicas e serviços de internet estavam obrigados por força da Lei n.º 32/2008, de 17 de julho, a conservar de *forma generalizada e indiferenciada* os dados de tráfego e localização dos seus clientes, para fins de investigação criminal. Ou seja, a lei permitia uma *conservação* massiva de dados dos clientes de tais empresas, com o propósito de serem utilizados probatoriamente numa investigação por crimes graves que fossem *relevantes*. Note-se, quer para provar a prática do crime por determinada pessoa, quer para provar a sua inocência, ou, pelo menos, colocar em dúvida as suspeitas que sobre si recaíam por via de outras *provas.* É importante frisar este aspeto: são dados que tanto podem interessar à acusação como à defesa. Basta pensar que um *dado de localização* pode corroborar a *tese da acusação* "colocando" o suspeito no local do crime

ou corroborar a *tese da defesa*, "afastando-o" do mesmo.

§ 7 O Acórdão n.º 268/2022 do Tribunal Constitucional declarou a inconstitucionalidade, com força obrigatória geral, da norma constante dos artigos 4.º, conjugada com o artigo 6.º da mesma lei *e* do artigo 9.º da Lei n.º 32/2008, de 17 de julho. Muito sinteticamente, o Tribunal Constitucional considerou desconforme à Constituição *a*) uma conservação generalizada e indiferenciada de dados de tráfego e localização; *b*) a conservação de dados em servidores fora da União Europeia e *c*) a não comunicação aos visados de que os *seus* dados conservados foram acedidos.

§ 8 Em consequência, *depois* do Acórdão n.º 268/2022 deixou de existir fundamento *legal* para as empresas de comunicações conservarem dados para fins de investigação de crimes graves ao abrigo Lei n.º 32/2008, de 17 de julho. E em relação às *bases de dados existentes* foi ordenada a sua eliminação pela Comissão Nacional de Proteção de Dados (https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-ordena-eliminacao-dos-dados-das-comunicacoes-conservados-ao-abrigo-de-norma-declarada-inconstitucional/). Em suma, a Lei n.º 32/2008, de 17 de julho, passou a ser uma lei morta, cujo renascimento dependeria de uma intervenção legislativa.

IV – As tentativas de o legislador sanar as inconstitucionalidades

§ 9 Seguiu-se ao Acórdão n.º 268/2022 do Tribunal Constitucional um esforço parlamentar para conformar a Lei n.º 32/2008, de 17 de julho, com a Constituição nos termos apontados por aquele Acórdão. Foram apresentados diversos projetos de lei. A discussão culminou com a aprovação de um texto de substituição apresentado pela Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, relativo aos Projetos de Lei n.ºs 70/XV/1.ª (PSD); 79/XV/1.ª (CH); e Proposta de Lei n.º 11/XV/1.ª (GOV) (que pode ser consultado em www.parlamento.pt). Remetido ao Sr. Presidente da República, e face às dúvidas sobre a constitucionalidade, foi suscitada a intervenção do

Tribunal Constitucional. Foi então prolatado o Acórdão n.º 800/2023. Muito sumariamente, o Tribunal Constitucional *aplaudiu* as alterações no sentido de se prever a possibilidade de notificação do visado cujos dados foram acedidos, bem como a exigência de a conservação ter que ocorrer no território da União Europeia. Nessa parte, considerou que o legislador conformou a lei com o Acórdão n.º 268/2022. No mais, embora reconhecendo o esforço do legislador para instituir regras legais maior rigorosas quanto ao modo de conservação, e de reduzir os seus prazos, evidenciou que, mesmo assim, a Constituição apenas permitia a conservação de dados de tráfego e localização para fins de investigação de crimes graves se a mesma fosse *seletiva.* Numa síntese muito apertada foi esta a "mensagem": incidindo a conservação sobre presumíveis inocentes a mesma só poderá ser admitida para fins exclusivos de investigação criminal de crimes graves verificando-se determinados factos que permitam concluir pela proporcionalidade, como por exemplo, a conservação em áreas geográficas com maior número de crimes.

§ 10 Perante o Acórdão do Tribunal Constitucional o diploma foi vetado e devolvido ao Parlamento. Seguiram-se propostas de alteração, discussão e aprovação de texto que deu origem ao decreto da Assembleia da República n.º 131/X, procurando conformar a Lei n.º 32/2008, de 17 de julho, aos Acórdãos do Tribunal Constitucional n.ºs 268/2022 e 800/2023. Deste feita o Presidente da República promulgou o diploma, «[c]*onsiderando que a conservação dos dados de tráfego e de localização fica agora dependente de autorização judicial*» (conforme Sítio Oficial de Informação da Presidência da República Portuguesa, que pode ser acedido em https://www.presidencia.pt/atualidade/toda-a-atualidade/2024/01/presidente-da-republica-apreciou-decretos-da-assembleia-da-republica/). Foi então publicada a Lei n.º 18/2024, de 05 de fevereiro, que procedeu a alterações à Lei n.º 32/2008, de 17 de julho e Lei da Organização do Sistema Judiciário.

V – O resultado final: as novas funções do Supremo Tribunal de Justiça

§ 11 Que solução foi então encontrada pelo legislador? De modo a afastar a inconstitucionalidade resultante de uma conservação obrigatória generalizada e

indiferenciada de dados de tráfego e localização relativos a todos os clientes das empresas de comunicações, a lei passou a prever intervenção de uma «*formação das secções criminais do Supremo Tribunal de Justiça, constituída pelos presidentes das secções e por um juiz designado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções*», para decidir da «*autorização judicial para conservação de dados de tráfego e de localização*» «*no âmbito da Lei n.º 32/2008, de 17 de julho*» (artigos n.º 6.º, n.ºs 2, 3 e 7, da Lei n.º 32/2008, de 17 de julho, 47.º, n.º 4, e 54.º, n.º 4, da Lei de Organização do Sistema Judiciário). Esta *Formação* já existia, mas foi alargada a sua competência a outras matérias (anteriormente a Formação apenas tinha competência, nos termos dos pretéritos artigos 47.º, n.º 4 e 54.º, n.º 4, da Lei de Organização do Sistema Judiciária, para proceder «*ao controlo e autorização prévia dos pedidos fundamentados de acesso a dados de telecomunicações e Internet nos termos do procedimento previsto na lei especial que aprova o regime especial de acesso a dados de base e a dados de tráfego de comunicações eletrónicas pelo Sistema de Informações da República Portuguesa*»). A *finalidade*, já referimos supra, foi compatibilizar a lei com os Acórdãos do Tribunal Constitucional n.ºs 268/2022 e 800/2023 que "exigiam" uma conservação *seletiva*. O legislador atribuiu a uma formação especializada do Supremo Tribunal de Justiça *a finalidade de selecionar os dados de tráfego e localização que podem ser conservados*. Significa que ao contrário da anterior redação da Lei n.º 32/2008, de 17 de julho em que as empresas estavam obrigadas a conservar *todos* os dados *ex lege*, agora *apenas* o deverão fazer a partir do momento em que exista uma decisão de uma formação especializada do Supremo Tribunal de Justiça e *apenas* em relação aos dados *selecionados*.

§ 12 É importante que fique claro que a Lei n.º 18/2024, de 05 de fevereiro, não teve qualquer intenção de atribuir competências de juiz de instrução criminal à formação especializada do Supremo Tribunal de Justiça. Esta formação *não* tem competência para apreciar pedidos formulado num *processo criminal em curso*, que tenham como finalidade a conservação ou acesso a dados de tráfego ou de localização. Essa competência continua a ser do *juiz de instrução criminal*.

§ 13 O procedimento que determina a intervenção do Supremo Tribunal de Justiça é um processo específico e autónomo, despoletado pelo Ministério Público nesse Tribunal, e que tem em vista decidir *quais* os dados de tráfego e localização que as empresas de comunicações devem conservar «*no âmbito da Lei n.º 32/2008, de 17 de julho*». É um procedimento que nada tem a ver com o processo criminal e não se confunde com este (para mais desenvolvimentos v. nossa anotação ao artigo 189.º, Comentário Judiciário do Código de Processo Penal, Tomo II, 4.ª edição, 2024). Nesse procedimento, a pedido do Ministério Público, a Formação *seleciona* os dados que devem ser conservados. Por exemplo, decidindo a conservação de dados de tráfego e localização em áreas geográficas com uma taxa de criminalidade acima de determinada percentagem. Só a partir do momento em que exista uma decisão do Supremo Tribunal nesse sentido, é que a Lei n.º 32/2008, de 17 de julho, ganhará vida. Ou seja, só então as empresas passam a ter *novamente* uma base de dados no *âmbito* da Lei n.º 32/2008, de 17 de julho. Base de dados que garantirá a *conservação* de dados de tráfego e localização de acordo com o *critério* decidido Formação do Supremo Tribunal de Justiça. E esses dados poderão *eventualmente* vir a ser utilizados *posteriormente* em processos criminais, mediante um pedido de acesso de um *juiz de instrução criminal* nos termos do artigo 9.º da Lei n.º 32/2008, de 17 de julho, e *não* da Formação especializada do Supremo Tribunal de Justiça.

§ 14 Ou seja, a Lei n.º 32/2008, de 17 de julho, passou a contemplar dois momentos de intervenção judicial. Um primeiro momento, sem qualquer conexão com um concreto processo criminal, *da competência de uma Formação especializada do Supremo Tribunal de Justiça*, e que serve apenas para "alimentar" uma base de dados que pode vir utilizada hipoteticamente para uma investigação de crimes graves. Uma segunda fase, já no âmbito de um processo criminal, em que por via de suspeitas que incidem sobre determinada pessoa ou pessoas, se procura aceder aos dados de tráfego e localização que foram conservados previamente por ordem da formação do Supremo Tribunal de Justiça, à luz da Lei n.º 32/2008, de 17 de julho. Este pedido de acesso é formulado no processo criminal, e a competência para decidir do mesmo é do *juiz de instrução criminal*, nos termos do artigo 9.º da Lei n.º 32/2008, de 17 de julho.

VI – O âmbito diverso de aplicação do artigo 189.º do Código de Processo Penal. A diferença entre normas processuais penais de acesso e de conservação. A importância *atual* do n.º 2 daquele preceito.

§ 15 O facto de durante cerca de vinte e quatro anos – 2008 a 2022 - os dados de tráfego e localização terem sido pedidos aos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações, ao abrigo da Lei n.º 32/2008, de 17 de julho, interpretada por vezes conjugadamente com a Lei do Cibercrime, de certa maneira, na prática judicial, relegou para "segundo plano" o artigo 189.º do Código de Processo Penal. De modo que, perante as transformações suprarreferidas no plano legal é muito importante atentar em alguns conceitos para que fique perfeitamente esclarecido a importância *atual* deste preceito no acesso a dados de tráfego e localização conservados, quer para descobrir o crime e seus agentes, quer para provar a inocência de uma pessoa. Pode ser a *diferença* entre proteger ou desproteger uma vítima quando é prova essencial para demonstrar o crime a que foi sujeita. Ou a *diferença* entre condenar ou absolver o arguido, quando é prova essencial para colocar em dúvida os factos da acusação.

§ 16 O artigo 189.º, n.º 2, do Código de Processo Penal e o artigo 9.º da Lei n.º 32/2008, de 17 de julho são normas processuais penais de acesso[1] [2], ou seja, normas processuais penais que estabelecem os pressupostos para aceder e transmitir ao processo criminal dados de tráfego e de localização conservados por entidades privadas ou públicas ao abrigo da lei, por decisão judicial, por via de um contrato ou de um qualquer ato de aceitação de uma pessoa (v.g. fins científicos, médicos, estatísticos, desde que não colida com a lei, bons

[1] Sobre o facto de «dados sobre a localização celular ou de registos da realização de conversações ou comunicações» a que alude o artigo 189.º, n.º 2, do Código de Processo Penal, abranger os denominados dados de localização e de tráfego, mais desenvolvidamente, v. anotação ao artigo 189.º do Código de Processo Penal, Comentário Judiciário do Código de Processo Penal, Tomo II, Almedina, 4.ª edição, 2024.

[2] O artigo 189.º, n.º 2, do Código de Processo Penal *também* é uma norma processual penal de conservação, ou seja, uma norma que estabelece os pressupostos para que sejam conservados para o futuro num processo criminal em curso dados de tráfego e localização que relevem para a investigação. Mas esta dimensão da norma não releva atento o objeto a que se circunscreve o tema deste escrito.

costumes, ou ordem pública, cf. artigo 280.º do Código Civil). São estas a porta de acesso a dados de tráfego e localização gerados por comunicações e conservados[3] por fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações. Mas com âmbito de aplicação e extensão diferenciáveis. O artigo 9.º da Lei n.º 32/2008, de 17 de julho, é a porta de acesso à base de dados criada por essa mesma lei e conservada pelos fornecedores de serviço para fins exclusivos de investigação criminal. Essa base de dados dependerá, como suprarreferido, de uma decisão de uma Formação especializada do Supremo Tribunal de Justiça, que, por sua vez, depende do impulso do Ministério Público. Ao que se sabe esse impulso ainda não existiu pelo que a base de dados está esvaziada. Ou seja, quer seja como prova da acusação, ou da defesa, enquanto não for alimentada a base de dados o artigo 9.º da Lei n.º 32/2008, de 17 de julho existe no papel, mas não na prática.

§ 17 Em relação ao artigo 189.º, n.º 2, do Código de Processo Penal está vivo, não foi revogado, nem derrogado e assume um papel importante, tal qual, aliás, tinha antes da Lei n.º 32/2008, de 17 de julho. Na verdade, mesmo antes da existência de uma base de dados criada exclusivamente para investigação criminal, já as empresas que forneciam serviços de comunicações conservavam dados de tráfego e localização para *fins contratuais*, nomeadamente para efeito de faturação detalhada e, não obstante, transmitiam ao processo penal essa informação, desde que verificados os pressupostos previstos no Código de Processo Penal. Aliás, no Ac. TC n.º 486/2009, num momento em que já vigorava a Lei n.º 41/2004, de 18 de agosto, *não* se julgou inconstitucional a possibilidade de transmissão de faturação detalhada e dados de localização. O essencial é que a autorização seja decidida pelo juiz de instrução criminal nos termos do artigo 269.º, n.º 1, alínea e), do Código de Processo Penal[4], numa interpretação conforme à

[3] O artigo 189.º, n.º 2, do Código de Processo Penal, aliás, é essencial para a efetividade dos atos de preservação previstos no artigo 12.º e 13.º da Lei do Cibercrime, já que esta norma não disciplina sobre os pressupostos do acesso e transmissão de dados de tráfego e localização conservados pelos fornecedores de serviço, mas apenas dos dados de base cf. artigo 14.º, n.º 4, da Lei do Cibercrime.

[4] São situações em que se considera que existem interesse prevalecentes sobre o segredo profissional das empresas que conservam esses dados. A ser invocado o segredo profissional devem seguir-se as regras do processo penal. Caso a empresa tenha conservado indevidamente dados está em causa uma situação de valoração probatória, em que se deverá

Constituição de que a ordem ou autorização não é apenas em relação ao *registo* para o *futuro* de dados de tráfego ou localização, mas abrange também o *acesso* a *registos* efetuados no *passado*.

§ 18 O artigo 189.º, n.º 2, do Código de Processo Penal, nomeadamente na parte em que admite o pedido de transmissão de dados de tráfego e de localização às empresas fornecedoras de serviços, que estejam conservados em base de dados *distintas* das criadas pela Lei n.º 32/2008, de 17 de julho (as relativas à investigação criminal), *não* se encontra abrangido pela declaração de inconstitucionalidade do Acórdão do TC n.º 800/2023. O seu parágrafo 40 distingue a base de dados «*para efeitos de faturação*», da Lei n.º 41/2004, de 18 de agosto, em que «*está em causa a conservação dos dados para efeitos de faturação e proteção comercial (relação jurídica de natureza cível)*» e a base de dados da Lei n.º 32/2008, de 17 de julho, em que está em causa «*a conservação de dados para efeitos de investigação e repressão criminal*».

19. A possibilidade do tratamento de dados parece também não estar vedada pelo artigo 23.º/1/d do Regulamento Geral de Proteção de Dados, ao admitir a transmissão se for necessária para a investigação e se revelar proporcional. Proporcionalidade que resulta da aplicação dos pressupostos previstos no artigo 187.º do Código de Processo Penal e da intervenção do juiz. E igualmente não se vislumbra que a própria Lei n.º 41/2004, de 18 de agosto o proíba. É perfeitamente possível interpretar o artigo 1.º, n.º 4, no sentido de que o artigo 189.º, n.º 2, do Código de Processo Penal, é «legislação especial», uma vez que contém uma norma *específica* sobre os pressupostos de transmissão para o processo penal. E o artigo 6.º, n.º 7, também pode ser interpretado subsumindo no conceito de «nos termos da legislação aplicável, com vista à resolução de litígios», a prova necessária para o processo criminal. Aliás, seria no mínimo estranho que os dados de tráfego e localização

atender ao caso concreto, e que convoca questões relativas a restrições admissíveis nos termos do artigo 18.º, n.º 2, da Constituição, quais os interesses comprimidos e que se visam salvaguardar e critérios de aproveitabilidade de prova em processo penal que extravasam o âmbito deste trabalho. Para alguns considerandos v. anotações ao artigo 125.º, 126.º e 190.º do Código de Processo Penal, em Comentário Judiciário ao Código de Processo Penal, Tomo II, 4.ª edição, 2024.

pudessem ser usados para um litígio de 100 euros e a ordem jurídica fosse perentória em proibir o seu uso no processo de homicídio. De todo modo, como se escreve no Ac. do STJ, Relator Lopes da Mota, processo n.º 170/11.2TAOLH-E.S1, 31.01.2024, www.dgsi.pt, «*cabe ao direito nacional determinar as condições em que os prestadores de serviços devem conceder às autoridades nacionais competentes o acesso aos dados de que dispõem*», que se encontra regulada pelos «*artigos 187.º a 189.º e 269.º, n.º 1, al. e), do Código de Processo Penal e pela Lei n° 109/2009, de 15 de setembro (Lei do Cibercrime)*», e «[o] *respeito por estas regras na aquisição da prova obtida por recurso aos dados pessoais objeto de conservação impedirá que se possa, em qualquer circunstância, formular um juízo negativo sobre a sua validade, nos termos do artigo 126.º, n.º 3, do CPP*» (sublinhado aditado). Aliás, mesmo para quem vir alguma incompatibilidade ou entenda que a Lei n.º 41/2004, de 18 de agosto, pode disciplinar sobre matéria de processo penal relativa ao acesso a prova, então sempre teria que considerar que o n.º 2 do artigo 189.º do Código de Processo Penal, sendo de 2007, é *posterior* à Lei n.º 41/2004, de 18 de agosto.

§ 20 E para terminar, importa ter presente que pelo uso de novas tecnologias a conservação de dados é uma realidade cada vez mais presente quer no âmbito da prestação de serviços ou mesmo a nível laboral. Pense-se, por exemplo, nos dados de localização que são conservados pela via de prestação de serviços – v.g. de natureza contratual – por exemplo em apps de saúde, que monitorizam corridas ou aquelas que indicam trajetos a veículos automóveis. Ou no plano laboral, dados de tráfego monitorizados e conservados relativos a comunicações em emails profissionais, nos termos contratualizados. Casos em que o artigo 189.º, n.º 2, do Código de Processo Penal (mas também o artigo 14.º, n.º 1, da Lei do Cibercrime) continua a ser uma norma processual crucial para decidir do acesso a dados conservados por terceiros.