Jurisprudência Temática de Direito Processual Penal
N.º 145 – Janeiro de 2026

PRESERVAÇÃO E REVELAÇÃO EXPEDITA DE DADOS DE TRÁFEGO, INJUNÇÃO PARA APRESENTAÇÃO OU CONCESSÃO DO ACESSO A DADOS E ACÇÕES ENCOBERTAS

JURISPRUDÊNCIA DO TRIBUNAL CONSTITUCIONAL

Acórdão n.º 403/2015 de 17 de setembro de 2015 (Processo n.º 773/15)
Inconstitucionalidade

«Decide pronunciar-se pela inconstitucionalidade da norma do n.º 2 do artigo 78.º do Decreto n.º 426/XII da Assembleia da República que «Aprova o Regime Jurídico do Sistema de Informações da República Portuguesa», por violação do n.º 4 do artigo 34.º da CRP.»

JURISPRUDÊNCIA DO SUPREMO TRIBUNAL DE JUSTIÇA

Acórdão n.º 10/2023 de 10 de novembro de 2023 (Processo n.º 184/12.5TELSB-R.L1-A.S1)
Acórdão de fixação de jurisprudência – Inquérito – Juiz de Instrução – Competência – Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – Lei do cibercrime

«Na fase de inquérito, compete ao juiz de instrução ordenar ou autorizar a apreensão de mensagens de correio eletrónico ou de outros registos de comunicações de natureza semelhante, independentemente de se encontrarem abertas (lidas) ou fechadas (não lidas), que se afigurem ser de grande interesse para descoberta da verdade ou para a prova, nos termos do art. 17.º, da Lei n.º 109/2009, de 15/09 (Lei do Cibercrime)»

Acórdão n.º 12/2024 de 20 de setembro de 2024 (Processo n.º 28999/18.3T8LSB-B.L1-A.S1)
Acórdão de fixação de jurisprudência – Processo de contraordenação – Concorrência – Apreensão de correio eletrónico e registos de comunicações de natureza semelhante – Natureza semelhante – Juiz de Instrução – Competência

«Em processo de contraordenação relativo a práticas restritivas da concorrência previstas no Regime Jurídico da Concorrência (Lei n.º 19/2012, de 8 de maio), compete ao juiz de instrução ordenar ou autorizar a apreensão de mensagens de correio eletrónico ou de outros registos de comunicações de natureza semelhante, independentemente de se encontrarem abertas (lidas) ou fechadas (não lidas), que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, nos termos do art. 17.º da Lei n.º 109/2009, de 15/09 (Lei do Cibercrime), aplicável por força do disposto no art. 13.º, n.º 1, do RJC, e do art. 41.º, n.º 1, do RGCO.»

JURISPRUDÊNCIA DO TRIBUNAL DA RELAÇÃO DE LISBOA

Acórdão de 11 de maio de 2023 (Processo n.º 215/20.5T9LSB-C.L1-9)
Cibercrime – Recolha de prova – Procedimento – Valoração – Juiz de Instrução

«I – A Lei do Cibercrime é uma legislação especial que veio estabelecer disposições penais materiais e processuais relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico (secundarizando o Código de Processo Penal) para fazer face a novas realidades e inerentes especificidades, tais como dos dados informáticos e do correio electrónico, justificando-se o sacrifício do

interesse individual numa comunicação livre de interferências alheias, em prol do exercício do "ius puniendi" estadual.

II - Mas, a apreensão (mesmo gozando de legitimidade formal pela existência de prévia autorização ou ordem judicial de apreensão) não legitima, "per si", a valoração dos elementos probatórios assim conseguidos.
Para o efeito, é ainda necessário que o Juiz seja a primeira pessoa a tomar conhecimento do conteúdo apreendido, conhecimento esse que não tem de ser obrigatoriamente completo/total.
Depois, os elementos apreendidos podem ser enviados pelo Juiz ao Ministério Público para que este emita proposta/parecer sobre a relevância, ou não, para a descoberta da verdade ou para a prova dos factos em investigação (pelo mesmo (Ministério Público face à estrutura acusatória de qualquer processo penal).
Então o Juiz estará em condições de melhor aferir qual o conteúdo relevante e ponderar da necessidade, ou não, da sua junção aos autos como meios de prova e, em caso afirmativo, com a inerente compressão de direitos constitucionais.

III - O Juiz de instrução é um garante dos direitos fundamentais dos diversos intervenientes no processo penal, porém não controla o exercício da ação penal.
A intervenção do Juiz de Instrução Criminal em sede de inquérito deve pautar-se por um princípio da intervenção enquanto Juiz das liberdades (e não como Juiz de investigação), respeitando o modelo constitucional de divisão de funções entre a magistratura judicial e a magistratura do Ministério Público.»

Acórdão de 11 de abril de 2023 (Processo n.º 267/21.0JELSB-Q.L1-5)
Perícia à voz – Valoração da prova obtida no estrangeiro – DEI (Decisão Europeia de Investigação) – Lei do Cibercrime

«Da leitura do artigo 155.º do Código de Processo Penal decorre que a presença de consultor técnico na perícia não é imperiosa ["1- Ordenada a perícia, o Ministério Público, o arguido, o assistente e as partes civis podem designar para assistir à realização da mesma, se isso ainda for possível, um consultor técnico da sua confiança." (…)], não tem que anteceder a realização da perícia ["3 - Se o consultor técnico for designado após a realização da perícia, pode, salvo no caso previsto na alínea a) do n.º 5 do artigo anterior, tomar conhecimento do relatório] e não pode constituir motivo para atrasar as démarches do processo ["4-A designação de consultor técnico e o desempenho da sua função não podem atrasar a realização da perícia e o andamento normal do processo."].

A emissão da DEI encontra-se rodeada de diversas cautelas, pressupõe a verificação de diversas condições e é suscetível de recurso, pelo que, inexistindo qualquer elemento nos autos ou qualquer notícia de que tenha sido emitida em desobediência aos respetivos preceitos legais que a regulamentam ou que sobre essa decisão tenha incidido qualquer recurso, não há qualquer razão que impeça o tribunal de fazer uso dos elementos de prova transmitidos ao processo, pelas autoridades francesas, através da DEI.

Nos casos em que os pedidos se reportam a dados já preservados, já obtidos e já armazenados por autoridades estrangeiras, em que se pretende a sua transmissão para um processo penal nacional, regem exclusivamente os artigos 12.º a 17.º da Lei do Cibercrime [Lei n.º 109/2009 de 15/09] e não o artigo 187.º do Código de Processo Penal.»

Acórdão de 25 de outubro de 2022 (Processo n.º 103/21.8TELSB-A.L1-5)
Lei do Cibercrime – Apreensão de correio eletrónico – Autorização – Despacho judicial prévio – Nulidade

«I - Face à arquitetura normativa patente na Lei do Cibercrime, tem de entender-se que o regime previsto no artigo 16º deve aplicar-se sempre que esteja em causa a apreensão de dados informáticos e o do artigo 17º sempre que esteja em causa a apreensão de correio eletrónico e registo de comunicações de natureza semelhante – que, sendo dados informáticos em si mesmos, se apresentam como qualitativamente diversos, em função do nível de intromissão na vida privada e nas comunicações que a sua apreensão é suscetível de importar.

II - A apreensão de correio eletrónico ou de registos de comunicações de natureza semelhante carece, *sob pena de nulidade*, de despacho judicial prévio.

III - Se, ao determinar a realização de busca não domiciliária, o MP antevê a apreensão de mensagens de correio eletrónico, tem de solicitar – e obter – *previamente* autorização judicial para o efeito, não podendo determinar a apreensão de «dados eletrónicos» para posterior apresentação ao Juiz de Instrução para validação.

IV - Estando o MP ciente, ao determinar a realização da busca não domiciliária, de que a mesma teria como consequência a interferência em dados protegidos – nomeadamente, comunicações de correio eletrónico – não pode acolher-se àquela que se configura como *válvula de segurança* do sistema, a situação *excecional* tida em vista no artigo 16º da Lei do Cibercrime. Aceitar tal asserção seria sufragar, precisamente, a posição que o acórdão TC 678/2021 julgou inconstitucional.»

Acórdão de 29 de setembro de 2021 (Processo n.º 158/19.5JELSB.A.L1-3)
DEI (Decisão Europeia de Investigação) – Lei do Cibercrime

«A DEI tem como objecto o estabelecimento do regime jurídico da emissão, transmissão e do reconhecimento e execução de decisões europeias de investigação, transpondo para a ordem jurídica interna a Directiva 2014/41/UE do Parlamento Europeu e do Conselho, de 3 de Abril de 2014, relativa à decisão europeia de investigação (DEI) em matéria penal (artº1). E aplica-se à obtenção de novos elementos de prova e à transmissão de elementos de prova na posse das autoridades competentes do Estado de execução, em todas as fases do processo.

Estamos perante questões relativas a aquisição probatória, que se mostram definidas na Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro) e, no caso dos autos, no âmbito de prova eletrónica preservada ou conservada em sistemas informáticos – isto é, já obtida e existente em processo que corre seus termos em jurisdição não nacional.
Nesses casos, o sistema processual penal aplicável é o previsto nos artigos 12º a 17º da Lei nº109/2009, de 15-09, Lei do Cibercrime (coadjuvado pela Lei nº 32/2008, neste caso se estivermos face à prova por "localização celular conservada"), pois estes artigos constituem um completo regime processual penal para os crimes que, nos termos das alíneas do nº 1 do artº 11º, ou estão previstos nessa lei, ou foram cometidos por meio de um sistema informático, ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

À situação dos autos não é aplicável o disposto no artº 18 da Lei do Cibercrime, razão pela qual se mostra inadmissível (quer pela sua própria natureza, quer pela ausência de norma que o suporte) proceder-se nestas situações (prova preservada ou conservada) à aplicação do regime previsto no nº6 do artº 187 do C.P. Penal.»

Acórdão de 06 de fevereiro de 2018 (Processo n.º 1950/17.0T9LSB-A.L1-5)
Correio electrónico – Apreensão de correspondência

«A Lei do Cibercrime, lei nº 109/2009, de 15 de Setembro, a qual transpõe para a ordem jurídica interna a Decisão Quadro nº 2005/222/JAI, do Conselho da Europa, de 24 de Fevereiro, relativa a ataques contra sistemas de informação e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, determina no seu art.º 17º, sob a epígrafe da "*apreensão de correio electrónico e registo de comunicações de natureza semelhante*", dispõe que, quando no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados armazenados nesse sistema informático ou noutro que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio electrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime de apreensão de correspondência previsto no Código de Processo Penal.

Aplicando-se assim o regime de apreensão de correspondência previsto no Código de Processo Penal, este encontra-se disciplinado no art.º 179º, o qual estabelece desde logo no n.º 1 que tais apreensões sejam determinadas por despacho judicial, "*sob pena de nulidade*" expressa (n.º 1), e que "*o juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida*", o que se aplica ao correio electrónico já convertido em ficheiro legível, o que constitui acto da competência exclusiva do Juiz de Instrução Criminal, nos termos do art.º 268º n.º 1 alínea d) do CPP, o qual estabelece que "*compete exclusivamente ao juiz de instrução, tomar conhecimento, em primeiro lugar, do conteúdo da correspondência apreendida*", o que se estendeu ao conteúdo do correio electrónico, por força da subsequente Lei nº 109/2009, de 15 de Setembro, constituindo a sua violação nulidade expressa absoluta e que se reconduz, a final, ao regime de proibição de prova.

A falta de exame da correspondência pelo juiz constitui uma nulidade prevista no art.º 120º n.º 2 alínea d) do CPP, por se tratar de um acto processual legalmente obrigatório.»

Acórdão de 19 de junho de 2014 (Processo n.º 1695/09.5PJLSB.L1-9)
Difamação – Internet – Dados de tráfego

«Estando apenas em causa a obtenção da identificação de um utilizador de um endereço IP ou o número de IP usado por um determinado indivíduo, em circunstâncias temporais determinadas, a competência para a respetiva obtenção é do Ministério Público.

A identificação de um determinado endereço de IP conjugada com a identidade de quem o utilizou num dado dia e hora não revela informação sobre o percurso da comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa

Os direitos constitucionais dos arguidos não são absolutos, face aos direitos dos restantes cidadãos, mormente das vítimas em processo penal, e as entidades públicas, ao enquadrar o uso dos diversos meios de prova têm de considerar os direitos dos vários intervenientes processuais.»

Acórdão de 22 de janeiro de 2013 (Processo n.º 581/12.6PLSNT-A.L1-5)
Lei do Cibercrime – Acesso ilegítimo – Dados de tráfego – Interceção

«A obtenção de um concreto endereço IP que esteve na origem da uma determinada comunicação efetuada é da competência do Ministério Público - e não do juiz.

A Lei do Cibercrime (Lei n.º 109/2009 de 15 de Setembro) nos seus artigos 12.º a 17.º respeitam a meios de obtenção de prova, mormente sua conservação e recolha. São eles: a "preservação expedita de dados", a "revelação expedita de dados de tráfego", a "injunção para apresentação ou concessão de acesso a dados", a "pesquisa de dados informáticos", a "apreensão de dados informáticos" e, finalmente, a "apreensão de correio eletrónico e registo de comunicações de natureza semelhante".

Com exceção desta última, em que se faz expressa menção à intervenção do juiz, todas as outras diligências são levadas a cabo por ordem da autoridade judiciária competente o que necessariamente inculca a ideia de que essa autoridade judiciária pode ser o Ministério Público ou o Juiz consoante a fase processual.

Este novo regime especial de obtenção de meios de prova teve em vista superar a lacuna da Lei n.º 109/91 de 17 de Agosto (Criminalidade Informática) que por não conter essas normas processuais que adequassem o regime legal às particularidades da investigação "empurrou" a jurisprudência para a interpretação de que só em relação a crimes de catálogo seria possível a obtenção de certo tipo de dados como os dados de tráfego e mercê da intervenção do juiz de instrução (cfr. por exemplo, o Ac. T.R.E. de 26.06.2007, proc. 843/07-1, em que estava em causa a investigação do crime de acesso ilegítimo do art. 7.º, n.º 1 da citada Lei nº 109/91).

Significa isto, na leitura integrada de todo o regime legal, que se julga adequada a interpretação de que se os dados a obter são "dados de tráfego", de acordo com a definição do art. 2.º, al. c) da Lei do Cibercrime, e tiverem de ser recolhidos junto de uma operadora localizada em território nacional, independentemente de estarmos perante "crimes graves", enunciados no artigo 2º, nº 1, alínea g) da Lei 32/2008 de 17 de Julho, poderá a autoridade judiciária competente, tendo em vista a descoberta da verdade, ordenar que estes sejam disponibilizados sob pena de punição por desobediência. É o que resulta do disposto no art. 14.º, n.ºs 1, 2, 3 e 4 da mesma Lei.

Pedir à operadora que forneça os dados em questão não é a mesma coisa que proceder a uma interceção de uma comunicação, mesmo que com esta se vise proceder ao registo de "dados de tráfego".»

Acórdão de 11 de janeiro de 2011 (Processo n.º 5412/08.9TDLSB-A.L1-5)
Correio eletrónico – Apreensão de correspondência – Juiz de instrução criminal

«Iº A Lei do Cibercrime (Lei nº109/09, de 15Set.), ao remeter no seu art.17, quanto à apreensão de mensagens de correio electrónico ou registos de comunicações de natureza semelhante, para o regime geral previsto no Código de Processo Penal, determina a aplicação deste regime na sua totalidade, sem redução do seu âmbito;

IIº As mensagens de correio electrónico ou registos de comunicações de natureza semelhante, que se afigurem de grande interesse para a descoberta da verdade ou para a prova, podem ser apreendidas, aplicando-se correspondentemente o regime de apreensão de correspondência previsto no CPP;

IIIº Tais apreensões têm de ser autorizadas ou determinadas por despacho judicial, devendo ser o juiz a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida, sob pena de nulidade;

IVº Em caso de urgência, isto é, de perda de informações úteis à investigação de um crime em caso de demora, o juiz pode autorizar a abertura imediata de correspondência (assim como de correio electrónico) pelo órgão de polícia criminal e o órgão de polícia criminal pode mesmo ordenar a suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações, nos termos dos nºs2 e 3, do art.252, do Código de Processo Penal, devendo a ordem policial ser convalidada no prazo de 48 horas, sob pena de devolução ao destinatário caso não seja convalidada, ou caso seja rejeitada a convalidação;»

JURISPRUDÊNCIA DO TRIBUNAL DA RELAÇÃO DO PORTO

Acórdão de 11 de dezembro de 2024 (Processo n.º 5722/22.2T9AVR-A.P1)
Convenção de Budapeste – Lei do Cibercrime – Interpretação da Lei – Elementos essenciais – Jurisprudência internacional – Princípio da territorialidade – Sistema informático – Dados pessoais – Acesso a dados – Legalidade

«I - Contextualizando-se a interpretação com um sentido atualista dos art.ºs 19º, 22º e 32º da Convenção sobre o Cibercrime, adotada em Budapeste em 23 de novembro de 2001, à luz dos respetivos objeto e fim, tendo-se devidamente em conta os elementos sistemático e teleológico, assim como a jurisprudência internacional relevante, nomeadamente os Acórdão do Supremo Tribunal Federal Suíço, de 24/05/2017, e do Supremo Tribunal da Noruega, de 29/03/2019 (caso *Tidal*), cujos países são Partes naquela Convenção, não haverá violação do princípio da territorialidade no acesso e recebimento de dados informáticos armazenados em *Cloud Computing*, num servidor localizado em território estrangeiro, quando, de harmonia com a legislação interna, os dados pesquisados, ainda que localizados fora do respetivo território, o foram através de credenciais que em si permitiam o acesso legítimo a esses mesmos dados por parte da entidade investigada, a partir do seu próprio território, não assumindo ademais a busca informática realizada uma dimensão que pudesse materialmente pôr em causa o princípio da soberania de outro Estado.

II - O princípio da territorialidade, nos termos previstos na Convenção de Budapeste, assim como o princípio do primado do direito internacional convencional sobre o direito ordinário interno, não terão possibilidade de aplicação quando a busca informática a realizar tiver por objeto dados de um sistema informático situado num "espaço virtual" relativamente ao qual se desconhece o local geográfico das máquinas ou dos materiais físicos de suporte onde tal sistema informático e respetivos dados se encontram guardados, ou, conhecendo-se esse local, o respetivo país não tenha ratificado, aceitado ou aprovado aquela Convenção, nos termos dos art.ºs 2º da Convenção de Viena sobre o Direito dos Tratados e 36º da Convenção sobre o Cibercrime.

III – Concomitantemente não haverá qualquer questão de ilegalidade por confrontação de normas de direito internacional convencional com as normas de direito ordinário interno, e assim também qualquer violação do art.º 8º, nº 2, da Constituição da República Portuguesa.

IV - A determinação pelo Ministério Público, na qualidade de autoridade judiciária, no sentido de se proceder cautelarmente à realização de cópias digitalmente encriptadas, devidamente seladas, sendo uma delas para entregar ao Juiz de instrução criminal, de cujo conteúdo virá este a ter conhecimento em primeiro lugar, tendo em vista a apreciação da existência ou não de grande interesse da mesma para a descoberta da verdade ou para a prova, harmoniza-se com o regime legalmente previsto na Lei do Cibercrime, nomeadamente no seu art.º 17º, relativo à apreensão de correio eletrónico, mostrando-se ademais devidamente salvaguardado o sigilo da correspondência, bem como a garantia de reserva de juiz na tutela dos direitos fundamentais com ela relacionados, tal como sucederá quando no decurso de uma busca informática venham a ser detetados dados suscetíveis de revelar informação de natureza pessoal ou íntima dos visados, nos termos do artigo 16º, nº 3, daquela Lei.

V - A envergadura da investigação, a sua dimensão e a quantidade de dados a pesquisar, torna proporcional e justificada a pesquisa informática sem a utilização de 'palavras-chave', sob pena de ficar inabalavelmente prejudicada a pesquisa a realizar e com ela a descoberta da verdade.»

Acórdão de 18 de janeiro de 2023 (Processo n.º 47/22.6PEPRT-P.P1)

Dados de tráfego – Interceção – Localizador celular – Comunicação – Roaming – Tempo real – Interceção de conversa telefónica – Equiparação – Metadados

«- Os fundamentos de inconstitucionalidade declarada, com força obrigatória geral, no ac TC n.º 268/2022, de 19.04, não têm aplicação na interceção de dados de tráfego, incluída localização celular, em tempo real durante a investigação.

II – A interceção de dados de tráfego, como a faturação detalhada, onde constem as chamadas efetuadas e recebidas (trace-back), as localizações celulares e a identificação dos números que os contactem e as comunicações em roaming, quando obtidas em tempo real, durante a investigação, em relação a suspeitos ou arguidos (nº 4, al. a) do art.187º, do CPP), não implica uma ingerência desproporcional nos direitos fundamentais ao respeito pela vida privada e familiar e à proteção de dados pessoais previstos nos art.ºs 7.º e 8.º da C.D.F.U.E., bem assim nos nºs 1 e 4 do art.35.º e do n.º 1 do art.26.º, da C.R.P.

III - À semelhança dos dados de conteúdo (escutas telefónicas), a interceção de dados de tráfego, incluídas localizações celulares, em tempo real, durante a investigação, pressupõe a interceção ou monitorização dos mesmos, à semelhança das escutas telefónicas, e não o recurso a base de dados de conservação ou armazenamento das operadoras relativas a todos os assinantes e utilizadores registados, situação, única, a que se refere o ac TC 268/2022 e a Lei nº 32/2008, de 17 de julho.

IV – Permitir o acesso e valoração no processo penal de metadados obtidos e tratados para efeitos de faturação entre cliente e operadora é o mesmo que consentir na sua utilização para uma finalidade diferente daquela para a qual foram conservados, defraudando o âmbito de regulamentação prevista na Lei 41/2004, de 18 de agosto, para acudir à investigação criminal.

V - Relativamente aos dados de tráfego, incluídas localizações celulares, em tempo real, o regime de extensão contido no artigo 189.º, nº 2, continua a ter a aplicação aos crimes de catálogo previsto no art.187º, nº1, ambos do Código Processo Penal. Nesse caso, também o regime especial do art.18º, nº 1 e

3, da Lei n.º 109/2009, de 05.09 (Lei do Cibercrime) continua a ter a aplicação aos crimes de catálogo previstos nesse normativo.

VI – O arguido ou suspeito, cujos dados de trafego e dados de localização virão a ser intercetados, beneficia das garantias de controlo estabelecidas para as escutas telefónicas nos art.s 187º e 188º, do CPP, aqui aplicáveis mutatis mutandi, não havendo razão para impor à interceção de dados de tráfego, em tempo real, uma comunicação que é dispensada na interceção de dados de conteúdo (escutas telefónicas), a pretexto do direito à autodeterminação informativa e tutela jurisdicional efetiva previstos no n.º 1 do art.35.º e do n.º 1 do art.20.º, da C.R.P..»

Acórdão de 05 de abril de 2017 (Processo n.º 671/14.0GAMCN.P1)
Lei do Cibercrime – Facebook – Prova

«I – O Facebook é uma rede social que funciona através da internet, operando no âmbito de um sistema informático pelo que a recolha de prova está sujeita à Lei do Cibercrime - DL 109/2009 de 15/9.

II – Constitui prova legal a cópia de informação que alguém publicita no seu mural do Facebook sem restrição de acesso.

III – Só esta sujeita à disciplina do art.º 16º 1 e 3 da Lei do Cibercrime a apreensão da informação original inserta na plataforma, esteja ou não disponível.»

Acórdão de 12 de setembro de 2012 (Processo n.º 787/11.5PWPRT.P1)
Prova proibida – SMS (Short Message Service)

«I - O órgão de polícia criminal pode proceder a pesquisa em telemóvel ou outro suporte informático, sem prévia autorização da autoridade judiciária, para que decida da conveniência da sua apreensão. Porém, essa possibilidade está limitada aos casos em que a mesma seja voluntariamente consentida por quem tiver a disponibilidade ou o controlo desses dados – desde que o consentimento prestado fique, por qualquer forma, documentado – ou, nos casos de terrorismo, criminalidade violenta ou altamente organizada, quando haja fundados indícios da prática iminente de crime que ponha em grave risco o vida ou a integridade de qualquer pessoa.

II – Não sendo essa a situação, se as sms [short message service] guardadas no telemóvel do arguido foram lidas e transcritas pelo órgão de polícia criminal sem o seu consentimento nem foi autorizada a sua apreensão pelo juiz de instrução criminal, autoridade judiciária naquele momento competente para o efeito, estamos perante um caso de prova proibida.»

JURISPRUDÊNCIA DO TRIBUNAL DA RELAÇÃO DE COIMBRA

Acórdão de 12 de outubro de 2022 (Processo n.º 538/22.9JALRA.C1)
Metadados – Dados de base – Dados de tráfego – Dados de conteúdo – Dados de localização celular – Obtenção de dados de localização – Obtenção de facturação detalhada; Declaração de inconstitucionalidade com força obrigatória geral das normas a que se reporta o Ac. do TC n.º 268/2022 – Âmbito de aplicação dos artigos 187.º e 189.º do CPP – Da Lei 32/2008 de 17-17 – Da Lei 109/2009 de 15-09 e da Lei 41/2004 de 18-18

«I - «Metadados» são dados referentes ao tráfego das comunicações electrónicas e de localização, bem como os dados conexos necessários para identificar o assinante e/ou utilizador, permitindo determinar todos os dados atinentes àquela forma de comunicabilidade, com excepção do seu teor ou conteúdo, onde se incluem as informações de localização, de identificação de fonte e destino, data, hora, duração da comunicação, tipo de comunicação e o equipamento utilizado.

II – Os serviços de telecomunicações compreendem, fundamentalmente, os dados de base, os dados de tráfego e os dados de conteúdo.

III – Os dados de base são os dados respeitantes à conexão à rede, ou seja, são os dados através dos quais o utilizador da rede de telecomunicações tem acesso à ligação.

IV – Os dados de tráfego correspondem aos dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede.

V – Por último, os dados de conteúdo são os dados alusivos ao conteúdo da comunicação ou da mensagem.

VI – Os dados de localização, inseridos no âmbito dos dados de tráfego, são os dados tratados numa rede de comunicações electrónicas que indicam a posição geográfica do equipamento terminal de um assistente ou de qualquer utilizador de um serviço de comunicações electrónicas acessíveis ao público.

VII– Só cabem dentro dos dados de localização os autênticos dados de comunicação ou de tráfego, i.e., aqueles que se reportam a comunicações efectivamente realizadas ou tentadas/falhadas entre pessoas.

VIII - O regime estabelecido pela Lei n.º 32/2008, de 17 de Julho, aplica-se à obtenção de dados correspondentes a comunicações já ocorridas e que se encontram preservados ou conservados.

IX – Tratando-se de obter prova por "localização celular conservada", isto é, concernente aos dados previstos no artigo 4.º, n.º 1, da Lei n.º 32/2008, o regime processual aplicável assume especialidade nos artigos 3.º e 9.º deste diploma, regime que, sendo especial, se sobrepõe ao de carácter geral instituído pelos artigos 12.º a 17.º da Lei n.º 109/2009, de 15 de Setembro – Lei do Cibercrime –, a qual, de resto, expressamente ressalva, no artigo 11.º, n.º 2, que as suas disposições processuais não prejudicam o regime do outro corpo de normas referido.

X – Já o artigo 189.º, n.º 2, do CPP, com a extenção do regime das escutas telefónicas nele consagrada, remetendo para os requisitos de admissibilidade fixados no artigo 187.º, n.ºs 1 e 4 do mesmo diploma, tem em vista os dados recolhidos em tempo real.

XI – Por sua vez, a aplicação da Lei 41/2004, de 18 de Agosto, limita-se à protecção contratual, no contexto das relações estabelecidas entre as empresas fornecedoras de serviços de comunicações electrónicas e os seus clientes, não sendo lícito recorrer a ela para efeitos de investigação criminal.

XII – Mesmo a considerar-se aplicável este diploma, à luz do artigo 6.º, n.º 2, ele não permitiria o pedido de dados de localização.

XIII – A declaração de inconstitucionalidade, com força obrigatória geral, das normas a que se reporta o recente Acórdão n.º 268/2022 do Tribunal Constitucional, tendo por base a consideração de que as mesmas permitiam lesão desproporcionada da reserva da intimidade e da vida privada dos cidadãos, veda o acesso aos dados não permitidos com recurso à Lei 32/2008; de outro modo, a declaração de inconstitucionalidade permitiria o efeito contrário àquele que definiu.

IVX – Não existindo qualquer identidade formal ou material entre a previsão legal do artigo 2.º, n.º 1, alínea a), da Lei n.º 32/2008 e o catálogo de crimes delineado no artigo 187.º, n.º 1 e 189.º, do CPP – com a "virtual" excepção da alínea b) do n.º 1 do artigo 187.º –, não há revogação do segundo pelo primeiro dos dois regimes.

XV – Se assim é, não se tem de aplicar, por repristinação, nenhuma norma do CPP.

XVI – "Caída" a Lei 32/2008, e na impossibilidade de aplicação do CPP e da Lei 41/2004, recorrer, na questão da localização celular, às normas da Lei 109/2009 seria seguir um caminho espúrio, face à enunciada declaração de inconstitucionalidade e aos fundamentos que a determinaram.

XVII – O que significa que no caso específico de obtenção por localização celular conservada, isto é, a obtenção dos dados previstos no artigo 4.º, n.º 1, da Lei 32/2008, o regime processual aplicável assume especialidade nos artigos 3.º e 9.º deste diploma (para estes casos ganhando relevo o conceito de «crime grave», já que nos termos do artigo 3.º, n.º 1, ainda do mesmo compêndio legislativo, a obtenção de prova da localização celular conservada só é prevista para crimes que caibam nesse conceito) - desaparecendo a especialidade, não é consentido recorrer à generalidade e permitir localização celular para além desses crimes é defraudar o espírito do legislador.

XVIII – A facturação detalhada, integrando também dados de tráfego relativos às comunicações efectuadas – pelo menos, informações atinentes a todas as chamadas realizadas num determinado período, números de telefone chamados, data da chamada, hora de início e duração de cada comunicação –, inviabiliza a aplicação da norma do artigo 14.º, n.º 4, da Lei 109/2009, não sendo também de aplicar o preceito contido no artigo 18.º, apenas destinado a intercepções em tempo real, a exemplo das normas do CPP para que remete, anotando-se ainda que, no caso dos autos, o prazo de três meses, previsto no artigo 12.º, n.º 3, já se extinguiu.»

Acórdão de 04 de fevereiro de 2015 (Processo n.º 73/14.9JALRA-A.C1)
Cibercrime – Dados de base – Dados de conteúdo

«I - Quando os elementos pretendidos, funcionalmente constituem já elementos inerentes à própria comunicação, na medida em que permitem identificar, em tempo real ou à posterior, os utilizadores, o relacionamento directo entre uns e outros através da rede, a localização, a frequência, a data, hora, e a duração da comunicação, devem participar das garantias a que está submetida a utilização do serviço, especialmente tudo quanto respeite ao sigilo das comunicações.

II - Desde que os dados de base estejam em interligação com dados de tráfego ou dados de conteúdo, torna-se necessária a autorização do Juiz para a sua obtenção e junção aos autos.»

Acórdão de 03 de outubro de 2012 (Processo n.º 84/11.6JAGRD-A.C1)
Telecomunicações – Segredo de telecomunicações – Cibercrime – crime de falsidade informática – Dados de tráfego – identificação de IP – Juiz de instrução

«Por força da lei do Cibercrime é legalmente admissível o recurso à interceção de comunicações em processos relativos a crimes previstos na referida lei, aí se incluindo o tipo legal de falsidade informática;

A informação relativa à identificação de determinado IP que realizou uma concreta comunicação em certo grupo data/hora, respeita a dados de tráfego;

Assim a obtenção e junção aos autos de tais dados e a sua validade enquanto meio de prova está dependente da intervenção e autorização do Juiz de Instrução.»

JURISPRUDÊNCIA DO TRIBUNAL DA RELAÇÃO DE ÉVORA

Acórdão de 08 de outubro de 2019 (Processo n.º 180/19.1GHSTC.E1)
Comunicações telefónicas – Crime informático – Prova - Cibercrime – Prova eletrónica – Furto qualificado

«i) a conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves.

ii) entendendo-se por dados, os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador.

iii) e por crime grave, crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima.

iv) o crime de furto qualificado não se integra no conceito de crime grave, a que se reporta a al.ª g), do n.º 1, art.º 2.º, da Lei n.º 32/2008, de 17 de julho.

v) o regime processual das comunicações telefónicas previsto nos artigos 187.º a 190.º do Código de Processo Penal deixou de ser aplicável por extensão às "telecomunicações eletrónicas", "crimes informáticos" e "recolha de prova eletrónica (informática) " desde a entrada em vigor da Lei n.º 109/2009, de 15.09 (Lei do Cibercrime), como regime regra.

vi) esse mesmo regime processual das comunicações telefónicas deixou de ser aplicável à recolha de prova por "localização celular conservada" - uma forma de "recolha de prova electrónica" - desde a entrada em vigor da Lei n.º 32/2008, de 17.07.»

Acórdão de 20 de janeiro de 2015 (Processo n.º 648/14.6GCFAR-A.E1)
Crime informático – Cibercrime – Prova eletrónica

«O regime processual das comunicações telefónicas previsto nos artigos 187.º a 190.º do Código de Processo Penal deixou de ser aplicável por extensão às "telecomunicações eletrónicas", "crimes informáticos" e "recolha de prova eletrónica (informática)" desde a entrada em vigor da Lei n.º 109/2009, de 15-09 (Lei do Cibercrime) como regime regra.

Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável à recolha de prova por "localização celular conservada" – uma forma de "recolha de prova eletrónica – desde a entrada em vigor da Lei n.º 32/2008, de 17-07.

Para a prova eletrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11.º a 19.º da Lei n.º 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei n.º 32/2008, neste caso se estivermos face à prova por "localização celular conservada".

Nessa Lei do Cibercrime coexistem dois regimes processuais: o regime dos artigos 11.º a 17.º e o regime dos artigos 18.º e 19.º do mesmo diploma. O regime processual dos artigos 11.º a 17.º surge como o regime processual "geral" do cibercrime e da prova eletrónica. Isto porquanto existe um segundo catálogo na Lei n.º 109/2009, o do artigo 18.º, n.º 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. Só a este segundo regime – o dos artigos 18º e 19º - são aplicáveis por remissão expressa os artigos 187.º, 188.º e 190.º do C.P.P. e sob condição de não contrariarem e Lei n.º 109/2009.

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

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

Assim, o Capítulo III da Lei n.º 109/2009, relativo às disposições processuais, deve ser encarado como um «escondido Capítulo V ("Da prova eletrónica"), do Título III ("Meios de obtenção de prova") do Livro III ("Da prova") do Código de Processo Penal …» (Dá Mesquita).

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

Em suma, numa interpretação conjugada das Leis n.ºs 32/2008, 109/2009 e da Convenção de Budapeste sobre o Cibercrime do Conselho da Europa (aprovada pela Resolução da Assembleia da República nº 88/2009, publicada no DR de 15-09-2009), devem ter-se em consideração os seguintes catálogos de crimes quanto a dados preservados ou conservados: - o catálogo de crimes do n.º 1 do artigo 11.º da Lei n.º 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11.º a 17.º dessa Lei;
- o catálogo de crimes do n.º 1 do artigo 18.º da Lei n.º 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18.º e no 19.º dessa Lei aos crimes previstos na al. a) do artigo 18.º;
- o catálogo de crimes do n.º 1 do artigo 187.º do Código de Processo Penal, por remissão expressa da Lei n.º 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18.º e no 19.º dessa Lei para os crimes previstos na al. b) do artigo 18.º;
- o catálogo de crimes ("crimes graves") do artigo 3.º da Lei n.º 32/2008 quanto a especiais "dados conservados" (localização celular), como requisito de aplicação dos artigos 3.º e 9.º da Lei n.º 32/2008.

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

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

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

Consequentemente devemos concluir que o regime processual da Lei n.º 32/2008, designadamente o artigo 3.º, n.º 1 e 2 e o artigo 9.º:
- mostra-se revogado e substituído pelo regime processual contido na Lei n.º 109/2009 para todos os dados que não estejam especificamente previstos no artigo 4.º, n.º 1 da Lei n.º 32/2008 ou seja, dados conservados em geral;
- revela-se vigente para todos os dados que estejam especificamente previstos no artigo 4.º, n.º 1 da Lei n.º 32/2008, isto é, para os dados conservados relativos à localização celular. Só para este último caso ganha relevo o conceito de "crime grave".

Antes da entrada em vigor das Leis n.ºs 32/2008 e 109/2009 podia afirmar-se que havia duas formas úteis – processualmente úteis – de usar a localização celular. Uma delas a medida cautelar de polícia prevista no artigo 252º-A do C.P.P. e a outra o meio de obtenção de prova previsto no artigo 189.º, n.º 2 do mesmo código, que se mantém em vigor para a localização celular em tempo real.

Agora coexistem três realidades distintas através do acrescento da obtenção de dados de localização celular "conservados" por via da Lei n.º 32/2008.

Os requisitos do número 3 do artigo 9.º da Lei n.º 32/2008 mostram-se de verificação alternativa. O conceito de "suspeito" dele constante exige "determinabilidade" e não "determinação".

A previsão do artigo 252.º-A do Código de Processo Penal é claramente uma previsão de carácter excecional para situações de carácter excecional.»

Acórdão de 6 de Janeiro de 2015 (Processo n.º 6793/11.2TDLSB-A.E1)
Cibercrime – Crime informático – Prova eletrónica

«As Leis nº 32/2008, de 17-07 e 109/2009, de 15-09 (Lei do Cibercrime) revogaram a extensão do regime das escutas telefónicas, previsto nos artigos 187º a 190º do Código de Processo Penal, às áreas das "telecomunicações electrónicas", "crimes informáticos" e "recolha de prova electrónica".

A pretensão do legislador (quer o nacional quer o da Convenção de Budapeste sobre o Cibercrime) é o de alargar o âmbito da aplicação da lei até onde haja necessidade de fazer prova com o conteúdo existente em qualquer "sistema informático".

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

Mas co-existem dois regimes processuais na Lei n. 109/2009: o regime dos artigos 11º a 17º da dita Lei; o regime dos artigos 18º e 19º do mesmo diploma. Podemos, portanto, caracterizar o regime processual especial dos artigos 11º a 17º como o regime processual "geral" do cibercrime e da prova electrónica.

Isto porquanto existe um segundo *catálogo* na Lei n. 109/2009, o do artigo 18º, n. 1 do mesmo diploma a que corresponde um segundo regime processual de autorização e regulação probatória. O artigo 18º, n. 1 da Lei 19/2009, exclui daquele novo sistema "geral" de autorização e acesso probatório relativamente aos crimes (*a*) nela previstos 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, **desde que** (em ambos os casos) **esteja em causa a intercepção de comunicações**.

Nestes casos aplica-se, por remissão do n. 4 do artigo 18º da Lei 109/2009, o regime previsto nos artigos 187º, 188º e 190º do Código de Processo Penal, no que constitui uma remissão expressa que substitui o regime de extensão previsto no artigo 189º do Código de Processo Penal

O elemento distintivo entre os regimes processuais contidos nos artigos 11º a 17º da Lei n. 109/2009 e o regime previsto no artigo 18º da mesma é, portanto, o conceito de "intercepção em tempo real de comunicações", sendo que esta intercepção pode abranger os dados de tráfego e de conteúdo.

Destarte, só após esta constatação – a de que a diferenciação de regimes se faz pela natureza actualista, em tempo real, da intervenção – é realizável fazer apelo às características dos dados, assumindo que onde se permite o mais se permite o menos, para concluir que:
a) - no caso do artigo 17º da Lei n. 109/2009 estamos a tratar de dados, armazenados, de tráfego e de conteúdo de correio electrónico;
b) - no caso do artigo 18º falamos de interceptar em tempo real dados de tráfego e de conteúdo;
c) - no caso dos artigos 12º a 16º - e na competência do M.P. - é possível pesquisar e apreender dados armazenados de base e de tráfego (v. g. artigo 1º, nº 2 da Lei n. 32/2008, não revogado pela Lei n. 109/2009).

Nos dois primeiros casos é necessária a intervenção de Juiz, no terceiro da entidade judiciária que presidir à fase processual. Neste último caso será sempre necessária a intervenção judicial se forem encontrados dados a inserir na previsão do artigo 16º, ns. 3 e 6 da referida Lei.

Face à Lei nº 109/2009 devem ter-se em consideração três catálogos de crimes:
a - o catálogo de crimes do n. 1 do artigo 11º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nos artigos 11º a 17º dessa Lei;
b - o catálogo de crimes do n. 1 do artigo 18º da Lei 109/2009 como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei;

c - o catálogo de crimes do n. 1 do artigo 187º do Código de Processo Penal, por remissão expressa da Lei 109/2009, como pressuposto de aplicação do regime processual contido nesse artigo 18º e no 19º dessa Lei para os crimes previstos na al. b) do artigo 18º.

O catálogo de crimes mais restritivo do artigo 187º do Código de Processo Penal apenas é aplicável havendo "intercepção de comunicações" e apenas nos casos dos crimes previstos na al. b) do artigo 18º.

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

JURISPRUDÊNCIA DO TRIBUNAL DA RELAÇÃO DE GUIMARÃES

Acórdão de 23 de janeiro de 2024 (Processo n.º 743/23.0JAVRL-A.G1)
Metadados – Dados de base – Dados de tráfego – Dados de conteúdo – Dados de localização celular

«Os dados da faturação detalhada e os dados da localização celular que fornecem a posição geográfica do equipamento móvel com base em atos de comunicação, na medida em que são tratados para permitir a transmissão das comunicações, são dados de tráfego respeitantes às telecomunicações e, portanto, encontram-se abrangidos pela proteção constitucional conferida ao sigilo das telecomunicações.

Tem sido entendimento maioritário que, tratando-se de dados de comunicações "conservadas" ou "preservadas", não é possível aplicar o disposto no artigo 189º do Código de Processo Penal – a extensão do regime das escutas telefónicas – aos casos em que são aplicáveis as Leis n.ºs 32/2008 e 109/2009. Isto é, para a prova de comunicações preservadas ou conservadas em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, com as especificidades supra assinaladas, coadjuvado pelos artigos 3º a 11º da Lei nº 32/2008, se for caso de dados previstos nesta última.

O acórdão do Tribunal Constitucional n.º 268/22, de 19-04, veio declarar a inconstitucionalidade, com força obrigatória geral, de várias normativos da Lei n.º 32/2008, mais concretamente: da norma constante do artigo 4.º da Lei n.º 32/2008, de 17 de julho, conjugada com o artigo 6.º da mesma lei, por violação do disposto nos n.ºs 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo n.º 18.º, todos da Constituição; e da orma do artigo 9.º da Lei n.º 32/2008, de 17 de julho, relativa à transmissão de dados armazenados às autoridades competentes para investigação, deteção e repressão de crimes graves, na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros, por violação do disposto no n.º 1 do artigo 35.º e do n.º 1 do artigo 20.º, em conjugação com o n.º 2 do artigo 18.º, todos da Constituição.

Em causa está a transmissão, por operadoras de serviços de telecomunicações, de dados conservados de tráfego e de localização celular emergentes da detenção e/ou utilização de aparelhos telefónicos, que, segundo o entendimento que sufragamos, é regulada e disciplinada especificamente pela Lei n.º 32/2008. Contudo, nos presentes autos investigam-se factos suscetíveis de integrar a prática de um crime de incêndio, previsto e punível pelo artigo 274º, n.º 1, do Código Penal, com pena de prisão de 1 a 8 anos. Ora, tal crime que não integra o catálogo de crimes que preenchem a definição de «crime grave» contemplada no artigo 2º, n.º 1, al. g), da Lei n.º 32/2008, complementada pelo esclarecimento constante do artigo 1º, alíneas i), j) e m) do Código Penal quanto ao que deve entender-se por «terrorismo», «criminalidade violenta» e «criminalidade altamente organizada».

Com efeito, a obtenção de prova de localização celular conservada apenas pode ser admitida quando está em causa *crime grave* de acordo com a apontada restrita definição, sendo este pressuposto essencial de aplicação da Lei n.º 32/2008.

Como tal, mostra-se inexoravelmente arredada a aplicabilidade da Lei n.º 32/2008 e prejudicada a apreciação dos restantes pressupostos de que depende – nomeadamente a qualidade [processual] da

pessoa a que se referem os dados cuja transmissão é pretendida, conforme exige o n.º 3 do artigo 9º [designadamente, o suspeito, previsto na al. a)] e, bem assim, a questão dos efeitos decorrentes da declaração de inconstitucionalidade de alguns dos seus dipositivos nos sobreditos termos.

De igual modo é de excluir a aplicabilidade do regime de extensão previsto nos artigos 189º, n.º 2, e 187º do Código de Processo Penal, porquanto é pedida a obtenção de dados passados conservados, e não de dados futuros ou em tempo real, circunstância que, só por si, perfilhando-se o entendimento *supra* explanado, a afasta de modo incontornável.

Ainda que assim se não entendesse, pese embora esteja em causa crime incluído no catálogo de crimes elencados no artigo 187º, n.º 1 [mais concretamente, previsto na alínea a) – crimes puníveis com pena de prisão superior, no seu máximo, a 3 anos], já o mesmo não se verificava quanto ao catálogo de visados discriminados no n.º 4 do mesmo preceito, mormente pessoa com a qualidade processual de *suspeito* ou *arguido* [al. a)].

Com efeito, no inquérito ainda nem sequer há suspeitos. O artigo 1º, al. e), do Código de Processo Penal define «suspeito» como sendo *"toda a pessoa relativamente à qual exista indício de que cometeu ou se prepara para cometer um crime, ou que nele participou ou se prepara para participar"*. Ora, como assertivamente se sustentou na decisão alvo de recurso, tem sido amplamente defendido pela jurisprudência dos Tribunais superiores que se os dados de localização celular que se pretendem obter não têm como alvo um suspeito, mas antes um universo de pessoas não identificadas e unidas apenas pelo simples facto de estarem num dado local num dado momento, não é admissível, pois, além de não respeitar os princípios da proporcionalidade e da adequação, não permitem o enquadramento no conceito jurídico-penal de "suspeito".»

Acórdão de 15 de abril de 2012 (Processo n.º 68/10.1GCBRG.G1)
Transcrição – Mensagens SMS – Autorização Judicial – Juiz – Prova

«Da interpretação da norma do artº 189º, nº 1 do CPP, na redação da Lei 48/07 de 29 de Agosto, decorre que a transcrição de mensagens sms existentes no telemóvel de um queixoso pode valer como prova apesar de não ter sido ordenada pelo juiz de instrução.»

Acórdão de 29 de março de 2011 (Processo n.º 735/10.0GAPTL-A.G1)
Telecomunicações – Cibercrime – Cartão de telemóvel – Mensagens SMS

«I - Tendo o Ministério Público determinado a pesquisa de dados informáticos supostamente guardados no telemóvel da denunciante, a apreensão das mensagens (SMS) ali encontradas deve ser autorizada pelo juiz de instrução -artigo 17º da Lei do Cibercrime (Lei n.º 109/2009, de 15/9).

II - A lei não estabelece qualquer distinção entre mensagens por abrir ou já abertas.»

Francisco Marques Vieira
Adriana Silva Soares
André Gil Dias