jurisprudência.pt

Tribunal da Relação de Évora
Processo nº 188/21.7GAVNO.E1

Relator: GOMES DE SOUSA
Sessão: 22 Fevereiro 2022
Votação: UNANIMIDADE

CIBERCRIME **LOCALIZAÇÃO CELULAR** **DADOS DE TRÁFEGO**

Sumário

I. Quer a Lei do Cibercrime (Lei nº 109/2009), quer a Lei de Conservação ou Retenção de Dados (Lei nº 32/2008), são leis especiais no seu campo de ação relativamente ao regime das escutas constantes do Código de Processo Penal.
II. Esta interpretação supõe a conjugação das previsões dos artigos 1º, nº 1, al. g), 3º e 9º da Lei nº 32/2008, enquanto regime de previsão normativa base (crimes graves como finalidade exclusiva da conservação), de competência orgânica (via autorização do Juiz de instrução) e pressupostos de deferimento («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»).
III. Tal interpretação, no aspeto processual, evita os óbvios perigos substantivos de violação da Constituição da República Portuguesa, da Convenção Europeia dos Direitos do Homem e – como bem salientado pelo TJUE – da Carta dos Direitos Fundamentais da União Europeia.
IV. A Lei nº 32/2008, de 17/07, expressamente afirma no seu artigo 1º, nº 1, ser uma transposição da Diretiva nº 2006/24/CE, mas como foi muito claramente declarada inválida pela Grande Secção do Tribunal de Justiça da UE no acórdão de 08-04-2014 nos processos Digital Rights Ireland Ltd (C-293/12) e Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl (C-594/12), deve ser hoje analisada como uma Lei nacional autónoma.
V. O facto de um acto normativo comunitário ter sido declarado inválido não arrasta ipso facto a invalidade de um ato normativo nacional que o pretendia transpor. Nada o afirma em termos normativos no Tratado da União Europeia ou no Tratado sobre o Funcionamento da União Europeia. E não há uma invalidade automática e subsequente do acto legislativo nacional de transposição.

VI. A Diretiva (UE) 2019/713 contém uma dupla perspetiva, a Fraude e a Contrafação. O termo “contrafação” exige uma vertente de “falsificação material” de um instrumento ou meio de pagamento. O termo “fraude” é usado aqui num sentido amplo que inclui modelos de tipos criminais clássicos, como ela própria refere, «formas de conduta clássicas, como fraude, falsificação, furto e apropriação ilícita, que já foram delineadas pelo direito nacional antes da era digital» e «o envio de faturas falsas».
VII. Assim, o termo “fraude” pode incluir qualquer tipo penal clássico que seja praticado com meios digitais, incluindo a burla, crime que aqui está em causa.
VIII. Mas, contrariamente ao que a própria Diretiva sugeriu, o legislador nacional na Lei 79/2021 não seguiu o conselho quanto à “fraude”, limitou-se a seguir o conselho da Diretiva quanto à contrafação, criando vários tipos penais de contrafação que veio a incluir na Lei nº 109/2009, a Lei do Cibercrime, nos artigos 3º-A a 3º-F.
IX. E, depois, viu-se na necessidade de alterar a al. g), do nº 1 do artigo 2º da Lei nº 32/2008 para incluir a expressão «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» apenas para conseguir incluir as novas “contrafações da Lei do Cibercrime e alargar o objeto da “conservação” e o seu prazo.
X. A localização celular constitui violação da privacidade do cidadão. Estamos, pois, a falar de intrusão do Estado na privacidade do cidadão.
XI. E a defesa do cidadão faz-se, habitualmente, pela definição clara de “catálogos de crimes” a que fica sujeita a ação dos operadores de comunicações e do Estado à face dessa legislação, à imagem do que ocorre com o catálogo de crimes do CPP e da Lei do Cibercrime. E, neste particular ponto, entendemos que os artigos 3º e 9º da Lei nº 32/2008 só podem ter o significado que lhe atribuímos, o de um catálogo de crimes limitador da ação do Estado face à privacidade do cidadão.

Texto Integral

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

A - Relatório
Nestes autos de recurso penal provenientes do Tribunal Judicial da Comarca de Santarém Juízo de Instrução Criminal de Santarém - pretende-se que este Tribunal da Relação profira decisão que revogue o despacho da Mmª JIC que

indeferiu o pedido do Ministério Público que «*por se revelar idónea e necessária – senão mesmo indispensável – à obtenção da prova e aos fins do processo, além de proporcional aos indícios existentes, à gravidade do crime de burla informática em investigação e ao avultado valor do prejuízo patrimonial sofrido pelos ofendidos, remeta os autos ao Mmo. Juiz de Instrução, a quem, nos termos e para os efeitos do disposto nos artigos 187.º, n.ºs 1, alínea a) e 4, alínea a), 189.º, n.º 2, e 269.º, n.º 1, alínea e), todos do Código de Processo Penal, o Ministério Público promove que seja solicitado à operadora ALTICE PORTUGAL que, no prazo de 10 dias, forneça a faturação detalhada, registo e listagem de trace back (chamadas efetuadas/recebidas e SMS e MMS enviadas/recebidas), com indicação da respetiva localização celular (antenas/BTS), relativamente ao número de telemóvel xxx.xxx.xxx, desde o início do dia xx-xx-xxxx a xx-xx-xxxx*».

*

Inconformada com aquela decisão, dela interpôs o Digno Magistrado do Ministério Público o presente recurso, com as seguintes conclusões:
1. Nos presentes autos, em que se investiga um crime de burla informática qualificado, previsto e punido pelo artigo 221.º, n.ºs 1 e 5, alínea a) do Código Penal, e um crime de falsidade informática, previsto e punido pelo artigo 3.º, n.ºs 1 e 2 da Lei n.º 109/2009, de 15 de setembro, por ser essencial à descoberta da verdade material, o Ministério Público promoveu a obtenção de dados de localização celular e registos de comunicações, atinentes ao n.º de telemóvel xxx xxx xxx - usado pelo(a) suspeito(a) na fraude-, no período compreendido entre xx e xx-xx-xxxx.
2. A decisão ora recorrida, indeferiu tal promoção, com fundamento na não aplicação in casu do disposto nos artigos 187.º e 189.º do Código de Processo Penal, entendendo que esta última norma foi revogada tacitamente pelo disposto na Lei n.º 32/2008, de 17 de julho, relativas a dados preservados ou conservados, em cujo catálogo de "crimes graves", previsto no artigo 2.º, n.º 1, alínea g) do referido diploma, não se incluíam os aqui investigados.
3. Porém, o entendimento da decisão recorrida traz incoerência ao sistema legislativo existente e conduz, em termos práticos, a soluções absolutamente incongruentes, à luz dos direitos à reserva da intimidade da vida privada, ao sigilo nas comunicações e à proteção de dados pessoais que se pretendem acautelar, uma vez que, por um lado, reserva os meios de obtenção de prova menos restritivos e lesivos dos direitos dos visados a um núcleo limitado de crimes (previsto no artigo 2.º, n.º 1, alínea g) da Lei n.º 32/2008, de 17 de julho) , mas por outro lado, permite a aplicação dos meios de obtenção de prova ocultos e mais intrusivos a um catálogo "mais abrangente" de crimes, ao

abrigo do artigo 187.º, n.º 1 do Código de Processo Penal (Por exemplo, no caso dos nossos autos, permite, em abstrato, que os suspeitos sejam escutados e localizados, diariamente, em tempo real, para investigar a prática de factos similares, mas não admite o pedido que foi feito por nós nos autos).
4. Além disso, o entendimento sufragado pela decisão recorrida olvida as regras gerais sobre interpretação e revogação de leis, nomeadamente de que não pode haver revogação tácita quando há compatibilidade entre as novas disposições da Lei 32/2008 e as regras precedentes previstas no Código de Processo Penal,
5. Com efeito, foi sempre intenção legislador que as normas gerais do Código de Processo Penal concorressem com as previstas na referida Lei 32/2008, conforme vertido no artigo 1.º n.º 2 deste último diploma (…) - "sem prejuízo do disposto na Lei n.º 41/2004, de 18 de Agosto, e na legislação processual penal relativamente à interceção e gravação de comunicações".
6. Neste sentido, a infeliz dispersão de leis existentes reclama uma interpretação e uma aplicação, uniforme, que permita a concordância prática dos interesses em conflito e, simultaneamente, atribua alguma harmonia e coerência a todo o sistema, o que o Tribunal a Quo não se esforçou minimamente em fazer
7. Assim, a Lei n.º 32/2008, de 17 de julho - que transpôs para o direito interno a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março - é de aplicação muito específica, destinando-se, apenas, à conservação e transmissão de dados gerados ou tratados para efeitos de deteção e repressão de "crimes graves", tendo fixado um novo prazo o- de um ano, a contar do terminus comunicação- para que as operadoras conservem os dados de tráfego.
8. Ou seja, a Lei n.º 32/2008 não revogou o regime geral do artigo 6 n.º 3 da Lei 41/2004 e do 189.º, n.º 2 do Código de Processo Penal, que sempre estabeleceu um prazo reduzido de seis meses (cf. artigos 1.º, n.º 2, alínea d) e 10.º, n.º 1 da Lei n.º 23/96) para preservação e transmissão de dados conservados de tráfego, relativamente aos crimes (graves ou não) previstos no catálogo do artigo 187.º, n.º 1 do Código de Processo Penal,
9. Assim, a Lei 32/2008 prevê um regime especial, que estabelece um prazo alargado de um ano para conservação e transmissão de dados, precisamente porque apenas é aplicável a um catálogo restrito de crimes graves, previsto no artigo 2.º, n.º 1, al g) da Lei n.º 32/2008.
10. De igual modo, a Lei n.º 109/2009, Lei do Cibercrime, que transpôs para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, e adaptou o direito interno à Convenção sobre Cibercrime do Conselho da Europa, não se prevê nenhuma norma de teor coincidente com o

do artigo 189.º, n.º 2 do Código de Processo Penal, motivo pelo qual também não operou qualquer revogação tácita, relativamente a este específico propósito.
11. Assim sendo, quanto aos dados de tráfego conservados, onde se inclui a localização celular, temos dois regimes perfeitamente compatíveis:
a. um regime geral, decorrente do disposto nos artigos 6 n.º 3 da Lei 41/2004 e 189.º, n.º 2 do Código de Processo, que permite a obtenção dos referidos dados desde que o pedido tenha menos de 6 meses após a realização das comunicações, seja emitido por despacho fundamentado do Juiz, quanto ao catálogo de crimes e segundo as formalidades dos regimes das escutas, nos termos do disposto no artigo 187 e 189 do CPP; e
b. um regime especial, para os dados conservados com mais de 6 meses, até ao máximo de um ano, em que tais pedidos só são admissíveis para a investigação dos crimes graves previstos no catálogo mais restritivo, do artigo 2.º, n.º 1, alínea g) e em relação às pessoas referida no artigo 9.º, n.º 3, da Lei 32/2008, também por despacho fundamentado do juiz de instrução – [É este entendimento que tem vindo a ser seguido, na prática pelos departamentos jurídicos das operadoras, que só exigem despacho judicial com alusão à Lei 32/2008 relativamente a pedidos referentes a dados de tráfego conservados há mais de 6 meses (somos ponto de contacto do gabinete do Cibercrime, da PGR para área norte da Comarca de Santarém)].
12. Nestes termos tratando-se, in casu, de dados conservados ainda dentro do prazo de 6 meses, estando verificados os pressupostos constantes dos artigos 189.º, n.º 2 e 187.º, n.ºs 1, alínea a) e 4 do Código de Processo Penal e revelando-se este meio não só necessário à prova e aos fins do processo, mas também proporcional à gravidade dos crimes e ao avultado prejuízo patrimonial sofrido pelos ofendidos, impõe-se concluir estarem preenchidos todos os pressupostos para que seja deferida a promoção do Ministério Público (não caindo a presente situação no âmbito de aplicação do regime especial da Lei 32/2008) – [No mesmo sentido ao aqui defendido, vide o recentíssimo Ac. do TRG de 5-7-2021, relatado por Teresa Coimbra e ainda, que sem se referir expressamente à aplicação da Lei 32/2008, o também recente Ac. Do TRE de 25-5-2021, relatado por Martinho Cardoso, que deferiu pedido similar à promoção destes autos, ambos disponíveis em www.dgsi.pt].
13. Por todo o exposto, a decisão recorrida violou, assim, o disposto nos artigos 187.º, n.ºs 1, alínea a) e 4, alínea a), 189.º, n.º 2, e 269.º, n.º 1, alínea e), todos do Código de Processo Penal, e ainda o disposto no artigo 1.º da Lei 32/2008, 7.º e 9.º do Código Civil e 6.º da Lei 41/2004, devendo, como tal, ser substituída por outra que defira a promoção do Ministério Público.
Nestes termos e nos mais de Direito aplicáveis, deve o presente recurso

merecer provimento e, em consequência, ser revogada a decisão recorrida, na parte em que indeferiu a promoção de obtenção dados de localização celular e registos da realização de conversações, sendo substituída por outra que defira a promoção do Ministério Público de xx-x-xxxx, ordenando que se solicite à operadora ALTICE PORTUGAL que, no prazo de 10 dias, forneça a faturação detalhada, registo e listagem de trace back (chamadas efetuadas/recebidas e SMS e MMS enviadas/recebidas), com indicação da respetiva localização celular (antenas/BTS), relativamente ao número de telemóvel xxx.xxx.xxx, desde o início do dia xx-x-xxxx a xx-xx-xxxx, assim fazendo V. Exas. a costumada Justiça.

*

Nesta Relação o Exmº Procurador-geral Adjunto emitiu douto parecer no sentido da procedência do recurso.

*

B.1 - Fundamentação

É o seguinte o teor do despacho recorrido:

«Indiciam os autos que o saldo da conta bancária com o IBAN PT50 xxxxxxxx, em valor não apurado, sediada no Banco X tenha sido utilizada como destino de transferências realizadas por suspeito não apurado, induzindo o aqui denunciante e ofendido Pi..., em erro, levando-o a realizar um conjunto de procedimentos, mediante a utilização de MBway e assim tendo tal pessoa acesso a contas bancárias do mesmo e familiares, causando-lhe prejuízo patrimonial global no valor de 10 400 euros (fls. 30).

Indicia-se, assim, que o saldo de tal conta bancária constitui produto de ilícitos criminais, investigando-se nos autos a prática de crimes de falsidade informática e burla informática (fls. 40, 41 e 42).

Importa, assim, apreender, tal valor, como garantia de que a tal produto de ilícito criminal será dado o oportuno destino.

Nesta medida, entende o Tribunal que tal apreensão terá que realizar-se ao abrigo do Artigo 178º, nº 1 do CPP, mas não ao abrigo do Artigo 181º, nº 1 do mesmo diploma legal que está pensado para apreensões materiais, in loco, em diligência presidida pelo JIC.

Não obstante, podendo haver entendimentos em sentido contrário, o Tribunal determina tal apreensão, apesar de, nos termos do Artigo 178º do CPP, a mesma puder ser realizada por autoridade judiciária, o que abrange o M.P.

DECISÃO:

Assim, ao abrigo do Artigo 178º, nº 1 do CPP, determino a apreensão do saldo da conta bancária sediada no Banco X, a que corresponde o IBAN PT50 xxxxxxxxxx, até ao valor de 4 100 euros (quatro mil e cem euros).

Notifique e DN.

*
Indiciam os autos que suspeito não apurado utilizou para a prática dos factos ilícitos supra referenciados, que aqui se dão por reproduzidos, o numero de telefone xxx.xxx.xxx .
O M.P. requer o envio de facturação detalhada, registo de trace-back e localização celular atinente a tal numero de telefone no período compreendido entre xx a xx de Junho de xxxx.
Ora, se assim é, a nosso ver, não é aplicável o disposto nos Artigos 187º e segs. do C.P.P., que têm como âmbito de aplicação a interceção de comunicações telefónicas ou diversas (189º), entre presentes ou em tempo real, mas antes as normas relativas a dados preservados ou conservados, insertos em suporte eletrónico (tudo sublinhados nossos)
Neste âmbito há que atentar na Lei nº 32/2008 de 17/07 e na Lei 109/2009 de 15/09 (Lei do Cibercrime).
Sendo ambos os diplomas de aplicação coincidente a uma mesma situação fáctica, há que distinguir em que situações se aplica um ou outro, consabido que os requisitos e pressupostos da sua aplicação são distintos, mormente por referência ao catálogo de crimes que permitem essa aplicação (artigo 11º da Lei do Cibercrime e Artigo 1º e 2º, nº 1, al. g) da Lei nº 32/2008 de 17/07, quanto ao conceito de crimes graves).
Assim, sem prejuízo de se conhecerem posições jurídicas diversas, tem alguma jurisprudência entendido que se a informação a obter se reportar ao Artigo 4º da Lei do Cibercrime, quanto a tais dados, não se encontrando revogada a Lei nº 32/2008 de 17/07 (por ressalvada a sua aplicação pela Lei do Cibercrime e por um diploma ter caracter geral e outro especial, não tendo derrogado lei posterior lei anterior), aplica-se esta (Lei nº 32/2008 de 17/07) e, logo o conceito de crimes graves que constitui o catálogo de crimes que permite a aplicação de tal diploma legal (Ac do TRE de 20/01/2015, entre outros).
Ora, no âmbito de tal catálogo de crimes não avultam os crimes aqui em apreço, sendo que os mesmos não integram o conceito de criminalidade violenta ou altamente organizada, dado o teor do Artigo 1º do CPP ou os mencionados, na al. g) do nº 1 do Artigo 2º de tal normativo legal.
Desta maneira, não consideramos que ocorra fundamento legal para se deferir o requerido, quanto a dados de tráfego e localização celular, sendo que os ilícitos aqui em causa são puníveis com pena de prisão até 5 anos ou multa (falsidade informática) e pena de prisão até 5 anos ou multa (burla informática e nas comunicações, agravada pelo valor elevado).
DECISÃO:
Termos em que, face ao exposto, se indefere, por falta de fundamento legal, o requerido quanto a dados de tráfego e localização, relativos ao numero de

telefone xxx.xxx.xxx.
Notifique e DN.
Devolvam-se os autos aos serviços do M.P..
*

Cumpre conhecer.

B.2 – Os dados e o Código de Processo Penal.

Uma é, formalmente, a questão suscitada pelo recurso, a aplicabilidade dos artigos 189º, nº 2 e 187º, nº 1 do C.P.P. ao caso dos autos.
Sobre a matéria do presente recurso já emitimos relatos em vários processos desta Relação, designadamente nos acórdãos de 20-01-2015 e 25-10-2016.
Tais decisões vieram a ter os seguintes sumários:

- TRE de 20-01-2015 (processo 648/14.6GCFAR-A.E1):
«1 - O regime processual das comunicações telefónicas previsto nos artigos 187º a 190º do Código de Processo Penal deixou de ser aplicável por extensão às "telecomunicações electrónicas", "crimes informáticos" e "recolha de prova electrónica (informática)" desde a entrada em vigor da Lei 109/2009, de 15-09 (Lei do Cibercrime) como regime regra.
2 - Esse mesmo regime processual das comunicações telefónicas deixara de ser aplicável à recolha de prova por "localização celular conservada" – uma forma de "recolha de prova electrónica – desde a entrada em vigor da Lei 32/2008, de 17-07.
3 - Para a prova electrónica preservada ou conservada em sistemas informáticos existe um novo sistema processual penal, o previsto nos artigos 11º a 19º da Lei 109/2009, de 15-09, Lei do Cibercrime, coadjuvado pela Lei nº 32/2008, neste caso se estivermos face à prova por "localização celular conservada".
4 - …»

- TRE de 25-10-2016 (processo 223/16.0GBLLE.E1):
1 - No caso de investigação e repressão de infrações penais relativas a "comunicações, dados de comunicações e sua conservação" existe legislação especial que secundariza o Código de Processo Penal e torna quase irrelevantes as Leis nº 5/2004 e 41/2004 para efeitos processuais penais.
2 - Tal legislação especial são as Leis nº 32/2008, de 17-07 (Lei 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) e 109/2009, de 15-09 (Lei do Cibercrime), assim como a Convenção do Conselho da Europa sobre o Cibercrime de 23/11/2001 (Resolução da AR n.º 88/2009, de 15 de Setembro), também designada

Convenção de Budapeste.
3 – Tratando-se de dados de comunicações "conservadas" ou "preservadas" já 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 nº 32/2008 e 109/2009 e a Convenção de Budapeste. 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, coadjuvado pelos artigos 3º a 11º da Lei nº 32/2008, se for caso de dados previstos nesta última;
4 - A Lei nº 32/2008 tem um regime processual "privativo" da matéria por si regulada, assente na existência de "dados conservados" nos termos do artigo 4.º, nº 1 pelos fornecedores de serviços.

Desculpar-nos-á o Digno Magistrado recorrente mas iremos limitar a nossa fundamentação por remissão ao que já consta desses acórdãos por se não justificar repetir aqui o ali dito. O que não impede - até se impõe por respeito ao recorrente - uma revisão em dois passos, um o das recentes alterações legislativas sobre a matéria, outro a análise da argumentação expendida no recurso, com o fito de apurar se algo deve ser revisto.
Sempre com a noção, já adquirida na altura dos ditos relatos, que a matéria é complexa e a interpretação sistemática sobre o objecto do recurso, sendo difícil, não foi facilitada pelo legislador nacional.
Uma aproximação à leitura realizada pelo Digno recorrente impõe-nos que recordemos o que já afirmámos a propósito do regime processual penal das escutas telefónicas e sua extensão a outros domínios.
O regime processual penal das escutas telefónicas contido nos artigos 187º a 189º do Código de Processo Penal continha, desde início, uma norma de extensão do regime – então no artigo 190º - a uma realidade diversa mas próxima do regime das comunicações telefónicas clássicas, a das "*conversações e comunicações transmitidas por qualquer meio técnico diferente do telefone*".
Esta norma de extensão vem posteriormente – com as alterações introduzidas pela Lei n.º 48/2007, de 29/08 – a sedear-se no artigo 189º (passando a nulidade do artigo 189º para o artigo 190º do diploma), já com um considerável alargamento das realidades ali previstas.
Nesta evolução – que apenas nos interessa na vertente "interpretação histórica" – é essencial notar que a revisão do Código de Processo Penal de 2007 encarou os crimes e a prova de crimes informáticos com uma superficial alteração da regra remissiva no nº 2 do artigo 189º do diploma (anterior artigo 190º), sendo a evolução do recurso legislativo ao regime de extensão

bastante significativo, para além de revelador de um aproveitamento levado ao extremo do regime das escutas telefónicas, como segue:

Artigo 190.º
(Extensão)
O disposto nos artigos 187.º, 188.º e 189.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone (Redacção dada pelo Decreto-Lei n.º 78/87, de 17 de Fevereiro);
Artigo 190.º
(Extensão)
*O disposto nos artigos 187.º, 188.º e 189.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, bem como à intercepção das comunicações entre presentes (*Redacção dada pela Lei n.º 59/98, de 25 de Agosto);
Artigo 189.º
(Extensão)
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 intercepção 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 (actual redacção, dada pela Lei n.º 48/2007, de 29/08).

Como já afirmámos, o regime processual penal das escutas telefónicas contido nos artigos 187º a 189º do Código de Processo Penal está delimitado pela previsão do nº 1 daquele primeiro artigo que determina que o seu objecto é "*a intercepção e a gravação de conversações ou comunicações telefónicas*", entendidas estas como estando a ocorrer, ou seja, *a intercepção e a gravação de conversações ou comunicações telefónicas* em tempo real. Dito de outra forma, intercepção e gravação de dados de conteúdo de conversações e comunicações telefónicas em tempo real.
Destarte, tudo o que era *conversação* ou *comunicação* e tudo o que lhe é conexo, seja a fonte telefónica ou informática, passou a caber no âmbito de

previsão dos artigos 187º a 189º do Código de Processo Penal, mesmo que efectuadas sem intermediação tecnológica, como ocorre com a conversação entre *presentes*. E abarcou, igualmente, dados informáticos, que se "conservaram" resultantes de *conversações e comunicações*.
Esta considerável extensão veio a tornar o regime das escutas telefónicas o regime subsidiário de realidades para as quais não foi pensado até que o choque com uma nova realidade se vem a concretizar com a vigência das Leis n. 32/2008, de 17-07 (Lei de Retenção ou Conservação de Dados) e 109/2009, de 15-09 (Lei do Cibercrime), ambas posteriores à vigência das alterações de 2007 ao C.P.P.
E a questão essencial em termos de apreciação normativa global consiste em apurar se a realidade processual "*regime das comunicações telefónicas*" contido naqueles preceitos do processo penal é compatível com um regime especial e posterior de crimes – não relativos a comunicações telefónicas – sim relativos a comunicações que não usam o telefone, à informática e aos dados "conservados" daí resultantes, por este regime já dispor de legislação específica que afaste aquele regime do C.P.P..
A que acresce, no caso em apreciação, **o saber se os ficheiros resultantes de "conservação" de dados de comunicações telefónicas efectuadas no passado relativas à localização celular e armazenadas para efeitos processuais penais, se continuam a inserir no regime do artigo 189º, nº 2 do C.P.P. ou se no novel regime, designadamente na Lei nº 32/2008, de 17-07**.
O legislador processual penal de 2007 já tinha um acervo generoso de diplomas relativos ao Cibercrime a atender na revisão do C.P.P., tendo optado por um modesto e inadequado alargamento do regime de extensão das escutas telefónicas ao invés de procurar solução processual mais adequada e directa, por previsão no código de processo penal.
Esta opção minimalista do legislador – a de colocar no regime de extensão a regulação processual de matérias distintas – foi largamente criticada pela doutrina, por recusar um tratamento processual consistente do processo necessário às novas realidades das telecomunicações e da informática.[1]
E era este regime processual aplicável a toda a criminalidade informática que se entendia necessário existir pois que, apesar da subsistência de outros diplomas, estes limitavam o seu normativo ao direito substantivo, como a Lei da Criminalidade Informática, Lei nº 109/91, que se bastava com a previsão dos crimes informáticos e na estatuição de penas acessórias ou a Lei 41/2004, de 18-08, que se limitava a estabelecer a privacidade no sector das comunicações electrónicas, ambas sem qualquer norma processual penal com

relevo sistemático completo.
Isto apesar de Portugal ter já assinado, em 23-11-2001, a Convenção de Budapeste [2] sobre o Cibercrime que já dispunha de um completo regime processual penal que se impunha transpor para o direito interno. [3]
Só em 15 de Setembro de 2009 – quase oito anos depois e só após a revisão do C.P.P. – esta Convenção será aprovada pela Resolução da Assembleia da República nº 88/2009, ratificada pelo Decreto presidencial nº 91/2009 e publicada naquela data, no mesmo Diário da República que igualmente acolheu a publicação da Lei 109/2009 que, precisamente, "*aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa*".
Ora, aprovada esta Lei, o espanto estava no desprezo da praxis sobre a sua existência, que apenas é explicável pelo efeito de atracção, quase hipnótico e excludente, que é exercido sobre o intérprete pelos artigos 187º a 190º do C.P.P.
É que nessa altura, como hoje ao que parece, o intérprete esqueceu-se do brocardo latino que espelha bem uma norma de interpretação legal – normas de interpretação a que o recorrente faz apelo – que se concretiza no *Lex specialis derogat legi generali*.
Ambos os regimes posteriores ao Código de Processo Penal na versão de 2007, a Lei do Cibercrime e a Lei de Conservação de Dados, são leis especiais no seu campo de acção relativamente ao regime das escutas constantes do Código de Processo Penal.
Logo, o regime de extensão das escutas telefónicas ao campo de acção dessas duas novas leis está revogado pois que um novo regime preenche o campo de previsão da lei anterior.
É claro que este regime é incómodo para o Ministério Público, mas este, como é evidente, é "parte" no processo e não deve poder escolher o regime que melhor se adeque, no seu entendimento, aos seus interesses acusatórios.
Assim, este recurso é o comprovante de que a extensão do regime processual das escutas telefónicas clássicas é mais favorável à investigação policial e à instrução dos autos pelo Ministério Público, daí não decorrendo que ele deva ser aplicado, não só pelas razões já indicadas, em suma que **tal extensão já não se justifica por haver regime próprio especial nas duas indicadas leis**, também com o argumento de que quando o legislador pretende manter o regime anterior a parte da realidade, dá disso claramente nota, como ocorre com o nº 4 do artigo 18º da Lei nº 109/2009.
Aqui, na Lei do Cibercrime, é clara a expressa previsão de que o regime das

escutas telefónicas já não é aplicável por extensão a este normativo, excepto quando o próprio o prevê, como ocorre com o referido artigo 18º da Lei. É claro também que a previsão completa do novo regime de Conservação de Dados com a vigência da Lei nº 32/2008 revoga *in totum* a extensão do regime das escutas telefónicas por absoluta desnecessidade. Concordar ou não com o novel regime é outra questão.
Argumento *ab absurdum* seria defender que o regime das escutas telefónicas é ainda necessário pois que os Dados Conservados podem conversar entre si. Obviamente que o Digno recorrente não o faz, mas fazemo-lo nós apenas para afirmar que o regime das escutas telefónicas é aqui chamado pois que é mais favorável à investigação policial! É pouco! Esquece o equilíbrio com o direito à privacidade do cidadão. É coisa incómoda isto da privacidade mas, por ora, ainda está na lei.
Essa nossa interpretação, que implica a conjugação das previsões dos artigos 1º, nº 1, al. g), 3º e 9º da Lei nº 32/2008, enquanto regime de previsão normativa base (crimes graves como finalidade exclusiva da conservação), de competência orgânica (via autorização do Juiz de instrução) e pressupostos de deferimento («*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***»), evita a conclusão a que igualmente chega a CNPD nos seus Pareceres.
É, pois, muito claro e explícito o artigo 9º do diploma, esquecido pelo Digno recorrente, ao asseverar que a diligência só potencialmente pode ser deferida se se tratar de «… ***investigação, detecção e repressão de crimes graves***»).
Ora, o caso concreto sequer ultrapassa o primeiro requisito processual, não se trata de crime grave, tal como definido na al. g), do nº 1 do artigo 1º da citada Lei.
A interpretação que nós fazemos da Lei nº 32/2008 no aspecto processual evita os óbvios perigos substantivos de violação da Constituição da República Portuguesa, da Convenção Europeia dos Direitos do Homem e – como bem salientado pelo TJUE – da Carta dos Direitos Fundamentais da União Europeia, através do referido diploma.
Este nosso entendimento mantém-se e não há no recurso razão bastante para o alterar.

*

B.3 – A Lei n.º 79/2021, de 24-11-2021

Quanto ao primeiro passo, confessamos não ver nas redacções dadas pela **Lei n.º 79/2021**, de 24-11-2021 às **Leis n.º 32/2008**, de 17 de julho, que

transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações e **n.º 109/2009**, de 15 de setembro, que aprova a Lei do Cibercrime, qualquer alteração que imponha ou sequer sugira uma diferente aproximação jurisprudencial ao tema que nos obrigasse a um diferente posicionamento.
As alterações introduzidas pela Lei n.º 79/2021, de 24-11-2021 a ambos os diplomas poderiam, de facto, ter sido mais explícitas e modificadoras caso o legislador entendesse que o seu labor estaria a ser contrariado pela jurisprudência que, a nosso ver, surge como maioritária.
Constatamos que a al. g) do nº 1 do artigo 2º da Lei nº 32/2008 - precisamente a que prevê a definição de "crimes graves" - não sofreu alteração que inclua o caso concreto.
De facto entre a inicial redacção e a agora vigente apenas a parte que vai a *bold* foi acrescentada e, claramente, não se aplica ao caso *sub iudicio*. Assim: «*g) 'Crime grave', crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou de títulos equiparados a moeda,* ***contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação*** *e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima*».
Desta forma, a leitura que realizámos anteriormente desta alínea, devidamente enquadrada pelos artigos 3ª, 4º e 9º do diploma, pode manter-se tal como a efectuámos nos acórdãos citados.
É claro que dois entendimentos diversos subjazem na corrente jurisprudência, como é aliás indicado pelo Digno recorrente. Mas, lidos os acórdãos indicados no recurso, não vemos razões para alterar a nossa posição pelas razões que serão indicadas infra.
A CNPD (Comissão Nacional de Protecção de Dados) já se pronunciou sobre esta matéria em dois Pareceres (24/2017 e 74/2021) e uma deliberação (641/2017) recentes cuja leitura é aconselhável, não só pelo acerto da interpretação jurídica, mas também pelo que revela de alertas que já fez ao legislador para que a Lei nº 32/2008 fosse alterada por via da existência de acórdãos do TJUE que muito claramente seguem a via do aresto Digital Rights Ireland Ltd c. Minister for Communications, de 2014. [4]
O parecer de junho de 2021 (parecer 74 de 2021) emitido pela CNPD à AR por

via da Proposta de Lei nº 98/XIV/2ª Gov. que pretendia transpor a Directiva (UE) nº 2019/713 relativa ao «combate à fraude e à contrafação de meios de pagamento que não em numerário» é muito claro quanto à alteração proposta para a Lei nº 32/2008 e que ficou, *ipsis verbis*, a constar da Lei nº 79/2021, de 24 de novembro. Na sua conclusão 47ª do indicado parecer afirma-se:
*47. Quanto à alteração à Lei nº 32/2008, de 7 de julho (Lei da Retenção de Dados), que vem proposta no artigo 4º da Proposta, limitando-se a aditar uma nova conduta às já constantes do conceito de 'crime grave', **mal se compreende que, depois de o TJUE ter declarado inválida a Diretiva que esta lei transpõe e quando está a ser julgada a sua própria constitucionalidade, a alteração legislativa tenha este teor, em vez de corrigir ou suprir as normas em crise.** Entende a CNPD, por isso, **que ao legislador só resta proceder à revisão profunda e meticulosa do regime substantivo e processual da referida lei**. Tal afirma-se como um imperativo resultante da jurisprudência constante do TJUE e condição essencial para superar a atual situação de fragilidade, para dizer o menos, em que a lei se encontra.*
Para completar o quadro normativo já produzido devemos atender, igualmente, aos diplomas comunitários fonte parcial dos diplomas citados, a Directiva 2002/58/CE, a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação e a tão badalada Directiva 2006/24/CE do Parlamento Europeu e do Conselho de 15-03-2006, relativa a obrigações dos fornecedores de serviços de comunicações electrónicas publicamente disponíveis.
O grande argumento que o Digno recorrente poderia utilizar – e nós já expressamente o negámos na nota de rodapé 3 de fls. 8 no nosso relato no acórdão de 20-01-2015, no entanto sem uma análise detalhada sobre o tema comunitário porquanto no processo isso não se justificava – seria **a circunstância de a Lei nº 32/2008, de 17/07, expressamente afirmar no seu artigo 1º, nº 1, ser uma transposição da Directiva nº 2006/24/CE, que foi muito claramente declarada inválida pela Grande Secção do Tribunal de Justiça da UE no acórdão de 08-04-2014 nos processos Digital Rights Ireland Ltd (C-293/12) e Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl (C-594/12)**.
Saber se a validade do legislado no contexto nacional em 2008 não foi afectada por essa decisão é uma interessante questão de aplicação do direito comunitário, expressa na dúvida sobre a validade formal de uma norma nacional de transposição face à invalidade judicialmente declarada da norma comunitária "transposta", considerando o primado do direito comunitário.
Mas negámos essa interpretação ab-rogante da Lei nº 32/2008 apenas devido

à circunstância de se tratar de um diploma nacional que exige interpretação autónoma, independente da leitura e validade dada hoje à Directiva nº 2006/24/CE.
A circunstância de um acto normativo comunitário ter sido declarado inválido não arrasta *ipso facto* a invalidade de um acto normativo nacional que o transpõe. Nada o afirma em termos normativos no Tratado da União Europeia ou no Tratado sobre o Funcionamento da União Europeia. Não há uma invalidade automática e subsequente do acto legislativo nacional de transposição.
Apesar de o acto legislativo nacional ter uma função de transposição legislativa, perde-a face à declarada invalidade do normativo comunitário de 2006 e apresenta uma autonomia assente na réstia de soberania nacional que os Estados membros ainda mantêm, implicando portanto uma análise jurídica autónoma.
Isto é, tratando-se de legislação nacional e não comunitária, a Lei nº 32/2008 deve ser interpretada como lei nacional na análise de cada caso concreto nacional, pelo tribunal nacional, sem prejuízo de eventuais efeitos de direito comunitário derivados da Directiva repristinada, no caso, a Directiva de 2002, que, esses sim, podem ser apreciados pelo TJUE já que este tribunal não pode apreciar a validade de actos legislativos nacionais isoladamente considerados.
O que não pode ocorrer é, como faz o aresto nacional invocado no recurso, interpretar a lei nacional com apoio de acto normativo comunitário declarado inválido pelo TJUE. É uma contradição nos seus próprios termos.
Nós, na nossa posição - que sempre assumiu e assume agora no caso *sub iudicio* um cariz processual - entendemos que a reserva de soberania sempre implicaria um juízo sobre a eventual validade da dita lei nacional de forma expressa por instância nacional que apreciasse substancialmente se os vícios apontados – violação dos artigos 7º, 8º e 11º da Carta dos Direitos Fundamentais da União Europeia – inquinam a dita Lei 32/2008 e a tornam violadora da referida Carta de Direitos.
Ou seja, nunca nos foi necessário emitir um juízo sobre a substância do diploma em causa nos seus aspectos substanciais pois que sempre nos limitámos a emitir juízo sobre a inadmissibilidade processual dos pedidos formulados no processo e no recurso. Designadamente sobre a natureza dos dados conservados e da previsão do diploma quanto aos critérios de guarda e acesso a tais dados.
Isto é, o saber se os dados conservados – ou seja, a letra do artigo 4º da Lei nº 32/2008 – encerram em si, pela sua abrangência, e pelos critérios de guarda e acesso aos dados, a necessidade de um juízo de inconstitucionalidade e/ou de violação da Convenção Europeia dos Direitos do Homem e da Carta.

Essa tem sido sempre, nos casos por nós analisados, uma questão diversa e que aqui não é colocada pelo recurso na medida em que **sendo um aspecto substantivo na análise destes diplomas sobre dados informáticos, é sempre precedido pela análise processual de admissibilidade do pedido e a sua inadmissibilidade, declarada no processo, nos dispensa daquela análise substantiva**.
Para esta leitura substantiva (licitude dos normativos de carácter substantivo) e para demonstrar a natural repristinação da Diretiva 2002/58/C.E. apreciem-se os seguintes dois arestos, de 2020 e 2021, naturalmente posteriores ao aresto *Digital Rights*:
- Acórdão do Tribunal de Justiça (Grande Secção) de 6 de outubro de 2020 - processo C-623/17, **Privacy International contra Secretary of State for Foreign and Commonwealth Affairs,** pedido de decisão prejudicial nos termos do artigo 267.o TFUE, apresentado pelo Investigatory Powers Tribunal (Tribunal de Instrução, Reino Unido):
Descritores - «Reenvio prejudicial — Tratamento de dados pessoais no sector das comunicações eletrónicas — Prestadores de serviços de comunicações eletrónicas — Transmissão generalizada e indiferenciada de dados de tráfego e de dados de localização — Salvaguarda da segurança nacional — Diretiva 2002/58/CE — Âmbito de aplicação — Artigo 1º, nº 3, e artigo 3º — Confidencialidade das comunicações eletrónicas — Proteção — Artigo 5º e artigo 15º nº 1 — Carta dos Direitos Fundamentais da União Europeia — Artigos 7º, 8º, 11º e 52º, nº 1 — Artigo 4º, nº 2, TUE»
Decisão
1) O artigo 1º, nº 3, o artigo 3º e o artigo 15º, nº 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lidos à luz do artigo 4º, nº 2, TUE, devem ser interpretados no sentido de que ***o âmbito de aplicação desta diretiva abrange uma regulamentação nacional que permite a uma autoridade estatal impor aos prestadores de serviços de comunicações eletrónicas a transmissão de dados de tráfego e de dados de localização aos serviços de segurança e de informações para efeitos da salvaguarda da segurança nacional****.*
2) O artigo 15º, nº 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz do artigo 4º, nº 2, TUE e dos artigos 7º, 8º e 11º e 52º, nº 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que ***se opõe a uma regulamentação nacional***

que permite a uma autoridade estatal impor aos prestadores de serviços de comunicações eletrónicas, para efeitos da salvaguarda da segurança nacional, a transmissão generalizada e indiferenciada de dados de tráfego e de dados de localização aos serviços de segurança e de informações.

- Acórdão do Tribunal de Justiça (Grande Secção) de 2 março de 2021 - processo C-746/18, **H. K., contra Prokuratuur**, pedido de decisão prejudicial apresentado, nos termos do artigo 267º TFUE, pelo Riigikohus (Supremo Tribunal, Estónia):
Descritores - «Reenvio prejudicial — Tratamento de dados pessoais no setor das comunicações eletrónicas — Diretiva 2002/58/CE — Prestadores de serviços de comunicações eletrónicas — Confidencialidade das comunicações — Limitações — Artigo 15º, nº 1 — Artigos 7º, 8º, 11º e 52º, nº 1, da Carta dos Direitos Fundamentais da União Europeia — Legislação que prevê a conservação generalizada e indiferenciada dos dados relativos ao tráfego e dos dados de localização pelos prestadores de serviços de comunicações eletrónicas — Acesso das autoridades nacionais aos dados conservados para efeitos de inquéritos — Luta contra a criminalidade em geral — Autorização dada pelo Ministério Público — Utilização dos dados no âmbito do processo penal enquanto elementos de prova — Admissibilidade»
Decisão
1) O artigo 15º , nº 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva Relativa à Privacidade e às Comunicações Eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7º, 8º, 11º e 52º , nº 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que ***se opõe a uma regulamentação nacional que permite o acesso de autoridades públicas a um conjunto de dados de tráfego ou de dados de localização, suscetíveis de fornecer informações sobre as comunicações efetuadas por um utilizador de um meio de comunicação eletrónica ou sobre a localização dos equipamentos terminais por ele utilizados e de permitir tirar conclusões precisas sobre a sua vida privada, para fins de prevenção, de investigação, de deteção e de perseguição de infrações penais, sem que esse acesso esteja circunscrito a processos que visem a luta contra a criminalidade grave ou a prevenção de ameaças graves à segurança pública, independentemente da duração do período em relação ao qual o acesso***

aos referidos dados é solicitado e da quantidade ou da natureza dos dados disponíveis sobre tal período.
2) O artigo 15º , nº 1, da Diretiva 2002/58, conforme alterada pela Diretiva 2009/136, lido à luz dos artigos 7º, 8º, 11º e 52º, nº 1, da Carta dos Direitos Fundamentais, deve ser interpretado no sentido de ***que se opõe a uma regulamentação nacional que atribui competência ao Ministério Público, cuja missão é dirigir a instrução do processo penal e exercer, sendo caso disso, a ação pública num processo posterior, para autorizar o acesso de uma autoridade pública aos dados de tráfego e aos dados de localização para fins de instrução penal.***
Estamos longe destes problemas de cariz substancial da legislação nacional, analisada hoje à luz da Diretiva 2002/58/C.E., ficando este nosso processo à porta da admissibilidade processual e não tendo que analisar o normativo da Lei 32/2008 à luz destes recentes arestos do TJUE, isto é, **o saber se a dita lei nacional cumpre os requisitos da indicada Directiva, da Carta dos Direitos Fundamentais da União Europeia, da Convenção Europeia dos Direitos do Homem e da Constituição da República Portuguesa**.
O que, por nós, não afasta a constatação de que **a leitura que o Digno recorrente faz** – assim como a dos acórdãos por ele citados – **recolocam o problema nessa sede, o da violação dos indicados artigos da Carta dos Direitos Fundamentais da União Europeia pela Lei 32/2008**.
Isto é, depois de terem considerado que o pedido era admissível em termos processuais, **teriam que analisar todo o dispositivo da Lei nº 32/2008 para apurarem da sua conformidade constitucional, da sua conformidade com a Convenção Europeia dos Direitos do Homem e com a Carta dos Direitos Fundamentais da União Europeia**. E não vimos isso a ser feito por qualquer dos acórdãos citados no recurso.
Deve ser por esta razão que, apesar dos repetidos avisos da CNPD o tema destas (in)conformidades da Lei nº 32/2008 passou à condição de *tabu* legislativo.
*
B.4 – A Directiva (UE) 2019/713 e a Lei 79/2021.
Questão mais linear mas que o Digno recorrente – por ser desnecessária para a sua argumentação – não considerou, é a mera leitura literal comparada dos normativos aqui citados, o comunitário e o nacional.
Repare-se que a Directiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, se diz e tem como objectivo o «***combate à fraude e à contrafação de meios de pagamento*** *que não em numerário*».
Dos seus considerandos, consta, de entre outros pontos, o seguinte:

(1) ***A fraude e a contrafação de meios de pagamento que não em numerário constituem uma ameaça à segurança, uma vez que representam uma fonte de rendimento para a criminalidade organizada****, sendo, por conseguinte, uma forma de facilitar outras atividades criminosas como o terrorismo, o tráfico de estupefacientes e o tráfico de seres humanos.*
(2) ***A fraude e a contrafação de meios de pagamento*** *que não em numerário constituem também um obstáculo ao mercado único digital, uma vez que minam a confiança dos consumidores e provocam perdas económicas diretas.*
*(3) A Decisão-Quadro 2001/413/JAI do Conselho (3****) necessita de ser atualizada e complementada a fim de incluir disposições suplementares sobre infrações, designadamente em matéria de fraude informática, e sobre sanções****, prevenção, assistência às vítimas e cooperação transfronteiriça.*
(4) ***A existência de lacunas e diferenças significativas na legislação dos Estados-Membros nos domínios da fraude e da contrafação de meios de pagamento*** *que não em numerário pode obstar à prevenção e à deteção desses tipos de infrações e de outras formas graves de criminalidade organizada com eles relacionadas ou por eles facilitadas, bem como a aplicação de sanções na matéria, e torna a cooperação policial e judiciária mais complicada e, por conseguinte, menos eficaz, com repercussões negativas na segurança.*
(5) ***A fraude e a contrafação de meios de pagamento que não em numerário têm uma importante dimensão transfronteiriça****, acentuada por uma componente digital cada vez maior, que realça a necessidade de medidas adicionais para aproximar a legislação penal nos domínios da fraude e da contrafação de meios de pagamento que não em numerário.*
(…)
(11) ***O envio de faturas falsas para a obtenção de credenciais de pagamento deverá ser considerado uma tentativa de apropriação ilícita no âmbito de aplicação da presente diretiva.***
(…)
(15) A presente diretiva faz referência a ***formas de conduta clássicas, como fraude, falsificação, furto e apropriação ilícita, que já foram delineadas pelo direito nacional antes da era digital. O âmbito alargado da presente diretiva no que diz respeito aos instrumentos de pagamento não corpóreos implica portanto a definição de formas de conduta equivalentes na esfera digital, que complementem e reforcem a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho.*** *A obtenção*

ilícita de um instrumento de pagamento não corpóreo que não em numerário deverá configurar uma infração penal, pelo menos quando envolva a prática de uma das infrações referidas nos artigos 3º a 6º da Diretiva 2013/40/UE, ou a apropriação ilegítima de um instrumento de pagamento não corpóreo que não em numerário. ***Por «apropriação ilegítima», deverá entender-se a utilização sem direito a tal, com conhecimento de causa, em benefício próprio ou de terceiro, de um instrumento de pagamento não corpóreo que não em numerário por uma pessoa a quem esse instrumento tenha sido confiado. A aquisição para utilização fraudulenta de um desses instrumentos obtido de forma ilícita deverá ser punível, sem ser necessário estabelecer todos os elementos factuais da obtenção ilícita, e sem exigir uma condenação anterior ou simultânea por uma infração subjacente que tenha dado origem à obtenção ilícita.***

(…)

Há, portanto, uma dupla perspectiva na Directiva: a Fraude e a Contrafacção.

O termo "contrafacção" exige uma vertente de "falsificação material" de um instrumento ou meio de pagamento.

E, não temos dúvida sobre o ponto, o termo "fraude" é usado aqui num sentido amplo que inclui modelos de tipos criminais clássicos, como ela própria refere, «*formas de conduta clássicas, como fraude, falsificação, furto e apropriação ilícita, que já foram delineadas pelo direito nacional antes da era digital*» e «*o envio de faturas falsas*».

Assim, o termo "fraude" pode incluir qualquer tipo penal clássico que seja praticada com meios digitais, incluindo a burla, crime que aqui está em causa.

Mas, contrariamente ao que a própria Directiva sugeriu, o legislador nacional não seguiu o conselho quanto à "fraude", limitou-se a seguir o conselho da Directiva apenas quanto à contrafacção, criando vários tipos penais de contrafacção que veio a incluir – de forma muito discutível – na Lei nº 109/2009, a Lei do Cibercrime, nos artigos 3º-A a 3º-F.

E, depois, viu-se na necessidade de alterar a al. g), do nº 1 do artigo 2º da Lei nº 32/2008 para incluir a expressão «*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*» apenas para conseguir incluir as novas "contrafacções da Lei do Cibercrime e alargar o objecto da "conservação" e o seu prazo.

Se a Directiva tem por objetivo acautelar, investigar e punir a «fraude e a contrafação de meios de pagamento que não em numerário», o legislador português apenas se preocupou com a «contrafação de meios de pagamento».

Olvidou um grande espaço de criminalidade digital, incluindo a dos autos.

Esqueceu-se (?) das fraudes em sentido amplo – incluindo as burlas - a que a Directiva se referia. E esqueceu-se também (?) de seguir o conselho avisado da CNPD para rever adequadamente a Lei nº 32/2008.
Reage o Ministério Público com um sentimento e uma razão de incoerência do sistema? É natural! Também nós pensamos que o sistema é incoerente, quer o processual penal e, agora, o penal. Mas a incoerência tem forma de Lei. Mas ao ver os pareceres do C.S. do Ministério Público e do CSM sobre a Lei 79/2021, tudo parece ir bem no Reino da Dinamarca! [5]
*
B.5 – Equilíbrio
Um outro aspecto que releva na apreciação da questão colocada no recurso é o acento tónico colocado pelo Digno recorrente nas necessidades de investigação policial e coerência do sistema de investigação e instrução dos autos, através de um notável trabalho comparativo entre regimes que, não temos dúvida, muito útil seria numa alteração pensada e coerente das leis aplicáveis, incluindo um capítulo – no processo penal - dedicado às questões da informática, de comunicações electrónicas, de drones e obtenção de prova por GPS e outras tecnologias.
Seria o tão desejado capítulo de prova electrónica e informática que, em vez de residir – onde deveria – no Código de Processo Penal, está disperso por vários diplomas que bastas vezes se confundem, baralham, sobrepõem e, seguramente, atrapalham quer o trabalho de investigação e instrução dos autos, mas também fases subsequentes do processo penal.
No entanto, o trabalho do tribunal não é fazer interpretação ab rogante das leis vigentes que, é bom recordar, se centram na defesa dos direitos do cidadão, pessoa singular, designadamente da sua privacidade e não apenas nas necessidades da investigação e instrução.
Nos acórdãos citados pelo Digno recorrente, o desta Relação de Évora de 25-05-2021 centra a sua atenção numa análise nos aspectos substantivos da Lei do Cibercrime mas não fundamenta de forma expressa o aspecto processual aqui tratado.
Quanto ao acórdão da Relação de Guimarães - que fundamenta o tema de forma expressa - olvida um aspecto essencial na abordagem do tema com uma preocupação centrada unicamente na busca, ao que parece de forma exclusiva e a qualquer custo, “da verdade e da justiça”, partindo de uma análise de equiparação dos papéis do Ministério Público e dos Juízes na busca dessa verdade e da justiça.
Na fundamentação do acórdão da Relação de Guimarães é claríssima a ideia de que a sua posição é assumida por interpretação “conjunta” da Lei nº 32/2008 e da Directiva nº 2006/24/CE, do Parlamento Europeu e do Conselho,

de 15 de março, como se surpreende nestes parágrafos:

A lei 32/2008 de 17 de julho foi criada para transpor para a ordem jurídica interna a Diretiva nº 2006/24/CE, *do Parlamento Europeu e do Conselho, de 15 de março (entretanto declarada inválida pelo TJUE no acórdão Digital Rights Ireland), 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, que alterou a Diretiva nº 2002/58/CE do Parlamento Europeu e do Conselho de 12.06, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.*
Do texto da Diretiva 2006/24/CE resultava clara, por um lado, a afirmação de que qualquer pessoa tem direito ao respeito da sua vida privada e da sua correspondência, mas, por outro, que as autoridades públicas só podem, mas podem, interferir no exercício desse direito quando tal se revelar necessário, numa sociedade democrática, *para a segurança nacional ou para a segurança pública, a defesa da ordem e a prevenção das infrações penais ou a proteção dos direitos e liberdades de terceiros.* ***Foi, pois, objetivo da Diretiva assegurar que nos diversos Estados-Membros fossem harmonizadas as obrigações que incumbiam aos fornecedores de conservarem determinados dados e assegurarem que eles pudessem ser disponibilizados para efeitos de investigação, deteção e repressão de crimes graves****, tal como definidos no direito nacional de cada Estado-Membro.*
Ora sendo o objetivo da Diretiva, que a Lei 32/2008 transpôs, harmonizar a obrigação de conservação de dados entre Estados – Membros, não será lícito retirar sem mais, como o faz o recorrente, que as normas que, no CPP, regulam a matéria das " Escutas telefónicas"- art. 187 e 188 do CPP e sua "Extensão"- art. 189 se encontram revogadas, ou que só se aplicam aos dados sobre a localização celular obtidos em tempo real. *Aliás, é a própria lei 32/2008 que no nº 2 do art. 1º ressalva a possibilidade de aplicação da legislação processual penal. E se a ressalva abrange a interceção e gravação, portanto, o conteúdo das comunicações, muito mais se tem de entender que abranja a obtenção de dados de localização celular, meio de obtenção de prova muito menos intrusivo da intimidade e da privacidade das pessoas, uma vez que se trata de meros registos de localização (aproximada) obtidos independentemente da utilização de telefones, por força do acionamento de células de rede (BTS- Base Transfer Station), menos intrusivo até que as tradicionais vigilâncias policiais.*

Ou seja, a posição e a fundamentação do dito aresto de Guimarães assenta na interpretação que faz da Lei nº 32/2008 em função do que consta da Directiva de 2006 que já foi declarada inválida pelo TJUE, declaração de invalidade essa que é válida para a ordem jurídica nacional por via da aplicação do princípio do primado do direito comunitário. Em breve, não é lícito a um tribunal nacional aplicar e fundamentar com base numa Directiva declarada inválida pelo Tribunal de Justiça da União Europeia.
E, apesar de o TRG atestar a declaração de invalidade da Directiva de 2006 pelo aresto *Digital Rights Ireland* não retira daí a devida ilação – de que a Directiva nº 2006/24/CE, do Parlamento Europeu e do Conselho não pode ser aplicada nem fundamentar a aplicação de normativo nacional – raciocinando como se a mesma fosse válida e interpretando a Lei nº 32/2008 com o apoio da Directiva inválida para sustentar a sua posição.
Uma análise mais substancial da matéria teria revelado que o TJUE nos arestos mais recentes tem centrado a análise jurídica sobre a conservação de dados – de forma natural e óbvia – não na Directiva inválida de 2006, o que seria um contrassenso, sim na Directiva de 2002, a Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao **tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas** (Directiva relativa à privacidade e às comunicações electrónicas). Esta Directiva de 2002 foi naturalmente repristinada em função da declaração de invalidade da Directiva de 2006.
Para além deste insustentável aspecto formal e orgânico recorde-se que as Directivas aplicáveis ao longo do tempo centram-se no campo dos direitos do cidadão, é na privacidade que colocam a questão e não no exercício dos poderes do Estado. Veja-se:
*- Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa **à protecção das pessoas singulares** no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*
*- Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao **tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas** (Directiva relativa à privacidade e às comunicações electrónicas)*
*- Directiva 2009/136/CE do Parlamento Europeu e do Conselho de 25 de Novembro de 2009 que **altera** a Directiva 2002/22/CE relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas, a **Directiva 2002/58/CE** relativa ao **tratamento de dados pessoais e à protecção da privacidade** no sector das comunicações electrónicas e o Regulamento (CE) n. 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da*

legislação de defesa do consumidor.
Estamos, pois, a falar de intrusão do Estado na privacidade do cidadão já que a localização celular constitui violação da privacidade do cidadão.
E o TRG inverte a norma geral – privacidade do cidadão – para excepção e transforma a excepção (a excepcional interferência no exercício desse direito quando tal se revelar necessário, numa sociedade democrática), em regra geral, de tal forma que a Directiva de protecção da privacidade já declarada inválida passa a ter por objetivo «*assegurar que nos diversos Estados-Membros fossem harmonizadas as obrigações que incumbiam aos fornecedores de conservarem determinados dados e assegurarem que eles pudessem ser disponibilizados para efeitos de investigação, deteção e repressão de crimes graves, tal como definidos no direito nacional de cada Estado-Membro*.» A privacidade passou a ser apenas um pretexto para a acção livre do Estado!
E esqueceu o artigo 9º da Lei 32/2008 e lá se foi a privacidade do cidadão.
E a defesa do cidadão faz-se, habitualmente, pela definição clara de "catálogos de crimes" a que fica sujeita a acção dos operadores de comunicações e do Estado à face dessa legislação, à imagem do que ocorre com o catálogo de crimes do C.P.P. e da Lei do Cibercrime. E, neste particular ponto, entendemos que os artigos 3º e 9º da Lei nº 32/2008 só podem ter o significado que lhe atribuímos, o de um catálogo de crimes limitador da acção do Estado face à privacidade do cidadão.
E tal ocorreu com a Lei nº 32/2008, continuando nós a entender que a sujeição da autorização da acção pretendida a um "catálogo de crimes" tem em vista concretizar um equilíbrio entre a violação dessa privacidade do cidadão e a necessidade de acautelar outros interesse relevantes. E, não nos parece, a permitir que o Estado se intrometa na privacidade em todos os casos e que, ainda por cima, os registos durem mais tempo.
Porque considerar que a Lei 32/2008 não contém um "catálogo de crimes" limitador é afirmar que o acesso aos dados conservados e referidos no artigo 4º da Lei nº 32/2008 é livre independentemente do crime ou contra-ordenação praticados. Se o resultado prático é este não percebemos o porquê da existência de tantas Directivas de "protecção da privacidade" e da própria necessidade de a Lei 32/2008 prever a intervenção judicial, já que nada haveria a ponderar. Tudo seria permitido a qualquer um, em qualquer momento!
E mantemos a nossa opinião de que se a situação concreta exposta nos autos não cabe nesse "catálogo" isso demonstra que ela não é permissiva da violação da privacidade do cidadão.
Sempre recordando que a Lei 32/2008 é lei interna e que as Directivas são lei

comunitária e, como tal, o primado do direito comunitário deve estar sempre presente, não permitindo que no caso a Lei nacional (ainda por cima de transposição de uma Directiva declarada judicialmente inválida), estabeleça um regime que significaria, de forma simples, a total revogação das ditas Directivas e a violação – sem resguardo judicial – da privacidade do cidadão e, nos termos da jurisprudência estabelecida nos processos Digital Rights Ireland Ltd (C-293/12) e Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl (C-594/12) e nos outros dois supra citados, pelo menos.
E partindo de uma visão claramente alicerçada numa sobreposição dos interesses da investigação policial sobre os direitos acautelados por esses normativos no âmbito da privacidade, reduzindo-os a zero. Trata-se de uma defesa implícita de um Estado policial.
Para finalizar, a leitura que o Digno recorrente faz – assim como a dos acórdãos por ele citados – recolocam o problema na sede de violação dos indicados artigos 7º, 8º e 11º da Carta dos Direitos Fundamentais da União Europeia pela Lei 32/2008 (principalmente, no caso, os artigos 7º e 8º) e artigos 26º, nº 1 e 34º, ns. 1 e 4 da Constituição da República Portuguesa, para além da violação do artigo 8º da Convenção Europeia dos Direitos do Homem.
Será esta leitura da Lei nº 32/2008 que os pareceres da CNPD consideram claramente inconstitucional e a merecer revisão, que já era urgente em 2017.
Por todas as razões, mas esperando acção legislativa esclarecedora ou recurso de fixação de jurisprudência, aqui facilitado pela existência de dois acórdãos contraditórios, o recurso é improcedente.
*
C - Dispositivo
Assim, em face do exposto se decide declarar o recurso improcedente.
Sem custas.
(elaborado e revisto pelo signatário antes de assinado).
Évora, 22 de Fevereiro de 2022

João Gomes de Sousa
António Condesso

[1] - V. g. o prof. Costa Andrade, «“Bruscamente no verão passado”, a reforma do Código de Processo Penal - Observações críticas sobre uma lei que podia e devia ter sido diferente», in RLJ, ano 137 (2008), passim; Dá Mesquita, in “Processo Penal, Prova e Sistema Judiciário”, Wolters Kluwer/Coimbra Editora, 2010, pags. 87-95.
[2] - http://www.gddc.pt/siii/im.asp?id=2083
[3] - Dá Mesquita, Paulo, ob. cit., pag. 94 e nota 23.
[4] - O Parecer 51/2015 sobre o SIRP não é tão explícito relativamente ao tema aqui tratado mas é igualmente crítico quanto à constitucionalidade da proposta aí apresentada e analisa igualmente a Lei nº 32/2008.
[5] - https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=110841