UNIVERSIDADE D
COIMBRA

Sofia Martins da Costa de Melo e Silva

A CONSERVAÇÃO E TRANSMISSÃO DE DADOS NOS TERMOS DA LEI Nº 32/2008 PARA FINS DE INVESTIGAÇÃO CRIMINAL

Dissertação no âmbito do Mestrado em Ciências Jurídico-Forenses orientada pela Professora Doutora Sónia Mariza Florêncio Fidalgo e apresentada à Faculdade de Direito da Universidade de Coimbra

Janeiro de 2022

SOFIA MARTINS DA COSTA DE MELO E SILVA

A conservação e transmissão de dados nos termos da Lei nº 32/2008 para fins de investigação criminal

The conservation and data transmission under the terms of Law nº 32/2008 for the purpose of criminal investigation

Dissertação apresentada à Faculdade de Direito da Universidade de Coimbra no âmbito do 2º Ciclo de Estudos em Ciências Jurídico-Forenses (conducente ao grau de mestre), sob a orientação da Senhora Doutora Sónia Mariza Florêncio Fidalgo

Coimbra, 2022

RESUMO

As novas tecnologias e, em especial, a *internet* vieram alterar radicalmente o modo como nos relacionamos uns com os outros, mas também o modo como os setores mais importantes das comunidades se desenvolvem.

As novas tecnologias trouxeram virtualidades que dispararam indiscutivelmente a qualidade de vida das pessoas, permitem que viajemos sem sair do sofá, que combatamos as saudades dos entes queridos quando estejam longe, que trabalhemos em qualquer parte do Mundo, entre outras. Porém, tais particularidades também foram transpostas para o mundo mais obscuro e violento, suscitando dificuldades que antes nunca tinham sido sentidas, especialmente quando nos deparamos com as insuficiências de adaptação dos métodos tradicionais às especificidades da realidade digital. A consciencialização de que as novas tecnologias tinham de ser inseridas na prática judiciária com vista a permitir que esta alcançasse o seu expoente máximo de eficácia, embora não tenha sido imediata, foi algo sentido desde há muito e, inerente a este sentimento, surgiram as preocupações e dúvidas relativamente à sua compatibilização com os direitos fundamentais de todos os cidadãos.

Na balança que se procura equilibrar temos, por um lado, a esfera íntima de cada um e o direito de estes controlarem o destino das suas informações pessoais, enquanto, por outro, temos uma realidade que depende de uma partilha de dados pessoais cada vez mais intensa, em muitos casos com a justificação de que é por um bem maior, com a justificação de que devemos deslocar a nossa prioridade do ente singular para o bem comunitário. A Lei nº32/2008, objeto de dissecação ao longo de toda a dissertação, é reflexo dessa dificuldade de compatibilização, pois, se visa fazer frente às dificuldades inerentes às investigações criminais de ilícitos em cuja execução se lançou mão das novas tecnologias e à sensibilidade da prova digital, não é menos verdade que consiste numa ordem de armazenamento de uma quantidade colossal de dados pessoalíssimos de todos os cidadãos que utilizem serviços de comunicações eletrónicas.

PALAVRAS-CHAVE

Cibercriminalidade - Lei nº 32/2008 - dados de tráfego e de localização - proteção de dados - privacidade - investigação criminal;

ABSTRACT

The new technologies and, especially, the *internet* changed radically the way we interact with each other, but also the way the most important communities' sectors develop themselves.

The new technologies brought virtual qualities that increased without a doubt the people's quality of life, these characteristics allowed us to travel without leaving our couch, to keep in touch with our loved ones even when they're faraway, to work from anywhere in the World, and many more. However, these features have also been transposed into a more obscure and violent world, raising difficulties the had never been felt before, especially when we come across the poorly adaptation of the traditional methods to the digital reality. The awareness that the new technologies needed to be added to the practice of law with the goal of achieving its maximum efficiency, although not instantly, was noticed for a long time and, associated with this feeling, some concerns and questions emerged regarding the compatibility with all citizen's fundamental rights.

On the scale with the purpose of balance we have, on one hand, the personal sphere of each person and the right to control the destiny of their personal information, while on the other hand, we have a reality that relies on increasingly sharing personal data, in many instances with the excuse that is for a greater good and that we should prioritize the common good before the individual good. The Law nº 32/2008, subject os dissection of this dissertation, it's the reflection of this difficulty of compatibilization, because it aims to overcome struggles related to criminal investigations of illegal actions in whose execution new technologies and the sensitivity of digital proof were used, it's not less true that consists of storage of an abnormal amount of personal data from every citizen that uses electronic communications services.

KEYWORDS

Cybercrime – Law nº 32/2008 – traffic and location data – data protection – privacy – criminal investigation

LISTA DE SIGLAS E ABREVIATURAS:

Ac. – Acórdão

Al. – Alínea

Art. – Artigo

CEDH – Convenção Europeia dos Direitos do Homem

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

IP – Internet Protocol

LC – Lei do Cibercrime

MP – Ministério Público

Nº - Número

P. – Página

RGPD – Regulamento Geral de Proteção de Dados

TC – Tribunal Constitucional

TJUE – Tribunal de Justiça da União Europeia

TRL – Tribunal da Relação de Lisboa

Índice

I. Introdução

1. Enquadramento da problemática no direito probatório

Em pleno século XXI, devido ao intenso desenvolvimento científico-tecnológico verificado, é comummente feita referência à globalização. Esta consiste, justamente, no processo de aproximação entre as diversas sociedades e nações de todo o mundo relativamente a todos os níveis de organização da vida individual ou coletiva, seja no setor cultural, económico, da justiça ou social. Consequentemente a esta aproximação, surge um outro conceito: o de "*aldeia global*" – termo elaborado por *Marshall McLuhan* que visava traduzir a ideia de que, com o avanço tecnológico, o encurtamento de distâncias e a possibilidade de comunicar diretamente e sem barreiras estaríamos mundialmente a viver a experiência própria duma aldeia[1].

A *internet* revolucionou os nossos dias, tornando-nos mais próximos e as suas virtualidades fizeram com que, num curto período de tempo, se tornasse impensável viver sem ela. Contudo, como na generalidade dos casos, esta é uma realidade ambígua: se, por um lado, nos permitiu aproximar uns dos outros, se instituiu facilidade e comodismo em realizar uma série de atividades sem sair do conforto das nossas casas, por outro, essas mesmas qualidades foram transpostas para o Mundo do Crime, facilitando o cometimento dos tidos como "crimes tradicionais", como impulsionando a criação de novas modalidades criminológicas. As novas tecnologias foram sendo introduzidas no *modus operandi* de inúmeros criminosos, nomeadamente nos grupos de crime organizado e terroristas, o que permitiu que estes se aproveitassem desmesuradamente destes instrumentos, potencializando não só a dimensão dos danos provocados, como também a capacidade de saírem impunes.

Assim, o surgimento do cibercrime reclamou, imediatamente, uma resposta clara e adequada do Estado e do Direito, essencialmente do direito penal e processual penal, de forma a evitar vazios jurídicos, lacunas insuportáveis no sistema e que os responsáveis por tais atos saiam impunes. Aliás, tais adaptações dos ordenamentos jurídicos às novas tecnologias eram desejadas, se não mesmo impostas, pelas próprias comunidades, pois dissipou-se um clima de medo e insegurança relativamente à utilização que poderia ser dada aos instrumentos tidos como facilitadores do quotidiano, especialmente com o sucesso

[1] MARSHALL, McLuhann, *"La Galaxia Gutenberg"*, p. 54.

obtido com ataques terroristas a grandes centros urbanos e com a proliferação da atividade criminosa levada a cabo por grupos de crime organizado que, devido à sua capacidade de adaptação, se têm aproveitado exageradamente das novas tecnologias[2].

Tendo surgido o direito penal enquanto um direito que visa proteger os bens jurídico-penais de uma determinada comunidade e incidindo sobre o Estado o dever de administrar e realizar a justiça penal, impôs-se que o ordenamento jurídico-penal fosse reforçado com um novo arsenal de métodos de investigação capaz de combater este tipo específico de criminalidade. Como é sabido, a "ciência total do direito penal"[3] é composta por três setores: o direito penal, o direito processual penal e o direito de execução das penas e das medidas de segurança. O direito penal para funcionar e atuar na realidade carece de uma regulamentação complementar que é, justamente, o direito processual penal - estabelecendo-se entre ambos uma relação de mútua complementaridade funcional. O direito processual penal, nas palavras do doutor Figueiredo Dias, consiste na *"argumentação jurídica da realização do direito penal substantivo, através da investigação e valoração do comportamento do acusado da prática de um facto criminoso"* [4]. Será, pois, o direito processual penal que estabelecerá os termos e métodos que devem ser seguidos na investigação, esclarecimento e aplicação de uma pena justa ao tipo de crime concreto. Figueiredo Dias diz, ainda, que o processo penal visa declarar "*o direito do caso concreto, i.e., definindo o que para este caso é, hoje e aqui, justo*", o que ressalva a necessidade constante de atualização dos métodos utilizados conforme as carências atuais da sociedade.

No que respeita a métodos de investigação, *maxime* a direito probatório, atualmente, as atualizações exigidas prendem-se, quase que essencialmente, na utilização das novas tecnologias, desde logo porque, como referido por Helena Carrapiço, "*a tecnologia é uma faca de dois gumes: se pode ser manipulada no âmbito de atividades ilícitas, também pode ser utilizada para combater estas últimas*"[5]. Com o surgimento do cibercrime, torna-se imprescindível recorrer aos meios digitais na procura de prova adequada à descoberta e

[2] CARRAPIÇO, Helena, "*O Crime Organizado e as Novas Tecnologias: uma Faca de Dois Gumes",* p. 181: "*A enorme capacidade de adaptação do crime organizado permitiu-lhe tirar partilho do progresso tecnológico, tendo-se tornado até um dos seus principais beneficiários. O desenvolvimento em áreas como as comunicações, os transportes e o ciberespaço aumentaram de forma exponencial o campo em que estes grupos podem operar".*
[3] ANTUNES, Maria João, "*Direito Processual Penal*", p. 7.
[4] DIAS, Jorge de Figueiredo, "*Direito Processual Penal*", p. 28.
[5] CARRAPIÇO, Helena, ob. cit. p. 177.

punição dos agentes responsáveis não só pelo cometimento de ilícitos informáticos em sentido amplo, mas também por aqueles em sentido restrito[6]. Atualmente, existe uma forte dependência da população sobre estas novas tecnologias, o que aumenta a probabilidade de os órgãos responsáveis pela investigação criminal conseguirem um rasto digital que as leve aos verdadeiros autores dos ilícitos.

Não obstante a exigida evolução por parte do ordenamento jurídico-penal português para fazer face a todas as metamorfoses vislumbradas na realidade, em consonância com um processo penal democrático, importa salientar que tal tipo de ação nunca pode deixar de ser realizado com pleno respeito pelos direitos fundamentais dos cidadãos, *maxime* da pessoa do arguido, de forma a garantir a validade epistemológica dos resultados cognoscitivos adquiridos ao longo do processo. Aliás, tal exigência encontra-se intrínseca na estrutura acusatória integrada por um princípio de investigação do nosso processo penal.

Assim, esta dissertação, após uma breve introdução sobre o sistema probatório que vigora em Portugal e sobre o fenómeno da cibercriminalidade, incidirá essencialmente sobre a Lei nº 32/2008, de 17 de julho de 2008, que transpôs para o ordenamento jurídico a Diretiva nº 2006/24/CE, do Parlamento Europeu e do Conselho, em 15 de março. Tal lei regula a conservação dos dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações para fins de investigação criminal. O objetivo será refletir sobre até que ponto é admitida a restrição de direitos, liberdades e garantias fundamentais dos cidadãos sob o preceito de medida adequada à manutenção da segurança comunitária, até que ponto é tolerável a intromissão da máquina estadual na privacidade dos cidadãos em nome de um bem maior…

II. Da prova física à prova digital

1. Cibercriminalidade

O fenómeno da cibercriminalidade introduziu-se no nosso dia-a-dia ao longo do início deste novo século, porém, tal não implica necessariamente que as pessoas tenham já perceção completa dos riscos que correm ao entrar no espaço cibernético, nem das cedências que admitem relativamente à sua esfera pessoal no mundo *online*.

[6]VENÂNCIO, Pedro Dias, "*Lei do Cibercrime- Anotada e Comentada"*. Os conceitos de criminalidade informática em sentido amplo e em sentido estrito serão densificados posteriormente.

O ano 2020 foi um ano que será recordado como poucos outros, marcado pelo contexto pandémico que revolucionou o quotidiano da população mundial, seja a nível pessoal, profissional ou económico. À revelia de todos os planos e projetos que haviam sido idealizados para 2020, impôs-se às pessoas que se restringissem às quatro paredes da sua habitação, o que as "obrigou" a mergulharem no mundo digital, de forma a poderem continuar a trabalhar, a viajar, a comunicar com o outro, a obter serviços básicos, entre outros. No relatório "Riscos & Conflitos 2021"[7], realizado pelo Centro Nacional de Cibersegurança em Portugal, é possível constatar o aumento dos ataques no ciberespaço e associá-los, inevitavelmente, ao período de confinamento social, o que revelou que os cibercriminosos, aproveitando a "migração para o mundo online" de grande parte da população mundial, começassem a tirar partido de inúmeras vulnerabilidades, fossem estas técnicas ou humanas.

Um dos maiores objetivos para fazer face a este fenómeno é, justamente, a sensibilização da população à perceção dos riscos que incorrem no mundo digital, procurando evitar a partilha negligenciada de dados cruciais. Assim sendo, o que é que deve ser entendido como criminalidade informática? Não existe consenso doutrinal sobre o que deve ser compreendido como tal, nem legislação que o defina expressamente. Garcia Marques e Lourenço Martins[8] foram dos primeiros autores em Portugal a dedicarem-se especialmente a esta matéria e, em 2006, consideraram como criminalidade informática: "*todo o ato em que o computador serve de meio para atingir um objetivo criminoso ou em que o computador é o alvo simbólico desse ato ou em que o computador é "objeto" do crime",* já o doutor Pedro Dias Venâncio encontra no conceito global de cibercriminalidade dois subconceitos[9]: a cibercriminalidade em sentido estrito e aquela em sentido amplo. A cibercriminalidade em sentido amplo abrange todos aqueles comportamentos criminosos que sejam levados a cabo por meios informáticos – a informática é somente um dos meios existentes para a prática daquele delito. Já a criminalidade informática em sentido estrito é composta por aqueles delitos em cujo tipo legal encontramos o elemento informático – a informática é um dos elementos integradores do tipo de ilícito ou o bem jurídico-penal a ser protegido. É com base nesta definição que o trabalho se desenrolará.

[7] https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_riscos_conflitos2021.pdf
[8] MARQUES, Garcia e MARTINS, Lourenço, "*Direito da Informática"*, p. 641.
[9]VENÂNCIO, Pedro Dias, *ob. cit.*, p. 17.

Os meios informáticos tornaram-se, com o decurso do tempo, verdadeiras "armas de crime" e levaram ao surgimento de um tipo de criminalidade que evoluiu exponencialmente mais rápido do que os métodos utilizados pelas entidades responsáveis pela sua investigação ou de ser alvo da devida atenção legislativa por parte da União Europeia, começando a levantar diversos problemas, nomeadamente na incapacidade de enquadrar os seus recortes nos mecanismos legais existentes.

Em primeiro lugar, inevitavelmente, é caraterística deste tipo de criminalidade a utilização de tecnologia como meio operacional para o cometimento de ilícitos. A utilização de instrumentos de alta tecnologia permite que os delinquentes consigam cometer os ilícitos "à distância de um *click*", potenciando os danos, as vítimas e os lucros. Aliás, tal meio permite a realização de ilícitos de forma automatizada, dispensando o impulso humano no momento da sua concretização – o que, mais uma vez, acentua as dificuldades de investigação, pois o agente responsável poderá estar a realizar o curso normal da sua vida e nunca deixar suspeita, em quem o rodeia, dos seus planos e intenções[10].

Associada à utilização de tecnologia e à indiferença da proximidade do alvo, torna-se claro que que a cibercriminalidade promove a internacionalização[11], ou seja, este tipo de criminalidade provocou uma alteração da metodologia tradicional de cometer crimes por deixar de implicar uma certa proximidade física. Com a utilização de meios tecnológicos para cometer crimes, basta que o agente criminoso tenha acesso a um computador com ligação à *internet* e, através dele, entrar na rede onde navegam milhões de utilizadores de todo o Mundo que realizam atividades das mais variadas áreas[12].

A transnacionalidade desta modalidade criminológica assume relevância não só na própria metodologia de cometer os ilícitos, mas também na "segurança" que lhes é atribuída, pois associada a esta caraterística assume papel central a simplicidade na manutenção do anonimato, permitindo, ainda, constituir parcerias e facilitar a cooperação entre grupos criminosos. Aliás, o estabelecimento deste tipo de relação é mais comum nos grupos de

[10] NATÁRIO, Rui, *"O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço"*, p. 9
[11] O caráter transfronteiriço desta modalidade criminológica é evidente não só na realização do ilícito, mas também na sua prova. É possível que as investigações criminais estejam a ocorrer num determinado país e as entidades competentes recorram a dados que se encontram armazenados em servidores de outros países. Tornando-se evidente a necessidade de estabelecimento de estreitas relações de cooperação entre os diversos Estados, sejam estes integrantes da União Europeia ou não (https://ec.europa.eu/info/sites/default/files/placeholder_2.pdf)
[12] NATÁRIO, Rui, ob. cit., p. 9.

crime organizado: "*Rather than treat each other as rivals, many criminal organizations are sharing information, services, resources, and market access according to the principle of comparative advantage. By doing so, they can reduce their risks and costs and are better able to exploit illicit criminal opportunities"*[13]. Por sua vez, a invenção de novas técnicas de dissimulação que dificultam a identificação do agente ou a criação de estruturas que facilitam a ocultação dos resultados provenientes da atividade ilícita (como empresas de fachada) são aspetos que favorecem a impunidade dos agentes que recorrem a estes métodos[14].

Já referido reflexamente acima, mas assumindo extrema importância, é a organização que se pode imputar à realização deste tipo de ilícitos. Os grupos de crime organizado, geralmente, assumem uma estrutura hierarquizada, dedicando-se a atividades ilegais e utilizam, em regra, métodos que lhes permitem destruir os obstáculos à sua atividade, nomeadamente através do uso de violência ou exercendo influência em áreas impactantes da vida social, como a política e a económica. Para além da organização que se aponta a este tipo de criminalidade, esta permite, como já referido, uma potencialização exponencial dos danos causados, sejam estes físicos ou económicos. Em 2020, a EMPACT (European Multidisciplinary Platform Against Criminal Threats[15]) conseguiu evitar a fraude de pagamentos no valor de 73,5 milhões de euros[16], contudo, não há estudos que permitam definir com precisão o impacto financeiro que continua a causar[17].

2. Especificidades da prova digital

Uma vez entendido o que deve ser concebido como a cibercriminalidade e as especificidades que esta reveste, importa analisar com detalhe a prova digital *per si.*

A prova digital pode ser definida como *"a prova produzida a partir de dados em formato digital (na forma binária), "que são manipulados, armazenados ou comunicados através de qualquer dispositivo, computador ou sistema informático, ou transmitidos*

[13] CARRAPIÇO, Helena, ob. cit. p.181.
[14] https://www.ojp.gov/pdffiles1/Digitization/189403NCJRS.pdf p. 16
[15] A EMPACT é uma iniciativa dos Estados Membros da União Europeia que tem como prioridade identificar e enfrentar as ameaças que são colocadas pelo crime internacional organizado. Uma das suas maiores preocupações é, justamente, o cibercrime e trabalha multidisciplinarmente, desde logo com a Europol, Frontex, Eurojust, entre outras) de forma a conseguir realizar eficazmente os seus objetivos.
[16] https://www.consilium.europa.eu/pt/infographics/results-eu-fight-against-crime-2020/
[17] Neste sentido, constata-se que "*as perdas provenientes das manipulações informáticas de conteúdo económico são em média muito mais elevadas que as decorrentes das fraudes tradicionais"* (MARQUES, Garcia e MARTINS, Lourenço, ob. cit. p. 645.

através de um sistema de comunicação""[18] sendo assim, é através desta que poderemos aceder a uma variadíssima categoria de dados (fotografias, dados de tráfego, de localização, conteúdos de e-mails, etc). Aliás, dentro dos diversos meios de prova que são categorizados pelo legislador, podemos incorporar a prova digital na prova pericial, por esta exigir conhecimentos específicos para a sua perceção e apreciação, mas também como prova documental, nos casos de redução a escrito ou outro meio técnico no processo de corporização por que passa no processo.

Primeiro que tudo, é possível apontar a imaterialidade ou invisibilidade da prova[19], isto é, a prova existe independentemente do suporte material que incorpore, consiste numa sequência de bits. Porém, importa salientar que, embora esta seja "invisível", carece necessariamente de transposição física para o processo penal, o que não implica a perda de identidade tecnológica da prova.

É, ainda, uma prova relativamente frágil e volátil, o que ressalta a importância do respeito total pela cadeia de custódia da prova, de forma a evitar que a mesma se perca e seja inviabilizada qualquer contribuição daquela para o processo[20]. A fragilidade e volatilidade desta prova revela-se na facilidade com que se conseguem ocultar dados ou substituir os mesmos, bem como nas cautelas acrescidas que são exigidas para o seu transporte e depósito, desde logo no sentido de ficarem afastados de campos eletromagnéticos e serem transportados em sacos anti-estáticos[21].

Paralelamente a este caráter frágil e volátil, podemos apontar um estudo realizado por Quin Yuhai e Fu Xiaolei que apontava como caraterística da prova digital a sua *"alta tecnologia científica"*. Segundo estes autores, se a cadeia de custódia for respeitada e não for dada oportunidade para eventuais deturpações, a prova digital assume um valor probatório bastante intenso, atribuindo-lhes uma alta taxa de fiabilidade com a realidade[22].

Por fim, e associado à sua volatilidade, importa analisar o caráter temporário da mesma, isto é, são dados que rapidamente podem deixar de existir. Assume elevada importância, para fazer face a esta adversidade, a Lei nº 32/2008, de 17 de julho, que impõe

---

[18] Fidalgo, Sónia, *"A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo"*, p. 133
[19] Ramalho, David Silva, "*Métodos Ocultos de Investigação Criminal em Ambiente Digital*", p. 104.
[20] Ramalho, David Silva, ob. cit., p. 105
[21] Ramos, Armando Dias, *"A Prova Digital em Processo Penal: o correio eletrónico"*, p. 99.
[22] *Apud* Ramos, Armando Dias, ob. cit., p. 98.

justamente a conservação genérica dos dados de tráfego e de localização por parte dos fornecedores de serviços. Por força desta lei, tais dados devem ser conservados pelo prazo de 12 meses, permitindo que, no decurso desse prazo e obedecidos os requisitos impostos pelo legislador português, as autoridades judiciárias possam aceder a estes para efeitos de investigação, deteção e repressão de crimes graves. Após o decurso do prazo, e na falta de uma ordem de preservação expedita de dados (art. 12º da Lei do Cibercrime), tais dados devem ser destruídos (art. 7º/e) da Lei nº 32/2008). Contudo, embora esta lei tenha permitido acesso a dados cuja existência era tão breve, tem levantado inúmeros problemas quanto à sua proporcionalidade e segurança relativamente aos dados conservados – questões estas que serão, posteriormente, objeto de análise pormenorizada. Não obstante a existência da Lei nº 32/2008, pode ser, ainda, apontada a Lei nº 23/96, de 26 de julho, a Lei dos Serviços Públicos. Porém, esta última, diferentemente da anterior, exige apenas a conservação dos dados necessários para efeitos de faturação (não especificando quais) e pelo prazo de 6 meses[23].

Terminada a análise e explicação das especificidades que moldam a prova digital, assume especial importância, neste âmbito, a ciência forense digital – *"ciência responsável pela recolha, preservação e análise de vestígios digitais, presentes nos mais diversos dispositivos de processamento, armazenamento e comunicação"*[24]. Tal categoria científica surgiu da constatação de que este tipo de prova tem de ser objeto de um manuseamento distinto daquele que é dedicado às provas ditas tradicionais, desde logo pela sua fragilidade e volatilidade. Tais métodos e procedimentos definidos para a sua recolha e obtenção, caso não sejam seguidos cautelosamente, podem acabar por tornar determinada prova inutilizável, com as inerentes consequências transportadas para a ação penal em causa. Associado à propagação dos meios digitais e à sua cada vez maior acessibilidade por parte de toda a população, o volume de dados armazenados tem vindo a aumentar exponencialmente e, consequentemente, o interesse das entidades investigadoras em aceder aos mesmos no âmbito de específicos processos penais. Porém, face à necessidade de o Estado reger a sua atuação com base numa imprescindível superioridade ética, tem-se tornado evidente a diferença entre as técnicas tecnológicas utilizadas para a prática de cibercrimes e aquelas

[23] Pinho, Carlos, "*Lei da retenção de dados de comunicações eletrónicas: aposentar ou reformar"*, Revista do Ministério Público, Nº 154, 2018, p. 171
[24] http://apcforenses.org/?page_id=36

que são mobilizadas no âmbito da ciência forense digital, o que, conjugado com falta de recursos, assume um caráter potencialmente lesivo relativamente às investigações em curso[25].

III. A Prova Digital em Portugal

1. Enquadramento Legislativo

Em 2021, celebraram-se os 20 anos de uma das maiores tragédias ocorridas desde sempre: o 11 de setembro – o atentado às Torres Gémeas e ao Pentágono nos Estados Unidos da América. Tal data ficou eternamente memorizada como um marco de mudança, mormente no respeitante à segurança nacional e à sua relação com os direitos fundamentais de cada um. Nesse dia, o Mundo mudou… ou só acordou para a face negativa da evolução tecnológica que se vem verificando ao longo dos anos.

A partir de 11 de setembro de 2001, e com a propagação de ataques terroristas, cada vez mais frequentes, no espaço europeu, verificou-se, à semelhança do apurado nos EUA, uma frenética criação de leis que visavam o combate a este tipo de criminalidade – o que resultou em leis que não foram devidamente pensadas ou debatidas[26]. Assim surgiu a Diretiva 2006/24/CE, do Parlamento e do Conselho, de 15 de março de 2006, 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, como expresso no ponto 10 do preâmbulo da mesma.

Contudo, previamente ao aprofundamento sobre o conteúdo desta Diretiva, importa analisar a evolução histórica da legislação nacional sobre a cibercriminalidade, começando pelas fontes internacionais. O instrumento que assumiu, em primeiro lugar, a nível internacional, importância suma foi a Convenção sobre o Cibercrime do Conselho da Europa (ou Convenção de Budapeste ou a Ciberconvenção), de 23 de novembro de 2001. Tal documento contou com a participação não exclusiva dos países europeus, encontrando-se contribuições de outros países como os Estados Unidos da América, o Japão, entre outros. Esta convenção tinha como principal objetivo "*realizar uma união mais estreita entre os seus membros"*[27], desde logo através da criação de uma política criminal comum, que

[25] FIDALGO, Sónia, ob. cit., p. 134.
[26] RAMOS, Armando Dias, ob. cit. p. 132 e ss.
[27] Preâmbulo da Convenção sobre o Cibercrime.

permitisse que os diversos Estados cooperassem de forma a proteger as sociedades contra a cibercriminalidade ao mesmo tempo que se encontrava o equilíbrio entre as medidas estabelecidas e a tutela dos direitos fundamentais dos cidadãos. Aliás, esta convenção, como é realçado no seu preâmbulo, tem como objetivo complementar outras convenções europeias, como é a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa de 1950, mas também o Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas de 1966, entre outros.

Fora a Convenção sobre o Cibercrime, é, ainda, de referir a emissão da Diretiva-Quadro do Conselho 2005/222/JAI, de 24 de fevereiro, sendo que esta tinha como objeto os ataques contra os sistemas de informação.

Portugal, embora a Convenção de Budapeste tenha sido adotada a 23 de novembro de 2001, apenas a ratificou e transpôs para o ordenamento jurídico nacional, juntamente com a Diretiva 2005/222/JAI do Conselho, de 24 de fevereiro, a 15 de setembro de 2009, aquando da criação da Lei nº 119/2009 – a Lei do Cibercrime. Tal lei, como disposto no seu artigo 1º, tem como objeto "*(...) as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte eletrónico (...)"*. Tal lei, embora erroneamente considerado inicialmente pelos aplicadores do direito, tem como escopo aplicativo a totalidade dos crimes que se encontram tipificados como tal pela lei portuguesa, não se limitando àqueles que estão previstos na própria Lei do Cibercrime – consubstancia, assim, um regime geral de obtenção de prova em suporte eletrónico.

A Diretiva nº 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, regulou a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, que, por sua vez, ao ser transposta para a legislação nacional, deu origem à Lei nº 32/2008. Tal diretiva visava essencialmente uma harmonização legislativa[28] respeitante à obrigação de conservação de dados que recai sobre os fornecedores deste tipo de serviços, desde logo porque tal poderia abrir portas a uma resposta mais eficaz e adequada à cibercriminalidade,

[28] Tal necessidade de harmonização urgiu com a constatação de que, ao abrigo da exceção prevista no artigo 15º, nº1, da Diretiva 2002/58, os Estados-Membros estavam a instituir obrigações de conservação de dados com uma extensão muito distinta. Expressão clara disso é o facto de o prazo de conservação que havia sido exigido na Irlanda ser de 4 anos, enquanto nos Países Baixos essa durava uns meros 3 meses.

mas também de forma a permitir que o mercado interno de comunicações eletrónicas fluísse – algo que iria ser conturbado caso as obrigações que recaíssem sobre os diferentes fornecedores não fossem as mesmas.

Então, assumindo que a prova digital será toda a informação passível de ser extraída de um dispositivo, computador, sistema informático ou, ainda, sistema de comunicação, é indiscutível a importância que esta assume face aos meios de prova "tradicionais", desde logo porque vivemos "*num momento histórico em que a localização, as preferências, o círculo de amizades, as conversações, os elementos de trabalho, as fotografias, os vídeos, são dados recolhidos e armazenados pelos sistemas informáticos"*[29]. É sabido que, no nosso ordenamento jurídico-processual penal, o direito probatório assume relevância supra, o que é evidente desde logo pela criação de um livro inteiramente direcionado à prova no atual Código de Processo Penal, o que expôs uma preocupação crescente do legislador em reunir todas as disposições com vista a facilitar a sua interpretação e aplicação. Porém, tal centralidade, que é desejável e benéfica para aplicação adequada e eficaz do direito positivo, foi abandonada no que respeita à prova digital. Existem, como referido, no ordenamento jurídico português, três diplomas legais relativos à obtenção de prova digital, que são: o Código de Processo Penal, a Lei nº 115/2009 – Lei do Cibercrime e a Lei nº 32/2008 – Lei 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.

Uma das justificações apontadas para esta perda de centralidade prendeu-se com a especificidade deste tipo de criminalidade. Contudo, tal argumento não deve proceder, desde logo porque o Código de Processo Penal tem sofrido, nos últimos tempos, variadas alterações. O facto da obtenção de prova digital se encontrar dispersa em três documentos legislativos leva a que se apurem incongruências e incompatibilidades que dificilmente se resolvem sem uma intervenção legislativa coesa[30]. Aliás, esta confusão normativa levanta uma série de dúvidas, nomeadamente quanto à relação que se estabelece entre os diversos instrumentos. Com especial relevância assume-se, imediatamente, a divergência doutrinal e jurisprudencial que existe sobre a relação que se deve estabelecer entre a Lei nº 32/2008 e a Lei nº 119/2009.

[29] SILVA, Flávio Manuel Carneiro, "*Apreensão e utilização processual de meios de prova existentes em material informático",* p. 13.
[30] MESQUITA, Paulo Dá, "*Processo Penal, Prova e Sistema Judiciário*", p. 101.

2. A Lei nº32/2008

A Lei nº 32/2008, de 17 de julho, como já referido anteriormente, resultou do processo de transposição para o ordenamento jurídico português da Diretiva 2006/24 CE, do Parlamento Europeu e Conselho, de 15 de março, visando um regime de conservação genérica de dados que fossem gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou redes públicas de comunicações, tendo em vista a deteção, investigação e repressão de crimes graves. Os dados que são conservados ao abrigo desta lei serão os dados de tráfego e os dados de localização (art. 1º/ a), 4º da Lei nº 32/2008), sendo expressamente afastada a possibilidade de conservação dos dados que traduzam o teor da comunicação pelo art. 1º/2 desta mesma lei. Importa salientar, ainda, que a entidade responsável pelo controlo e fiscalização da aplicação desta lei é a Comissão Nacional de Proteção de Dados (CNPD), como expresso no artigo 8º da Lei nº 32/2008.

No que respeita a dados informáticos e comunicacionais, é tradicionalmente feita a distinção entre três categorias: dados de base, dados de conteúdo e dados de tráfego[31]. Esta diferenciação tem na sua base a perceção de que nem todos os tipos de dados gerados no mundo digital deverão ser objeto da mesma tutela constitucional e legal do sigilo das telecomunicações. A categoria que aqui assume especial relevo é a dos dados de tráfego, sendo, porém, a sua definição perturbada pela tríade legislativa que regula a prova digital, desde logo porque a definição entendida para a Lei nº32/2008 não corresponde totalmente àquela do artigo 2º da Lei do Cibercrime. A Lei do Cibercrime considera como dado de tráfego os "*dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente"*. Por sua vez, a Lei nº 32/2008 remete esta definição para a Lei da Proteção de Dados Pessoais e Privacidade nas Telecomunicações (Lei nº 41/2004, de 14 agosto), como expresso no artigo 2º/2 da Lei nº 32/2008, que considera como dado de tráfego "*quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos de faturação da mesma",* bem como contém a definição dos dados de localização, que serão *"quaisquer*

[31] Parecer da Procuradoria-Geral da República nº16/94/complementar de 02/05/1996, p. 9

dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público" (art. 2º/1 d) e e) da Lei nº 41/2004).

Assim, partindo da noção que é pressuposta pela Lei nº 32/2008, os dados de tráfego e de localização ficam conservados durante o prazo de um ano a contar da data da conclusão da comunicação, sendo destruídos findo esse prazo (art. 6º e 7º/1 e) da Lei nº 32/2008). Porém, relativamente a este prazo, assume especial importância realizar um breve confronto entre esta conservação genérica de dados e a disposição processual prevista no artigo 12º da Lei do Cibercrime – preservação expedita de dados – e ver como se relacionam.

A preservação expedita de dados (ou *quick freeze*) consubstancia aqueles casos em que é emitido um pedido de preservação de dados específicos dirigido a quem sobre estes tenha disponibilidade ou controlo. Tal ordem tem o prazo de três meses, mas, de acordo com o disposto no nº 5 do art. 12º da Lei do Cibercrime, esse prazo pode ser prorrogado por outros três meses até ao máximo de um ano. Por sua vez, a conservação de dados traduz-se na conservação de dados de tráfego e de localização de todos os cidadãos, sendo uma ordem subjetivamente indiscriminada. Serem conservados pelo prazo de um ano tem como objetivo serem uma garantia de disponibilidade deste tipo de dados às autoridades judicantes que possam vir a precisar deles no decurso de uma ação penal que vise investigar crimes graves[32], segundo a Lei nº 32/2008. Assim, são dois instrumentos processuais que ocupam espaços diferentes e cuja existência deve ser complementada. No que respeita à afirmação da complementaridade que se impõe entre ambos os regimes, podemos apontar um acórdão do tribunal constitucional alemão, o qual foi chamado a pronunciar-se por alegação de que as normas introduzidas na Lei das Telecomunicações por força de implementação da Diretiva 2006/24 seriam inconstitucionais por violação do artigo 10º da Lei Básica – que consagra o

[32] A definição de crime grave na Lei nº 32/2008 não é a mesma definida pelo Código de Processo Penal no âmbito das escutas telefónicas (art. 187º/1 CPP) – o que consubstancia mais um ponto de conflito gerado pela dispersão legislativa relativa à obtenção de prova digital. Para efeitos de acesso aos dados conservados ao abrigo da Lei nº 32/2008, os crimes que legitimam o recurso a este tipo de dados são: "*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, 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 de contrafação e crimes abrangidos por convenção sobre a segurança da navegação aérea ou marítima"* (art. 2º/1 g) da Lei n 32/2008 atualizado pela Lei nº 79/2021).

direito ao sigilo da correspondência, comunicação postal e da telecomunicação. Ressalta que as restrições ao direito ao sigilo das comunicações são admitidas desde que proporcionais e subordinadas à proteção de objetivos considerados legítimos. É aquando da análise da idoneidade da medida que a confronta com o mecanismo de preservação expedita de dados, referindo: "*(...) Tal procedimento apenas pode obter a preservação de dados prévios ao pedido caso estes existam, pelo que não é tão eficaz quanto a conservação contínua, a qual garante a disponibilidade da totalidade dos dados relativos aos últimos seis meses"*[33].

A Lei nº 32/2008 é a única lei que consagra um regime de conservação de dados para efeitos de auxílio da ação penal e, nos tempos que correm, é indubitável a importância que assume um instrumento processual desta natureza, desde logo porque: o legislador ao consagrar determinado comportamento como ilícito criminal, se não criar, subjacente àquele, os meios adequados para chamar esses atores ao processo, o efeito dissuasor que provoca será bastante limitado, podendo criar insuportáveis vazios de punição. Para além deste aspeto de suma relevância, é importante ressaltar que, atendendo às especificidades da prova digital, assume, como referido, um papel de garantia para as entidades responsáveis pela condução do processo-crime, uma vez que contam com o armazenamento de determinados dados, podendo ser muito importantes para a investigação, durante um determinado período.

A consagração de um regime de conservação genérica de dados de tráfego e de localização encontra-se em diálogo (ou melhor, discussão) constante com os direitos fundamentais dos cidadãos, especialmente na questão da compatibilização da intrusão estadual na esfera de direitos pessoais e inalienáveis de todos os cidadãos europeus. Tal ingerência deve ser devidamente precavida, pois os dados sobre os quais a obrigação de conservação incide são particularmente sensíveis[34]. A Diretiva 2006/24/CE, a base da Lei nº 32/2008, tem sido objeto de intenso conflito, tendo vindo já a ser declarada inválida pelo Tribunal de Justiça da União Europeia – análise aprofundada infra-, por se considerar que a

---

[33] PINHO, Carlos, ob. cit. p. 180 e https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2010/03/rs20100302_1bvr025608en.html;jsessionid=1E448A82DA6A4A5C3FB65524723990C0.2_cid361

[34] *"Estes dados, considerados no seu todo, são suscetíveis de permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais e os meios sociais frequentados"*, Acórdão do Tribunal de Justiça da União Europeia de 8 de abril de 2014, ponto 27 do Acórdão *Digital Rights Ireland* (p. 15).

mesma não acautela com o cuidado exigido, essencialmente, o direito constitucionalmente consagrado de respeito pela vida privada e familiar (art. 26º/1 CRP) e de sigilo das comunicações (art. 34º CRP).

a. Acórdãos do Tribunal de Justiça da União Europeia

Neste ponto, importa analisar pormenorizadamente a Diretiva 2006/24/CE do Parlamento e do Conselho Europeu, de 15 de março de 2006, 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. Porém, antes de prosseguir, é importante fazer uma breve referência ao papel que as diretivas assumem no âmbito do direito da União Europeia. De acordo com o artigo 288º do Tratado de Funcionamento da União Europeia, juntamente com os regulamentos, as decisões, as recomendações e pareceres, as diretivas são fontes de direito secundário ou derivado e consubstanciam um instrumento através do qual se visa obter a harmonização e coordenação dos direitos internos de cada Estado Membro. As diretivas, por sua vez, fixam os objetivos que devem ser atingidos, mas concedem uma ampla margem de liberdade a cada Estado-Membro sobre os meios e formas pelas quais pretendem realizar essa transposição – consagração de uma ampla liberdade de conformação normativa[35]. São fontes de direito comunitário que, ao contrário do que acontece com os regulamentos[36], carecem de um ato nacional de incorporação no direito interno.

Como referido anteriormente, a Diretiva 2006/24/CE surgiu no âmbito do combate ao terrorismo e à criminalidade organizada e veio a derrogar o regime de confidencialidade das comunicações que havia sido consagrado na 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. Esta diretiva, aquando da sua criação, transpôs regras específicas do setor das comunicações eletrónicas que se

[35] Estritamente relacionada a esta liberdade de conformação normativa encontra-se a competência para levar a cabo a ponderação visada neste âmbito: entre os direitos fundamentais em causa e as medidas impositivas da conservação de dados por parte das operadoras de telecomunicações. A Provedora de Justiça, no pedido de fiscalização abstrata da constitucionalidade que emitiu, no ponto 20º e 21º, trata, justamente, da questão da competência jurisdicional para decidir o caso *sub judice*. Concluiu-se, porém, que havia sido atribuída ao legislador nacional uma ampla margem de discricionariedade, pelo que não se poderia considerar a Lei nº 32/2008, de 17 de julho, como um ato "inteiramente determinado" pelo direito da União Europeia.

[36] *"(...) O regulamento tem caráter geral. É obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros. A diretiva vincula o Estado-Membro destinatário quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios. (...)",* Artigo 288º do TFUE.

encontravam já estipuladas na Diretiva 95/56/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

O regime da confidencialidade previsto no artigo 5º da Diretiva 2002/58/CE impõe que: "*Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis. (…) O presente número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade"*, sendo complementado com o disposto no artigo 6º: "*(…), os dados de tráfego relativos a assinantes e utilizadores tratados e armazenados pelo fornecedor de uma rede pública de comunicações ou de um serviço de comunicações eletrónicas publicamente disponíveis devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação"*. Neste último artigo, consagra-se uma limitação a este regime de confidencialidade, ao estabelecer que os dados de tráfego podem ser objeto de tratamento por parte dos prestadores deste tipo de serviços para efeitos de faturação e de pagamento de interligações (nº2), bem como com vista a comercialização dos seus serviços e fornecimento de serviços de valor acrescentado (nº3). Não obstante, o tratamento previsto no nº3 está subordinado à verificação de duas condições cumulativas: que o tratamento se limite à medida e tempo necessário e que o assinante ou utilizador tenha consentido nesse mesmo tratamento.

A derrogação do regime da confidencialidade dos dados pessoais dos utilizadores e assinantes deste tipo de serviços foi consagrada à luz do artigo 15º da Diretiva 2002/58/CE, que veio a reiterar o disposto no artigo 13º da Diretiva 95/46/CE. De acordo com esta disposição, os Estados-Membros estão autorizados a restringir o âmbito das obrigações e direitos consagrados naqueles diplomas sempre que tal se demonstre necessário, adequado e proporcionado para salvaguardar uma série de interesses que são, exaustivamente, descritos no preceito, dentro dos quais encontramos a proteção da segurança nacional e pública, bem como a deteção, investigação e repressão de infrações penais. Inclusivamente, no final deste preceito, refere-se a possibilidade de os Estados procederem à conservação dos dados durante um determinado período de tempo. Consagra, então, a possibilidade de

limitação dos direitos salvaguardados pelas Diretivas 95/46/CE e [Diretiva] 2002/58/CE sob o manto da necessidade, adequação e proporcionalidade.

Foi com base neste preceito que se consagrou a conservação generalizada dos dados de tráfego e de localização que sejam gerados ou tratados no âmbito de oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, desde logo, por se aferir a importância do contributo que uma conservação deste género poderia assumir para as entidades investigatórias.

A 8 de abril de 2014, foi emitido, pelo Tribunal de Justiça da União Europeia, o Acórdão *Digital Rights Ireland* que concluiu, em resposta às questões prejudiciais[37] colocadas pela Irlanda e pela Áustria, a invalidade da Diretiva 2006/24/CE. As questões prejudiciais em causa tinham como objeto a validade da Diretiva 2006/24/CE e o TJUE começou por apreciar a sua validade à luz dos artigos 7º, 8º e 11º da Carta de Direitos Fundamentais da União Europeia (CDFUE) – direito ao respeito pela vida privada e familiar, proteção de dados pessoais e a liberdade de expressão e informação, respetivamente. Importa relembrar que o artigo 52º da CDFUE impõe que qualquer restrição que se realize dos direitos fundamentais dos cidadãos europeus deve proteger o núcleo essencial destes e orientar-se pelo princípio da proporcionalidade, pelo que tais medidas têm de ser necessárias, adequadas e proporcionais a prosseguir objetivos de interesse geral comunitário.

A Diretiva 2006/24/CE enuncia no seu considerando, mas também no artigo 1º, que a conservação generalizada de dados que impõe tem em vista o combate à criminalidade organizada, o que consubstancia, evidentemente, um objetivo de interesse geral da União. Aliás, no termo do ponto 42 do acórdão em análise, refere-se que o artigo 6º da CDFUE consagra não só o direito à liberdade como também o direito à segurança.

Partindo para o conteúdo da diretiva em causa, se esta passa no crivo da adequação e necessidade, ao permitir a conservação de dados cruciais para o desenrolar da investigação numa realidade facilitadora do anonimato, já no que respeita à sua proporcionalidade o TJUE apontou inúmeras falhas. Este princípio deve ser interpretado no sentido de que *"(...) os atos*

[37] O reenvio prejudicial (art. 267º do TFUE) consubstancia um mecanismo de controlo judicial indireto ou de colaboração na administração da justiça, mediante o qual os tribunais nacionais colocam questões de interpretação e validade das normas comunitárias ao Tribunal de Justiça da União Europeia. Este último não tem como função decidir o caso concreto, mas tão só esclarecer o órgão judicante nacional relativamente à interpretação e validade daquela mesma norma.

das instituições da União sejam adequados à realização dos objetivos legítimos prosseguidos pela regulamentação em causa e não excedam os limites do que é adequado e necessário à realização desses objetivos"[38]. A diretiva em causa devia ponderar e procurar compatibilizar a proteção dos dados pessoais dos utilizadores e assinantes destes serviços com a amplitude da ingerência em causa e, na verdade, não procedeu à criação de regras claras e precisas quanto à conservação que impunha. Consagrou a conservação de todos os dados de tráfego e de localização (bem como todos os dados conexos para identificar o agente em causa) de todos os meios de comunicações eletrónicas realizados por todos os cidadãos europeus. O TJUE concluiu pela falta de uma série de limites que considerava imprescindíveis para que se pudesse apurar a proporcionalidade da medida, desde logo critérios objetivos que limitassem o acesso das autoridades nacionais competentes, não estabelecendo requisitos objetivos para a definição do prazo, nem garantias suficientes no respeitante à segurança e proteção dos dados em causa. Por fim, critica ainda a inexistência de uma obrigação de conservação dos dados em território comunitário e de destruição definitiva desses no termo do período de conservação que seja fixado nas legislações nacionais, concluindo-se, assim, pela invalidade da Diretiva 2006/24/CE de 15 de março.

A par do Acórdão *Digital Rights Ireland*, encontramos o Acórdão *Tele Sverige2 AB* de 21 de dezembro de 2016 e que visou responder a questões prejudiciais colocadas pelo Kammarratten i Stockholm (Tribunal Administrativo de Segunda Instância de Estocolmo) e pela Court of Appeal (Tribunal de Segunda Instância de Inglaterra e País de Gales). No âmbito deste processo também foram colocadas dúvidas interpretativas da diretiva, nomeadamente no sentido da compatibilização do artigo 15º da Diretiva 2002/58 à luz os artigos 7º, 8º, 11º e 52º da CDFUE com uma obrigação de conservação generalizada de dados, bem como se abordou o impacto do Acórdão *Digital Rights Ireland* nas regulamentações legislativas nacionais neste âmbito.

No que respeita à compatibilização do artigo 15º da Diretiva 2002/58, interpretado à luz do art. 7º, 8º, 11º e 52º da CDFUE, com uma conservação generalizada dos dados de tráfego e de localização, o Tribunal de Justiça da União Europeia reforça a posição que havia sido construída no Acórdão *Digital Rights Ireland*. Reforçando a necessidade imposta pelo princípio da proporcionalidade de que as limitações aos direitos e obrigações consagrados

[38] Ponto 46 do Acórdão *Digital Rights Ireland*.

na Diretiva 2002/58 e [Diretiva] 95/46 se limitem ao estritamente necessário, relembra a sensibilidade do tipo de dados em causa que permitem, inclusivamente, *"(...) determinar (...) o perfil das pessoas em causa, informação tão sensível à luz do direito ao respeito da privacidade, como o conteúdo das próprias comunicações"*[39]. Reforça ainda que a letra da lei, ao abrir caminho para a criação de exceções à regra da confidencialidade dos dados, visa criar exatamente isso: exceções. Defende uma interpretação estrita do artigo 15º da Diretiva 2002/58, de forma a evitar que a conservação dos dados pessoais dos utilizadores ou assinantes daquele tipo de serviço assumam esta como a regra. Responde à primeira questão no mesmo sentido que o acórdão *Digital Rigths Ireland*, entendendo que a medida de conservação de dados de tráfego e de localização de todos os cidadãos europeus, enquanto utilizam todos os meios de telecomunicação, extravasa a medida do estritamente necessário, reforçando as propostas que haviam sido redigidas pelo TJUE a 8 de abril de 2014[40].

A segunda parte do acórdão aborda essencialmente a possibilidade de criar um instrumento processual de conservação dos dados de tráfego e de localização que seja compatível com esta abertura proporcionada pelo artigo 15º da Diretiva 2002/58. Um regime de conservação de dados pessoais de cidadãos europeus, dotados da sensibilidade já explicitada, impõe que o acesso a eles seja limitado ao estritamente necessário, que sejam obrigatoriamente conservados em território da União Europeia e, para além disso, que se justifique à base de um interesse geral comunitário – um dos exaustivamente enunciados na Diretiva 2002/58. Aquando a abordagem da questão de acesso aos dados conservados, o TJUE considerou que as entidades competentes pela investigação, em princípio, só deveriam ter acesso àquele tipo de dados relativamente a *"(...) pessoas suspeitas de terem planeado, de estarem a cometer ou de terem cometido uma infração grave ou ainda de estarem envolvidas de uma maneira ou de outra numa infração deste tipo"*[41], abrangendo, reflexamente, os dados de pessoas que, objetivamente, possam contribuir favoravelmente para o desenrolar da investigação. Considera que só o combate à criminalidade grave justifica uma medida deste género e reforça a necessidade de impor a fiscalização dos

[39] Ponto 99 do Acórdão *Tele2 Sverige AB*.
[40] Criação de medidas claras e precisas que regulem o âmbito e aplicação da medida de conservação de dados, desde logo a nível da estipulação de critérios objetivos que permitam estabelecer uma relação entre os dados a conservar e o objetivo em vista, delimitação do público visado e das situações abrangidas, entre outras.
[41] Ponto 119 do Acórdão *Tele2 Sverige AB*.

pedidos realizados pelas entidades interessadas por parte de uma autoridade administrativa independente ou de um órgão jurisdicional.

Embora ambas as decisões do TJUE tenham ido no mesmo sentido – o da desproporcionalidade da medida em causa e, como tal, pela sua invalidade-, proferiu-as como resposta a envios prejudiciais que os Estados-Membros requereram e, como tal, a Diretiva em causa continua eficaz – a declaração de invalidade não acarreta a imediata destruição do ato. A decisões têm efeito de caso julgado no caso concreto, ficando somente os Estados parte do processo vinculados a essa decisão[42].

b. Argumentos a favor da inconstitucionalidade

Terminada a análise dos acórdãos do TJUE mais relevantes relativamente à Diretiva 2006/24/CE, importa analisar que repercussões tais decisões tiveram no nosso ordenamento jurídico, essencialmente na Lei nº32/2008.

Neste ponto, assume especial pertinência avaliar as posições assumidas pela Comissão Nacional de Proteção de Dados (CNDP), entidade administrativa independente responsável pela fiscalização da aplicação do diploma legal em causa e por instituir os processos contraordenacionais necessários, e da Provedora de Justiça, Maria Lúcia de Amaral. Em 2017, a CNPD emitiu a Deliberação nº 1008/2017, na qual determina que, a partir daquele momento, deixará de aplicar a lei nos casos que lhe sejam submetidos e, para tal, acaba por subscrever os argumentos que haviam sido enunciados pelo TJUE no acórdão *Digital Rights Ireland* e, posteriormente, no *Tele Sverige2 AB*. Porém, importa não acusar a CNPD de ter sido imprudente ou demasiado radical, uma vez que a mesma já havia, a 29 de abril de 2014, chamado a atenção da Assembleia da República para os moldes do regime estatuído pela lei em causa, em audição na Comissão dos Assuntos Constitucionais, Direitos,

[42] Neste sentido, CORREIA, João Conde, *"Prova Digital: as leis que temos e a lei que devíamos ter"*, p. 38. Em sentido contrário, afigura-se Silva Ramalho e Duarte Coimbra. Estes autores lançam mão de um acórdão do TJUE (Acórdão *Internacional Chemical Corporation*), uma vez que este, na sua argumentação, expôs que "*(...) a invalidade de um ato de uma instituição (...), ainda que apenas se dirija diretamente ao órgão jurisdicional que colocou a questão ao TJ, constitui razão suficiente para qualquer outro órgão jurisdicional considere tal ato inválido para o efeito de uma decisão que deva tomar (...)"*. Assim, estes autores defendem que a declaração de invalidade da totalidade da Diretiva 2006/24 pelo TJUE assume eficácia erga omnes, com base em valores de coerência e harmonização que são tão valorizados no âmbito do direito comunitário. (RAMALHO, David Silva e COIMBRA, José Duarte, *"A declaração de invalidade da Diretiva 2006/24: presente e futuro da regulação sobre a conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves"*, p. 1020).

Liberdades e Garantias, bem como concluiu na Deliberação nº 641/2017[43] com a recomendação de revisão da Lei nº 32/2008, de 17 de julho. Neste sentido, pronunciou-se também a Provedora de Justiça em 2019, tendo iniciado o ano com uma recomendação de alteração do regime imposto relativamente à conservação de dados[44] e, em agosto, requerido ao Tribunal Constitucional a fiscalização abstrata da constitucionalidade do artigo 4º, 6º e 9º da lei em análise[45].

Previamente a um aprofundamento dos argumentos invocados por estas entidades a favor da inconstitucionalidade dos artigos 4º, 6º e 9º da Lei nº 32/2008, importa salientar os direitos que estão, essencialmente, aqui em causa: o direito ao sigilo das comunicações (art. 34º CRP), o direito à reserva da intimidade da vida privada e familiar (art. 26º CRP) e, por fim, o direito a uma tutela jurisdicional efetiva (art. 20º CRP).

Na esteira da posição sufragada pelos juízes do TJUE, também a CNPD e a Provedora de Justiça se manifestaram no sentido da invalidade da Diretiva que originou a Lei nº 32/2008 e na consequente necessidade da sua de revisão. Em consonância com os acórdãos *Digital Rights Ireland* e *Tele Sverige2 AB*, é apontada a desproporcionalidade da obrigação de conservação e armazenamento de dados impostos às empresas de telecomunicações, a incompreensão relativa ao prazo eleito pelo legislador nacional e, por fim, a imprecisão na definição das medidas destinadas a garantir um elevado nível de segurança e proteção dos dados. Previamente, a Provedora de Justiça esclarece que a competência para avaliar a conformidade da lei transposta com as exigências que derivam da Carta, desde logo na "*ponderação entre as razões de interesse público que poderiam determinar a conservação e armazenamento de dados por parte das operadoras de telecomunicações e a tutela de direitos fundamentais*"[46], é da jurisdição constitucional nacional, pelo facto de ter sido atribuída ao legislador português uma ampla margem de conformação do regime de conservação de dados cujos aspetos cruciais derivaram da Diretiva 2006/24/CE[47].

---

[43] Ambas as deliberações enunciadas disponíveis em: https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2017&type=2&ent=

[44] https://www.provedor-jus.pt/documentos/Rec_1B2019_2019_01_22_Recomendacao_da_Protecao_de_dados_Ministra_Justica.pdf

[45] https://www.provedor-jus.pt/documentos/q-7746-2017/

[46] Ponto 20º do pedido de fiscalização abstrata da constitucionalidade dos artigos 4º, 6º e 9º da Lei nº 32/2008.

[47] Em sentido contrário, no respeitante à competência para proceder à análise e regulação da matéria em causa, afirmam-se Alessandra Silveira e Pedro Miguel Freitas. Estes autores defendem que a entidade competente

Relativamente ao primeiro ponto, certo é que o legislador português adotou o regime que havia sido expressamente censurado por parte da jurisprudência comunitária analisada[48]: estatuiu um regime de conservação generalizada e indiscriminada de dados de tráfego e de localização, bem como dos anexos necessários à identificação do utilizador, de todos os cidadãos europeus mediante a utilização de todos os meios de telecomunicações. No que respeita à amplitude subjetiva da medida em causa, importa salientar que a Lei nº 32/2008 prescindiu da imposição de uma ligação, direta ou indireta, do titular dos dados a uma infração grave. Porém, embora não tenha definido uma qualidade subjetiva que coartasse a quantidade de dados a serem conservados pelas operadoras de telecomunicações, o legislador português estatuiu que só se poderia ter acesso aos dados dos sujeitos previstos no artigo 9º/3 da Lei nº 32/2008. Para além deste aspeto, o legislador português não acautelou com a devida atenção a relevância do sigilo profissional[49], não dispensando da "nuvem" de dados conservados aqueles que pertencem a profissionais subordinados àquele dever – dever constitucionalmente consagrado como inviolável.

Assim, para além de impor a conservação indiscriminada dos dados de localização e de tráfego de todos os portugueses, evidenciou-se a sensibilidade dos dados em causa, a Provedora de Justiça realçou *"a quantidade e qualidade da informação que por seu intermédio se poderá vir a obter: desde que a pessoa transporte consigo o seu telemóvel ou outro dispositivo eletrónico de acesso à internet, sempre será possível reconstituir aqueles que foram, ao longo do período de um ano, todos os lugares em que esteve, quanto tempo esteve em cada um desses lugares e, cruzando esta informação com dados respeitantes a*

---

para proceder à correção dos vícios constatados pelo TJUE é, não o legislador nacional, mas sim o legislador europeu. Se for o legislador nacional de cada Estado-Membro tal *"mina a efetividade do direito da União, compromete a homogeneidade da sua aplicação nos distintos Estados-Membros, e provoca diferenciações de tratamento injustificadas entre os cidadãos europeus em matéria de proteção dos seus direitos fundamentais"* (SILVEIRA, Alessandra e FREITAS, Pedro Miguel, *"Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos Estados-Membros da EU: uma leitura jusfundamental*", p. 58).

[48] Acórdão *Tele Sverige2 AB: "O artigo 15º, nº1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho (...) deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica*", ponto 1 da conclusão do acórdão.

[49] O sigilo profissional surge como uma garantia constitucional do direito do sigilo da correspondência, uma vez que este direito, para além de impor a abstenção da generalidade da população relativamente a comunicações que não lhe são dirigidas, visa garantir que "*terceiros que a elas tenham acesso não as divulguem*" – CANOTILHO, J.J. Gomes, MOREIRA, Vital, *"Constituição da República Portuguesa Anotada"*, p. 545.

outras pessoas, com quem esteve, onde e quando"[50]. A sensibilidade dos dados em causa é, ainda, evidenciada ao analisarmos qual a sua qualificação perante Regulamento Geral de Proteção de Dados da União Europeia (RGPD), o que pode demonstrar-se particularmente pertinente na medida em que se trata aqui de um tratamento automatizado dos dados pessoais dos cidadãos. O artigo 9º do regulamento em causa enumera que tipo de dados considera merecerem um tratamento especial face aos restantes, encontrando-se, entre outros, dados que revelem as opiniões políticas, convicções religiosas, bem como dados indicativos do estado de saúde dos indivíduos. A Provedora de Justiça, no ponto 77º do pedido de fiscalização abstrata que direcionou ao Tribunal Constitucional (TC), ao alertar para a capacidade de informação que era cognoscível a partir dos dados de tráfego e de localização salientou o facto de que estes permitem, justamente, "*inferir, com precisão, informações detalhadas sobre (...) inclinações político-partidárias, bem como aspetos da vida pessoal, tais como rotinas, hobbies e vulnerabilidades (por exemplo, em matéria de saúde)*". Se o tratamento dos dados em causa (pela capacidade de aferir dados considerados sensíveis para efeitos do RGPD) é totalmente afastado pelo nº1, já o nº2 vem enumerar as situações em que tal impedimento é levantado e, na alínea g), encontramos a possibilidade de tratar os dados sempre que tal for necessário por motivos de interesse público comunitário ou nacional, sujeitando, novamente, tal limitação ao princípio da proporcionalidade e impondo a adoção de medidas adequadas, nomeadamente a tutelar o núcleo essencial dos direitos. Ou seja, o tratamento dos dados em causa, por estarem intrinsecamente conexionados com direitos e liberdades fundamentais dos assinantes e utilizadores, deve obedecer às estritas condições constitucionalmente impostas para a limitação dos direitos que lhe são inerentes e o RGPD vem, por sua vez, reforçar a necessidade do seu cumprimento. Estamos, assim, perante dados que, para além de indubitavelmente pessoais de acordo com a definição depositada no artigo 4º, nº1 do RGPD, podem ser considerados, a este nível, particularmente sensíveis.

Neste mesmo documento, ainda se ressalta o sentimento de permanente vigilância que os cidadãos sentem por parte do Estado, o que se revela consequentemente nas suas ações, desde logo no exercício do seu direito à autodeterminação comunicacional. O direito à autodeterminação comunicacional deriva da incontornável sociabilidade que é associada ao ser humano, isto é, o Homem cresce e desenvolve-se em relação com os outros e estas

[50] Ponto 58º do pedido de fiscalização abstrata da constitucionalidade cit. supra.

relações devem ser protegidas. Repetindo o anteriormente dito, com a evolução tecnológica e científica que se vive nos dias de hoje, tais relações transpuseram-se, em grande parte, para a esfera digital e, como tal, são realizadas com a mediação de um terceiro – o fornecedor de serviços de comunicação. O direito à autodeterminação comunicacional, como referido no Acórdão nº 403/2015 do Tribunal Constitucional[51], assume-se como "*um direito de liberdade, liberdade de comunicar, sem receio ou constrangimentos de que a comunicação ou as circunstâncias em que a mesma é realizada possam ser investigadas ou divulgadas"*[52]. Ao propagar-se um ambiente de vigilância contínua por parte das operadoras a cada um dos cidadãos, é indubitavelmente afirmada a afetação desta liberdade de comunicar, quando o que se devia procurar atingir era conferir às comunicações eletrónicas a mesma segurança e confiança que nas comunicações realizadas "frente a frente".

Terminada a exposição dos motivos pelos quais se considera a medida de conservação generalizada dos dados gerados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações desproporcional, foram apontadas algumas propostas de como tornar a medida proporcional aos fins a que se propõe. As sugestões que foram referenciadas pela Provedora de Justiça, que haviam sido subscritas pela CNPD e já referidas no Acórdão *Digital Rights Ireland* e *Tele2 Sverige AB,* prendem-se com a necessidade de adotar critérios objetivos que permitam coartar os dados que são conservados pelas operadoras de telecomunicações, desde logo com base numa zona geográfica ou espaço temporal determinado, bem como pode ter em conta um círculo de pessoas que possam, efetivamente, estar implicadas na preparação ou prática das infrações graves que se visam combater.

Um segundo aspeto que é comummente criticado é relativo às medidas que visavam estabelecer elevados nível de segurança instituídas pela Lei nº32/2008. Não obstante também tenha sido uma matéria criticada relativamente à Diretiva 2006/24/CE, o legislador nacional foi mais cauteloso na regulação das medidas relativas à segurança e proteção dos dados em causa – como se verá posteriormente. É crucial, para a determinação das medidas organizativas e técnicas necessárias, que se tenha em conta a quantidade, bem como a qualidade dos dados em causa, mas também o incomensurável risco de acesso ilegítimo,

[51] Processo nº 773/15 de 17 de setembro.
[52] Ponto 13 do acórdão citado.

pois, no fundo, esta lei acaba por impor o armazenamento de dados pessoais de cada indivíduo num único "sítio".

Não obstante, embora o legislador nacional tenha salvaguardado algumas das críticas apontadas pelo TJUE, não as sanou totalmente. A Provedora de Justiça, bem como a CNPD, vêm a criticar o facto de a Lei nº32/2008 não ter, à semelhança da diretiva que a originou, uma disposição que expressamente obrigue a conservação dos dados em território da União Europeia e, para além deste aspeto, ressalva-se ainda a falta da consagração de um dever, direcionado às autoridades competentes que tenham acesso aos dados concretos, de alertar os visados do acesso aos seus dados. Aliás, é justamente com base na carência desta imposição que a Provedora de Justiça alega a violação do direito ao acesso a uma tutela jurisdicional efetiva – direito constitucionalmente consagrado no artigo 20º/1 da CRP. O direito de acesso ao direito e tutela jurisdicional efetiva é, como referido por Gomes Canotilho e Vital Moreira, "*uma norma-princípio estruturante do Estado de Direito democrático (...) e de uma Comunidade de Estados (União Europeia) informada pelo respeito dos direitos do homem, das liberdades fundamentais e do Estado de Direito"*[53]. Tal direito abarca um conjunto amplo de direitos conexos e pode ser densificado com recurso a outros princípios, nomeadamente o direito de defesa e o direito ao contraditório. O princípio do contraditório, enquanto princípio de prossecução processual, impõe que o mesmo se desenrole de forma a expor os motivos da acusação e da defesa, bem como institui que os sujeitos processuais devem poder participar constitutivamente na declaração do direito no caso[54]. Parece claro que, se a lei é silenciosa relativamente ao estabelecimento de um dever de informar o visado de que as autoridades competentes pela investigação criminal tiveram acesso a dados pessoais seus, afeta "*não apenas a possibilidade de se vir a conhecer a informação que, a respeito de cada um, obteve a autoridade pública, mas ainda a faculdade de reação e defesa contra eventuais acessos ilegítimos a essa mesma informação"*[55].

Importa, ainda, evidenciar que o nível de proteção e segurança que seria exigido tendo em conta os aspetos da vida pessoal de cada pessoa que são possíveis aferir com base naqueles mesmos dados são postos em causa diariamente pelo facto de a CNPD ter deixado, como acordado na Deliberação nº 1008/2017, de aplicar a lei nos casos que lhe sejam

[53] CANOTILHO, J.J. Gomes, MOREIRA, Vital, ob. cit. p. 409.
[54] ANTUNES, Maria João, ob. cit., p. 78.
[55] Ponto 94º do pedido de fiscalização da constitucionalidade.

submetidos para apreciação, justificando a sua decisão com base num juízo de violação por parte da Lei nº 32/2008 do conteúdo da CDFUE e CRP. Ou seja, neste momento, as empresas responsáveis pelos serviços de comunicações eletrónicas publicamente disponíveis e redes publicas de comunicações encontram-se a conservar dados pessoalíssimos dos portugueses sem qualquer tipo de fiscalização ou controlo externo! É de salientar que, embora o legislador nacional tenha restringido o acesso aos dados a "pessoas especialmente autorizadas", não determina qualquer critério que permita determinar ou delimitar quem são essas pessoas, especificando somente, no artigo 8º, nº 2 da Lei nº 32/2008, que as operadoras de telecomunicações "*devem remeter à CNPD, (...), os dados necessários à identificação das pessoas especialmente autorizadas a aceder aos dados*".

O artigo 7º/3 do diploma legal refere que a comunicação dos dados em causa se realizará conforme condições técnicas definidas em portaria. Para tal, foi emitida pelo Ministério da Administração Interna, da Justiça e das Obras Públicas, Transportes e Comunicações a Portaria nº 469/2009[56], diploma que estabeleceu as condições consideradas adequadas a conferir o grau de segurança e proteção devido tendo em conta os direitos em causa. Tal portaria foi alterada e atualmente em vigor encontra-se a Portaria º 694/2010. De entre as várias medidas consagradas, em primeiro lugar importa salientar que estas vieram a instituir que a comunicação eletrónica a que se refere o artigo 7º, nº 3 da Lei nº 32/2008 se fizesse através de uma aplicação informática específica – sistema de acesso ou pedido de dados às operadoras de comunicações (SAPDOC). Para além disso, prevê a obrigatoriedade de aposição de assinatura digital, seja no pedido de acesso a dados, seja no ficheiro de resposta, bem como a encriptação de todas as comunicações que sejam realizadas no âmbito daquele pedido. Consagra, por fim, a necessidade de realização de auditorias de segurança ao funcionamento da aplicação. No geral, tais medidas mostram-se adequadas a garantir o elevado nível de segurança, bem como celeridade no processo que não era permitida pelos meios físicos, que é exigido nestas matérias, porém, importa atentar no artigo 6º-A, introduzido pela Portaria nº 694/2010[57], que trata justamente do período experimental e onde se refere que a utilização da aplicação informática em causa, criada especificamente para a comunicação dos dados de tráfego e de localização, bem como de todos aqueles anexos

---

56 http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1265&tabela=lei_velhas&nversao=1&so_miolo=

57 http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?tabela=leis&nid=1267&pagina=1&ficha=1

necessário para identificar o assinante ou utilizador, é facultativa até a *"disponibilização aos utilizadores das funcionalidades do sistema e quando tal for determinado por despacho conjunto dos membros do Governo responsáveis pelas áreas da administração interna e da justiça*", vindo o nº2 do mesmo artigo explicitar que, durante o periodo experimental, quando não se utilize a aplicação, a transmissão dos dados deve ser realizada mediante os termos gerais, isto é, em CD-ROM, DVD-ROM ou outro suporte digital análogo. A verdade é que, 11 anos após a emissão da última portaria relativa ao modo de comunicação dos dados em causa, inexiste uma portaria que tenha vindo a estabelecer a obrigatoriedade da utilização da aplicação informática. Assim, a utilização da aplicação informática especificamente criada para efeito de comunicação dos dados em causa, com vista a exponenciar a segurança na "viagem" destes mesmos dados, não é, até hoje, obrigatória[58].

Por fim, a terceira grande "falha" apontada à Lei nº 32/2008, de 17 de julho, remete-se justamente à questão do prazo de conservação dos dados de tráfego e de localização que foi definido pelo legislador português. A Diretiva 2006/24/CE fixou uma janela temporal entre os 6 meses e os 2 anos, tendo a Lei nº 32/2008 estatuído o prazo de um ano de conservação dos dados em causa a contar da conclusão da comunicação em causa.

A delimitação de um período de conservação dos dados de tráfego e de localização, bem como de todos os anexos necessários à identificação do utilizador, está subordinada ao princípio da proporcionalidade, uma vez que este vai impor o armazenamento de dados pessoais de todos os portugueses e, como tal, mantê-los suscetíveis de recuperação em caso de necessidade para efeitos investigativos. Para além disso, deve balizar a opção legislativa a consciência da urgência em evitar uma concentração excessiva de dados que permitem, através do cruzamento com outros, "*a reconstituição do passado de cada um*"[59]. Aliás, só atendendo especialmente a esse facto é que se pode concluir pela efetividade do princípio da economia de dados que é, desde logo, imposta pelo legislador comunitário aquando da regulação da proteção de dados – artigo 5º, nº 1, alínea c) do RGPD. Tal princípio visa, essencialmente, subordinar o tratamento de dados pessoais ao princípio da necessidade e, assim, subsumir a conservação desses ao periodo estritamente necessário para o alcance das

[58] https://www.citius.mj.pt/portal/article.aspx?ArticleId=463
[59] Ponto 77º do pedido de fiscalização abstrata da constitucionalidade cit. supra.

finalidades previstas – neste caso, de deteção, investigação e repressão de crimes graves por parte das autoridades competentes.

Assumindo a subordinação ao princípio da proporcionalidade, a Provedora de Justiça, a fim de expor a alegada desproporcionalidade do prazo consagrado no ordenamento jurídico nacional, invocou uma decisão do Tribunal Constitucional Federal Alemão, de 2 de março de 2010[60]. Afigurando-se o sistema jurídico alemão e o sistema jurídico português ambos como sistemas de direito romano-germânico, torna-se particularmente pertinente a análise da jurisprudência alemã relativamente à matéria da conservação de dados originados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações. É importante, desde logo, porque pode funcionar como uma abertura de horizontes ao evidenciar diferentes opções legislativas e permitir analisar, "ao longe", a efetividade das mesmas. A Lei das Telecomunicações alemã consagrou a conservação dos dados em causa pelo período máximo de 6 meses – limite mínimo previsto na Diretiva 2006/24/CE – e o processo em causa versou justamente sobre as normas dessa lei e do Código de Processo Penal alemão que tinham sido criadas de forma a transpor o conteúdo da Diretiva 2006/24/CE, tendo culminado com a declaração de inconstitucionalidade das mesmas. No entanto, neste acórdão o prazo não foi contestado, tendo inclusivamente sido considerado como *"período de conservação constitucionalmente justificável"*[61], o que permite afirmar que, tendo em conta o tipo de dados em causa, o legislador alemão considerou o mínimo possível como o que melhor salvaguardava a segurança dos dados. Derivado do juízo de inconstitucionalidade, as alterações introduzidas à *Telekommunikationsgesetz* abrangeram o prazo de conservação e, aqui, foi estabelecida uma diferenciação de tratamento tendo em conta os dados em causa: os dados de tráfego deveriam ser armazenados pelo período de 10 semanas, enquanto os dados de localização somente por 4 (Artigo 113º *Telekommunikationsgesetz)*[62].

---

[60] http://www.bverfg.de/e/rs20100302_1bvr025608en.html

[61] Ponto 270 da decisão jurisprudencial alemã.

[62] Porém, a estipulação de um prazo tão curto não foi consensual. Em maio de 2015, a Associação de Juízes emitiu uma declaração no sentido de que tais prazos eram excessivamente garantísticos, não sendo constitucionalmente imposto um prazo tão curto, bem como não consideravam devidamente os interesses investigativos (https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2015/Downloads/05012015_Stellungnahme_DRB_RefE_Einfuehrung_Speicherfrist_Hoechstspeicherfrist_Verkehrsdaten.pdf?__blob=publicationFile&v=1)

A CNPD realça o facto de o legislador não ser livre para definir o prazo de conservação e, como tal, mostra-se insatisfeita com a fixação do prazo de um ano, pois refere que nos crimes considerados como "crimes graves" pela lei e, como tal, idóneos a legitimar a conservação dos dados durante esse mesmo prazo, é "*questionável que o conhecimento do crime não implique o imediato acesso aos dados"*, como exposto na Deliberação nº 641/2017.

c. Argumentos contra a inconstitucionalidade

Em contraposição ao entendimento exposto anteriormente, encontramos a posição do Ministério Público e dos operadores de telecomunicações portuguesas, que defendem, em traços gerais, que o legislador português, na elaboração da Lei nº 32/2008, de 17 de julho, foi para além do quadro básico exigido pela Diretiva 2006/24/CE, tendo acautelado aspetos que haviam sido censurados pelo TJUE aquando da declaração de invalidade da diretiva no acórdão *Digital Rights Ireland*.

Antes de proceder a uma análise pormenorizada dos aspetos salvaguardados pela lei nacional de conservação de dados de tráfego e de localização, importa averiguar a importância de uma obrigação geral de conservação de dados gerados pelas telecomunicações. Em 2015, em Haia, foi realizado o 10º Fórum Consultivo de Procuradores-Gerais e Diretores do Ministério Público dos Estados Membros da União Europeia. Neste, para além de outros aspetos, visava-se discutir os efeitos da declaração de invalidade da Diretiva 2006/24/CE pelo TJUE, bem como o caráter generalizado da obrigação e o acesso e uso dos dados. Pode ser pertinente enquadrar este documento temporalmente, relembrando que os sentimentos provocados pelos ataques terroristas de 13 de novembro em Paris ainda ressoavam no coração das pessoas, urgindo a necessidade de lançar de todos os meios possíveis para evitar ataques futuros[63].

Expõem, desde logo, que o instrumento processual de retenção de dados assume, no contexto e metodologia criminal atual, uma importância incontornável a nível de prossecução e investigação de crimes graves e expressão clara dessa necessidade retira-se do facto de, na Alemanha, um dos países que procedeu à anulação da lei nacional que havia

[63] Neste sentido, os membros salientaram: *"the importance of the early involvement of the judiciary, the speedy exchange of information with other Member States, and the positive feedback on the use of JIT's in such situations". ("Conclusions of Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the Member States of the European Union",* 10 de dezembro de 2015, Haia, p. 3.

transposto a Diretiva 2006/24/CE, 44,5% dos casos que exigiam pedidos de comunicação de dados de tráfego terem ficado sem outros meios que lhes permitissem continuar a investigação, tendo, justamente, 30% dos casos entrado em "colapso"[64]. As dificuldades investigatórias instam do facto de, inexistindo uma obrigação legal de conservação de dados de tráfego e de localização para efeitos de investigação e repressão de crimes graves, as operadoras de telecomunicações deixarem de ser obrigadas à conservação de dados que podem ser considerados essenciais para a prossecução da ação penal ou, mesmo que continuem a conservar alguns (nomeadamente aqueles que surgem de razões comerciais, de proteção dos consumidores e das próprias empresas), o armazenamento desse não fica sujeito às garantias de segurança adequadas tendo em conta a sensibilidade dos dados em causa. Para além dos problemas que são apostos à obrigação de retenção generalizada dos dados, acrescenta-se que os mesmos podem levar a "falsos positivos", incriminando sujeitos que não têm qualquer ligação com o crime[65]. Porém, como é possível retirar das conclusões do fórum em análise, os dados conservados não representam, em si, uma evidência direta de envolvimento no cometimento de um ilícito, dependendo o seu valor probatório da interligação com outros meios de prova à disponibilidade das entidades investigatórias. Os dados de tráfego e de localização, bem como os anexos necessários à identificação do utilizador ou assinante, assumem especial importância não só em identificar suspeitos da realização de determinado ilícito grave, mas também podem auxiliar na ponderação da necessidade de lançar mão de outros meios de prova mais intrusivos – desde logo a interceção e gravação de conversações ou comunicações (art. 187º do CPP). Como uma das maiores implicações da declaração de invalidade da Diretiva 2006/24/CE ressaltam as dificuldades que são inculcadas na cooperação judicial internacional. Havendo Estados-Membros que mantiveram as leis nacionais e outros que as declararam inválidas, erguem-se problemas de resolução de conflitos de jurisdição, na eficiência das *JITs* (*Joint Investigation Team*) e na obtenção e admissibilidade da prova[66].

---

[64] PINTO, Carlos, ob. cit., p. 184.
[65] RUCZ, Melinda, KLOOSTERBOER, Sam, "*Data Retention Revisited"*, European Digital Rights, p. 17-18.
[66] "*Conclusions of Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the Member States of the European Union",* p. 2. A JITs consiste num instrumento da Europol que visa promover a cooperação internacional entre autoridades judiciárias e de aplicação da lei com vista a realizar investigações criminais num ou mais Estados-Membros envolvidos. No que respeita às dificuldades de admissibilidade da prova, salienta-se a falta de claridade da admissão ou não, em Estados cujas leis de retenção foram consideradas inválidas, da prova obtida pela manutenção da obrigação de retenção de dados noutros Estados-Membros.

De forma a afunilar a exposição à Lei nº 32/2008, assume especial relevância a Nota Prática nº7/2015[67] do Ministério Público. Nesta é repetida a essencialidade que assume uma obrigação de caráter generalizado de conservação de dados de tráfego e de localização para efeitos de processo criminal, mas também se ressalta que muitos dos aspetos censurados pelo TJUE já tinham sido considerados pelo legislador português.

O acesso aos dados de tráfego e de localização, em território português, encontra-se dependente de três requisitos cumulativos, com a ressalva de que só são admitidos pedidos de acesso a dados referentes a suspeitos ou arguidos, pessoas que sirvam de intermediário e vítimas (art. 9º, nº3 da Lei nº 32/2008), que são: estar em causa a investigação de um crime grave, de acordo com a definição presente no artigo 2º, nº1, alínea g)[68], exigência da precedência de autorização judicial e a formulação de um juízo de que aquela prova é indispensável para a descoberta da verdade material ou a perceção de que, sem ela, seria impossível ou muito difícil de obter.

A subordinação do acesso aos dados de tráfego e de localização à investigação exclusiva de crimes graves, revela a perceção de que, em vista à salvaguarda de interesses de segurança nacional, só esses é que são suscetíveis de justificar a amplitude da limitação dos direitos fundamentais em causa. No que respeita à determinação do conceito de criminalidade grave, os Estados-Membros adotaram diferentes técnicas - uns basearam-se nos anos de prisão definidos nas leis nacionais, outros realizaram uma lista dos crimes considerados como graves e houve, ainda, quem procedesse a uma combinação de critérios- Portugal enumerou os crimes considerados como graves para aplicação da Lei nº 32/2008.

Para além disso, e satisfazendo uma das exigências do TJUE, o legislador português sujeitou o acesso aos dados à emissão de um despacho fundamentado do juiz de instrução. Aquando da ponderação sobre a transmissão ou não dos dados em causa, a autoridade judicante deve, como exigido pelo artigo 9º, nº4 da Lei nº 32/2008, obedecer aos princípios da adequação, necessidade e proporcionalidade. É, justamente, no âmbito desta avaliação levada a cabo pelo juiz de instrução que ele deve analisar a imprescindibilidade da diligência

67 https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_7_retencao_de_dados.pdf

68 Subsequentemente, para a determinação de "criminalidade violenta" e "criminalidade altamente organizada" deve-se olhar para o artigo 1º do CPP.

em causa, de forma a satisfazer o terceiro requisito – um requisito considerado de *ultima ratio*[69].

No que respeita às medidas determinantes do nível de segurança dos dados conservados, o legislador português demonstrou uma maior perceção da sensibilidade dos dados em causa e acautelou aspetos que haviam sido apontados pelo TJUE, desde logo ao consagrar expressamente a obrigação de destruição definitiva dos dados no termo do período de um ano de conservação – expressa no artigo 7º, nº1, alínea e) da Lei nº 32/2008 -, excecionando os casos em que tenha havido um pedido de preservação expedita de dados. Acresce à obrigatoriedade de destruição dos dados, a atribuição de competências de fiscalização da aplicação da lei a uma entidade administrativa independente, neste caso a Comissão Nacional de Proteção de Dados – artigo 7º, nº 5 da Lei nº 32/2008. A CNPD foi dotada, legalmente, do poder de controlar a aplicação do documento legal em causa, mas também de manter um registo de todas as "pessoas especialmente autorizadas" para aceder aos dados, bem como instituir os processos contraordenacionais necessários.

Uma vez abordado, em termos gerais, os termos em que o legislador português foi para além das diretrizes da Diretiva 2006/24/CE, torna-se pertinente expor os argumentos que surgem a favor da constitucionalidade da lei em causa e que justifiquem as opções nacionais.

No que respeita à obrigação de conservação de dados e ao seu caráter geral, o Ministério Público, na Nota Prática nº 7, é claro e sucinto quanto à necessidade do âmbito do armazenamento se manter geral e indiscriminado. Aponta-se que a obrigação de conservação de dados de tráfego e de localização de todos os assinantes e utilizadores só realiza a sua finalidade principal se mantiver este caráter indiscriminado, pois, aquando da conservação, não é possível averiguar que dados serão ou não importantes em termos de deteção, investigação e repressão de crimes graves – posição que reitera o que havia sido concluído no Fórum Consultivo entre os Procuradores-Gerais e Diretores do Ministério Público. É só após o cometimento e conhecimento do ilícito que tais dados adquirirão relevo probatório e suscitarão interesse por parte das autoridades competentes pela investigação, especialmente nos casos em que não existem suspeitos[70]. Aliás, a pertinência do recurso a

[69] PINHO, Carlos, *"Os problemas interpretativos resultantes da Lei nº 32/2008, de 17 de junho"*, p. 73.
[70] Há autores que designam a utilização deste tipo de tecnologias para identificar agentes que possam ter cometido ilícitos como "pesca de suspeitos". Tal conceito foi referido por Melinda Rucz e Sam Kloosterboer

este tipo de dados depende bastante da existência ou não de suspeitos já designados, pois, caso as autoridades competentes já tenham determinada pessoa sob investigação, existem outros mecanismos aptos a auxiliar a investigação.

É justamente neste ponto que ressalta a conveniência de avaliar a preservação expedita de dados, prevista no artigo 12º da LC e apontada comummente como uma alternativa adequada e menos intrusiva relativamente à obrigação de conservação generalizada de dados. Se, por um lado, a obrigação de conservação prevista na Lei nº 32/2008 impõe a conservação dos dados de todos os utilizadores e assinantes dos serviços de telecomunicações, a preservação expedita de dados ("*quick freeze*"), por sua vez, consubstancia um pedido de preservação remetido a quem tenha disponibilidade sobre os dados especificamente identificados pelas autoridades, de forma a evitar que os mesmos desapareçam, sendo que tal ordem tem um prazo de três meses – que pode ser renovado até ao prazo de um ano. O *quick freeze*, porém, não pode ser considerado uma alternativa idónea, desde logo porque: a não ser que o pedido de preservação seja emitido previamente ao cometimento do ilícito, na falta de uma obrigação de conservação geral de dados de tráfego e de localização, corre-se o risco de não existirem dados a preservar. As autoridades judicantes, com a instituição da obrigação de conservação generalizada, contam, e conduzem a investigação, com a garantia da existência de determinados dados com os quais não poderiam contar na inexistência dela. A propósito da contraposição entre estes dois instrumentos processuais, Carlos Pinho cria uma situação hipotética de aliciamento sexual de menor em que expõe a diferença de efetividade da existência ou não de uma obrigatoriedade de conservação de dados: "*se os dados relativos à ou às comunicações do agente do crime forem apagadas findas que sejam tais comunicações, não será possível, por qualquer outro meio, obter prova da origem de tais comunicações e, por conseguinte, identificar o agente do crime"*[71]. A preservação expedita de dados deve ser, assim, complementada com o regime de conservação generalizada dos dados resultantes das telecomunicações, nomeadamente em casos em que as autoridades investigatórias

na obra citada (p. 18), mas de forma a criticar tal prática, ressaltando a necessidade de acautelar associação de inocentes à prática dos crimes em investigação. Não obstante, se se pode correr o risco de colocar sob investigação pessoas que não tiveram qualquer ligação ao crime, também funcionam como uma ferramenta de "afastamento" de inocentes da mesma investigação – p. 7 de *"Conclusions: 10th Meeting of the Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the Member States of the European Union"*.

[71] PINHO, Carlos, *"Lei de retenção de dados de comunicações eletrónicas: aposentar ou reformar?"*, p. 181.

necessitem do acesso a determinados dados cujo prazo de conservação, estipulado no artigo 6º da Lei nº 32/2008, esteja a chegar ao fim. Porém, assumindo a relevância e utilidade que a conservação generalizada de dados assume no contexto criminológico atual, com a crescente divulgação e acesso às novas tecnologias, foram apontados critérios que permitiram limitar a conservação, desde logo com base em critérios geográficos, temporais ou até com base em determinados círculos de pessoas que "pudessem estar envolvidas de uma maneira ou de outra na prática de infrações graves"[72]. Porém, tal entendimento consubstancia uma violação do princípio da igualdade, princípio este constitucionalmente salvaguardado no artigo 13º, bem como na CEDH no artigo 14º. Em termos gerais, tal princípio implica que ninguém seja tratado de forma diferente perante a lei com base em razões discriminatórias, como a sua raça, sexo, língua, religião, etc[73]. Se, seguindo o exemplo proposto pela CNPD na Deliberação nº 641/2017, limitássemos a conservação à freguesia de Fátima, por ocasião da visita papal, poderíamos, para além de reduzir drasticamente a panóplia de dados disponíveis e potencialmente úteis à investigação por parte das autoridades policiais, estar a beneficiar agentes mais cautelosos no planeamento do ilícito. Tais poderiam planear antecipadamente o cometimento do ilícito com maior liberdade, conscientes de que, naquele período, as suas comunicações não seriam, pelo menos ao abrigo de uma obrigação geral, conservadas.

Uma crítica suscitada pela CNPD, bem como pela Provedora de Justiça, é o facto de o legislador português, aquando da regulação da amplitude da obrigação de conservação, não ter considerado e acautelado devidamente as comunicações sujeitas a sigilo profissional. Porém, tal não é verdade, pois embora não tenha instituído qualquer exceção ou limitação relativamente à conservação, este, no artigo 9º, nº 4 da Lei nº 32/2008, sublinha a necessidade do juiz, no seu juízo relativamente à admissão ou recusa de acesso aos dados, dever tomar em conta a "proteção do segredo profissional". Ou seja, especifica que o juízo do juiz de instrução deve nortear-se não só pelo princípio da adequação, necessidade e proporcionalidade, como expressamente salienta a necessidade de atentar à sensibilidade das comunicações e valores constitucionalmente protegidos em causa – aliás, o acesso a tais

[72] Ponto 72º do pedido de fiscalização abstrata da constitucionalidade cit. supra.
[73] *"(…) limiting retention to specific categories or particular persons reduces the effectiveness of investigations and may apply nebulous distinctions, leading to allegations of prejudice, profiling and unlawful discrimination", "Conclusions: 10th Meeting of the Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the Member States of the European Union",* p. 9.

dados encontra-se sujeito aos casos previstos no artigo 187º/4 e 5 do CPP. A solução adotada pelo legislador nacional ao densificar os requisitos de acesso aos dados é consonante com a opinião do Ministério Público relativamente à admissibilidade duma obrigação deste caráter: *"(…) a retenção de dados (em especial de tráfego) é imprescindível, aquilo que importa discutir não é a sua existência, mas antes as condições em que se processa*"[74]. Também é neste sentido que parecem ir os Procuradores-Gerais e Diretores do Ministério Público dos vários Estados-Membros da União Europeia, referindo que uma adequada regulamentação do acesso aos dados poderia representar a solução para algumas dificuldades que derivaram a invalidade de leis nacionais que impunham a conservação de dados.

Em consonância com o afirmado previamente relativamente à função do direito penal e à necessidade de adaptação dos métodos investigatórios ao contexto social atual, torna-se especialmente pertinente analisar o Acórdão do Tribunal Europeu dos Direitos Humanos (TEDH) K.U. vs *Finland*, de 2 de dezembro de 2008. Em termos gerais, tratou-se de um caso em que foi colocado, numa página de encontros *online*, um anúncio que utilizava a imagem e dados de um menor. Porém, aquando do sucedido, a lei finlandesa não tinha mecanismos que possibilitassem a identificação do agente, desde logo pela inexistência de uma obrigação legal que impusesse às empresas fornecedoras das telecomunicações a transmissão dos dados requeridos pelas entidades investigatórias em detrimento do direito à privacidade que molda as comunicações. O TEDH interpretou o artigo 8º da CEDH no sentido de que o direito ao respeito pela vida privada e familiar abrangia não só o direito de os cidadãos poderem viver sem interferências arbitrárias por parte do Estado na sua intimidade, mas também a imposição de obrigações estaduais positivas, no sentido de proteger adequadamente o direito em causa. Tal pressupõe, desde logo, disposições legais criminais eficientes, com vista uma efetiva dissuasão do cometimento de ilícitos graves – "*A existência de uma ofensa tem efeito dissuasor limitado se não contiver os meios adequados para identificar o autor do crime e trazê-lo à justiça. Os Estados têm a obrigação positiva de criminalizar as ofensas contra as pessoas e reforçar o efeito dissuasor da criminalização (…)*"[75].

Uma das críticas mais fortes do TJUE, bem como sublinhadas pelas principais subscritoras da inconstitucionalidade do diploma legislativo em causa, e que não se

[74] Ponto 2 da Nota Prática nº 7/2015 do Ministério Público.
[75] https://hudoc.echr.coe.int/eng?i=001-89964

encontram expressamente salvaguardadas pela Lei nº 32/2008 prende-se, justamente, com o silêncio da lei relativamente à localização do armazenamento dos dados de tráfego e de localização, bem como dos anexos necessários. Alega-se que, perante a falta de obrigatoriedade de conservação dos dados em causa em território comunitário, a segurança destes é posta em causa, desde logo pelas dificuldades que podem ser apostas à fiscalização. Porém, assume aqui particular acuidade a proposta do Parlamento Europeu e do Conselho de regulamento relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal[76]. Este regulamento visa promover a fluidez na cooperação judiciária entre os Estados-Membros ao estabelecer normas que vinculam e regulam as relações que urgem entre as autoridades investigatórias, os prestadores de serviços e as pessoas visadas, no âmbito de um processo penal específico. Embora este diploma não vise instituir uma obrigação geral de retenção de dados, tem como destinatários aqueles serviços cujo armazenamento de dados constitui parte da sua atividade e, embora não imponha a retenção, a sua efetividade pressupõe o armazenamento de dados, dados estes que se pressupõe que tenham importância prática para as autoridades policiais e judiciárias. Os destinatários do regulamento são, entre outros, os prestadores de serviços de comunicações eletrónicas – os mesmos que são pressupostos na Lei nº 32/2008 – e, na explicitação de que prestadores de serviços se encontrarão abrangidos pelo âmbito deste regulamento, prescinde-se da localização dos dados como um fator de ligação determinante, optando-se pela imposição de obrigações aos prestadores de serviços responsáveis. Neste sentido, o ponto 17 do Considerando da Proposta de Regulamento agora em análise refere que "*em muitos casos, os dados já não são armazenados ou tratados num dispositivo do utilizador, mas sim disponibilizados numa infraestrutura baseada na nuvem para serem acedidos a partir de qualquer lugar. (…) a aplicação do presente regulamento não deverá depender da localização efetiva do estabelecimento do prestador ou da instalação de tratamento ou armazenamento dos dados em causa"*. Embora este não seja um diploma que se encontre para já em vigor, é uma ideia a preconizar, pois a determinação do local de armazenamento está, na maioria dos casos, sujeita às regras de concorrência e, como tal, deve ser determinado por cada serviço com base em considerações comerciais. O artigo 7º da Lei nº 32/2008 obriga as empresas de telecomunicações a adotarem as medidas técnicas e

[76] O regulamento em análise deriva do designado "pacote prova eletrónica" que, para além deste regulamento, engloba uma proposta de diretiva relativa à designação de representantes legais para efeitos de recolha de provas em processo penal.

organizativas necessárias à proteção dos dados em causa. Da solução encontrada para a proposta de regulamento em análise, é possível deduzir a conceção de que a manutenção de um elevado nível de segurança é passível de ser atingido com a direção de obrigações diretamente aos fornecedores destes serviços.

A Diretiva 2006/24/CE estabelecia uma janela temporal de 6 meses a 2 anos de conservação, cabendo aos Estados-Membros a determinação do prazo que consideram adequado. Portugal optou pelo prazo de um ano, solução consentânea com o fórum consultivo referido anteriormente. É dito que a generalidade dos países considera que a conservação deve ser durante um prazo superior a 6 meses e, preferencialmente, de um ano. A CNPD estranha que o conhecimento do crime não implique o imediato acesso aos dados, porém, estamos perante crimes que podem ser levados a cabo com recurso à mais alta tecnologia e cuja investigação e deteção podem ser morosos, pelo que o prazo mínimo estabelecido na Diretiva poderia não ser suficiente para a emissão de um posterior pedido de preservação expedita dos dados. Aliás, tal é constatado, bem como objeto de sérias preocupações, no Relatório de Atividades (setembro 2015- dezembro de 2016) do Gabinete do Cibercrime do Ministério Público[77]. Aquando da análise das dificuldades práticas processuais com que o gabinete se defronta, salienta-se que um prazo de conservação de dados de 6 meses é excessivamente curto e, como tal, suscetível de prejudicar imensuravelmente as investigações, o que é realçado com o facto de, em casos de cibercriminalidade, ser imprescindível o recurso a perícias informáticas, realizadas pela Polícia Judiciária, podendo essas perícias demorar até três anos! Inclusivamente, a explicitação da demora das perícias, justificadas pela Polícia Judiciária por falta de recursos humanos, é feita no âmbito das investigações de crimes de pornografia infantil, um crime que integra a qualificação de "criminalidade violenta", segundo o artigo 1º, alínea f) do CPP, e, como tal, abrangido pela Lei nº 32/2008.

Por fim, é importante analisar o papel do RGPD e a sua relação com a Lei nº 32/2008, uma vez que esta implica um tratamento automático de dados pessoais de todos os cidadãos que utilizam os serviços de telecomunicações. Existem dois direitos contemplados no RGPD cuja restrição se demonstra particularmente relevante para efeitos de efetividade da Lei nº

77 https://www.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_anual_gabinete_cibercrime2015_02-03-2017.pdf

32/2008. O primeiro é o direito à oposição de tratamento de dados (art. 21º do RGPD), que atribui ao titular dos dados a possibilidade de este se opor ao tratamento dos seus dados pessoais. A restrição de qualquer direito imposto pelo RGPD carece de uma intervenção legislativa por parte de cada Estado-Membro e deve respeitar os requisitos da proporcionalidade, adequação e necessidade. A Lei nº 32/2008 ocupou-se especificamente da restrição do direito à oposição do tratamento no artigo 3º, nº 4. Porém, o mesmo já não se pode dizer relativamente ao direito consagrado no artigo 15º do RGPD e que impõe aos fornecedores de serviços competentes pelo tratamento de dados pessoais a comunicação aos visados de que houve pedido de acesso aos seus dados, qual a finalidade desse tratamento e a que entidades tais dados serão transmitidos. Ora, tal comunicação pode ser potencialmente lesiva do processo penal em curso, desde logo porque o titular dos dados percebe que está a ser investigado. Este é um silêncio da Lei nº 32/2008 que é salientado não só pela Provedora de Justiça, que, inclusivamente, refere a possibilidade de prever a hipótese de "não-comunicação"[78], mas também por Carlos Pinho, realçando a necessidade de alteração da lei neste aspeto[79].

d. Análise de jurisprudência – em especial o Acórdão nº 420/2017

No que respeita a jurisprudência nacional relevante respeitante à Lei nº 32/2008, de 17 de julho, assume pertinência especial o Acórdão do Tribunal Constitucional nº 420/2017[80]. Embora a sua análise se mostre importante, é de ressalvar que o objeto do recurso não visou a pronúncia do TC relativamente à amplitude da obrigação de conservação que a lei em causa institui, mas sim uma pronúncia relativamente à constitucionalidade do artigo 6º da Lei nº 32/2008[81].

No caso em apreço, o Ministério Público tinha emitido um pedido ao juiz de instrução que lhes permitisse o conhecimento da identidade do titular de um determinado IP, que tinha suscitado especial interesse no decurso da investigação de um crime de pornografia de

[78] "*Neste contexto, configurar-se-á, ainda, admissível a decisão de não-comunicação, naqueles casos em que for manifesto que de qualquer informação prestada ao interessado – independentemente do momento em que ocorra – sempre resultará frustração da investigação ou perigo para a vida ou integridade física de terceiros.*", ponto 96º do pedido de fiscalização abstrata da constitucionalidade cit. supra.
[79] PINHO, Carlos, ob. cit. p. 190.
[80] Processo nº 917/16 de 13 de julho.
[81] "*É sujeita a esta dupla restrição na sua dimensão normativa – art. 6º, com referência, mais precisamente, aos nºs. 1, 2ª parte e 2, alín. b) – iii) do art. 4º e subordinadamente conjugado com o art. 9º, todos da Lei nº 32/2008 -, que o objeto inicial do recurso é delimitado (art. 635º/4 do CPC)*", 3º parágrafo do ponto 2 do Relatório.

menores. O TC, neste âmbito, adotou a classificação tripartida dos dados eletrónicos que já havia sido explicitada no Acórdão nº 403/2015 do TC: dados de base (relativos à conexão à rede), dados de tráfego e de localização (relativos ao estabelecimento de uma comunicação e gerados pela utilização da rede) e, por fim, os dados de conteúdo (relativos ao conteúdo da própria comunicação). A explicitação desta divisão é particularmente relevante, desde logo em vista a enquadrar os dados a que o Ministério Público requeria o acesso. O IP (*Internet Protocol)* é classificado como dado de base, ou seja, aquele que existe independentemente do estabelecimento de uma ligação. O direito que fundamenta este recurso é, justamente, o direito à inviolabilidade das comunicações, previsto no artigo 34º/4 da CRP. Neste sentido, o TC concluiu que os dados de base têm um caráter pouco lesivo e, como tal, merecedor de uma tutela constitucional diferenciada daquela que é destinada aos dados de tráfego e aos dados de conteúdo, uma vez que estes só existem quando conectados a uma concreta comunicação – ao menos tentada-, pois estes já assumem um caráter muito mais intrusivo da privacidade dos cidadãos. Em consonância com tal entendimento, é expresso que os dados de base não contendem com o direito ao sigilo das comunicações, consubstanciando, antes, uma limitação do direito à reserva da vida privada e familiar (art. 26º CRP). Porém, aquando da análise da conformidade da restrição deste direito com base no artigo 18º da CRP, apura-se que a restrição causada pelo acesso aos dados de base não é desproporcional e, como tal, o TC concluiu pela não inconstitucionalidade das normas em apreço.

De forma a compreender melhor esta decisão, revela-se importante atentar no Acórdão nº 403/2015 do Tribunal Constitucional. Neste acórdão visava-se apurar a constitucionalidade do artigo 78º/2 do Decreto-Lei nº 426/XII da Assembleia da República, que aprovou o Regime Jurídico do Sistema de Informações da República Portuguesa. Esta norma atribuía legitimidade aos oficiais de informações para aceder a um variado conjunto de dados, entre os quais se encontravam os "(…) *dados de tráfego, de localização ou outros conexos das comunicações, necessário para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicações, bem como para identificar o equipamento de telecomunicações ou a sua localização* (…)". A primeira questão que o TC ficou encarregado de resolver era, justamente, se o acesso a metadados deve considerar-se como uma "ingerência nas telecomunicações para os efeitos previstos na norma constitucional". Aqui procedeu-se a uma análise particularmente cuidada dos diferentes tipos de dados que são suscetíveis de surgir da utilização das redes de

telecomunicações, subscrevendo a classificação tripartida do Conselho Consultivo da Procuradoria-Geral da República e realçando a ligação mais ou menos estreita de cada espécie com os direitos, liberdades e garantias dos cidadãos. É especialmente unânime a opinião de que os dados de tráfego, à semelhança do que acontece com os dados de conteúdo, integram o conceito de comunicações constitucionalmente relevantes, pois, caso contrário, a proteção constitucional revelar-se-ia incompleta[82]. Os elementos de tráfego permitem isolar uma determinada comunicação e inferir dados pessoalíssimos dos utilizadores das redes de telecomunicações, não devendo ser merecedores de uma tutela diferente daquela que é destinada aos dados de conteúdo. Já os dados de base, por não dependerem da tentativa ou da realização efetiva de uma comunicação, não são abrangidos pelo sigilo das comunicações.

O Acórdão nº 420/2017 adotou esta conceção, remetendo grande parte da sua fundamentação para o exposto no Acórdão nº 403/2015 e, com base nisso concluiu pela constitucionalidade da norma que imponha aos fornecedores dos serviços de telecomunicações a conservação dos dados de base. Porém, relativamente à proporcionalidade da obrigação de conservação de dados de tráfego e dados de localização intrinsecamente ligados a uma comunicação (efetivada ou tentada), o TC ainda hoje não se pronunciou expressamente.

Mais recentemente, no Acórdão nº 464/2019[83], requereu-se que o TC avaliasse a constitucionalidade do artigo 3º e 4º da Lei Orgânica nº 4/2017, de 25 de agosto, sendo que nestes artigos se regulava o acesso pelos oficiais de informações a dados de telecomunicações e *internet*. Os oficiais de informações pretendiam o acesso àqueles dados para efeitos de "mera" prevenção, não pressupondo, por isso, o cometimento de um ilícito já realizado, o que está subjacente ao acesso que é legitimado pela Lei nº 32/2008. A realização de um ilícito consubstancia um requisito importante para a admissão de uma ingerência desta amplitude, sendo tal constitucionalmente exigido pela parte final do artigo 34º/4 da CRP. Embora o TC tenha explicitado que não se iria pronunciar sobre a validade

[82] *"A Constituição protege, em primeira linha, o sigilo do conteúdo da correspondência (...). No entanto, essa proteção, especialmente nos modernos meios de comunicação, é ainda constitucionalmente garantida às circunstâncias em que realizam as comunicações"*, MIRANDA, Jorge e MEDEIROS, Rui, "*Constituição Portuguesa Anotada"*, p.561

[83] Processo nº 26/2018 de 21 de outubro.

desta lei, referiu a necessidade de avaliar a sua conformidade com o direito da União Europeia.

e. Reflexão crítica

De forma a decidir pela (in)validade e (des)necessidade do expediente processual em causa, importa clarificar alguns aspetos. O equilíbrio que se almeja atingir é, justamente, entre o direito à reserva da vida privada das pessoas e direito à proteção dos seus dados com a (crescente) necessidade de conservar alguns destes para efeitos de investigação criminal[84] sendo que, como referido por Silva Ramalho, o pêndulo vai variando consoante a época em que estejamos, em casos de maior tranquilidade, as comunidades são menos suscetíveis a admitir restrições aos seus direitos fundamentais, "*reivindicam o afastamento do Estado da sua esfera individual*"[85], enquanto perante situações que abalam verdadeiramente a paz jurídica comunitária, há uma maior consciencialização da necessidade de colocar os interesses da comunidade sobre os interesses individuais. A Diretiva 2006/24 surgiu, justamente, no rescaldo dos ataques terroristas em Madrid (2004) e no Reino Unido (2005).

A primária finalidade do processo penal é, justamente, a justiça, isto é, "*este não pode existir validamente se não for presidido por uma direta intenção ou aspiração de justiça"*[86]. De forma a atingir esse ideal, o processo penal tem de ser suscetível de se moldar às novas realidades e exigências, às novas prioridades de atuação e conseguir adaptar a sua dinâmica de forma a responder-lhes de forma legítima e adequada. É cognoscível que inerente a muitas modalidades criminológicas que legitimam a atuação da Lei nº 32/2008 se encontram extensas e profundas dificuldades investigatórias derivadas, em grande parte, de um conjunto de práticas que se podem designar como medidas anti-forenses. Se é certa a exigência que é imposta e sentida pelas entidades investigatórias de se desenvolverem e atuarem de modo consentâneo com a evolução da sociedade, também os criminosos têm esta consciência, pelo que reúnem esforços no sentido de dificultar a prossecução das investigações. Com vista a dissimular as provas digitais e a dissipar o seu rasto digital, delinquentes mais diligentes e dotados de conhecimentos técnicos avançados têm vindo a desenvolver técnicas, *softwares*, programas informáticos com a única finalidade de atrasar

[84] Ramalho, David Silva e Coimbra, José Duarte, ob. cit., p. 998.
[85] RAMALHO, David Silva e COIMBRA, José Duarte, ob. cit., p. 998.
[86] DIAS, Jorge de Figueiredo, "*Direito Processual Penal"*, p. 44

ou frustrar a deteção da atividade ilícita em causa[87]. Técnicas deste género assumem um caráter potencialmente lesivo das investigações em curso, pelo que se exige, com vista à prossecução da realização da justiça e à satisfação das exigências impostas pela comunidade, que o Estado se dote, igualmente, de técnicas (lícitas), expressivas da sua superioridade ética, idóneas à identificação e punição dos agentes e ao restabelecimento da paz jurídica comunitária.

Sem essa adaptação, não estará o direito penal apto a responder às exigências de prevenção geral que estão inerentes à aplicação de qualquer pena, nem, aprofundando a perspetiva para o plano singular, inibirá os agentes de incorrer na prática de ilícitos[88], pois estes podem pôr em perspetiva a possibilidade de o crime poder, efetivamente, compensar.

Claro é que as adaptações dos métodos investigatórios não podem ter em conta, exclusivamente, os interesses repressivos, punitivos e de restabelecimento da paz comunitária, tendo necessariamente de estar balizados pelos valores eminentes da nossa ordem jurídica, nomeadamente pelos direitos fundamentais dos cidadãos. É inquestionável o foco que os dados em ambiente digital assumem na atualidade – *"Estes dados representam um verdadeiro mercado para o comércio eletrónico (...)"*[89]- e, afunilando até a dados pessoalíssimos, torna-se clara a inerente necessidade de proteção dos mesmos, visando obstar a práticas abusivas. É necessário almejar a concordância prática[90] entre a finalidade de respeito pelos direitos fundamentais dos cidadãos por parte do Estado, enquanto realizador e administrador da ação penal, e a descoberta da verdade material e inerente realização da justiça.

A tecnologia e todas as suas virtualidades, especialmente (para o que nos importa) aquelas que são transpostas para o Mundo do crime, vieram para ficar e não consubstanciam um fenómeno de escassa importância[91]. Olhando para a balança que procura equilibrar o direito à reserva da vida privada e proteção dos dados pessoais com os interesses inerentes à investigação criminal, tendo a inclinar-me para a prevalência das necessidades de

[87] RAMALHO, David Silva, ob. cit., p. 151
[88] DIAS, Jorge de Figueiredo, *"Direito Penal"*, p. 55
[89] MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática"*, p. 439
[90] ANTUNES, Maria João, *"Direito Processual Penal",* p. 15.
[91] É representativo do relevo que este tipo de criminalidade representa o facto de aparecer como uma modalidade criminológica de prevenção e investigação prioritária na Lei nº 55/2020, que visou definir os objetivos, prioridades e orientações de política criminal.

investigação. Sendo decisiva a perceção de que os ilícitos que legitimam a aplicação da Lei nº 32/2008 assumem um elevado potencial lesivo de valores basilares da nossa ordem jurídica e, associado às dificuldades investigatórias já referidas, considero que não devemos cair na tentação de um discurso excessivamente paternalista e garantístico dos direitos fundamentais que frustre a criação de meios idóneos a detetar e punir os agentes que prezam pelo perfecionismo técnico.

Porém, embora defenda a manutenção da conservação indiscriminada dos dados de tráfego e de localização para efeitos de investigação criminal, tal não implica que a considere isenta de críticas, desde logo em vista a satisfazer as exigências derivadas da tutela dos direitos fundamentais que aqui são implicados. Apostar na constante atualização das medidas de proteção e segurança das bases de armazenamento de dados é crucial. Embora os dados sejam conservados durante o período de um ano pelas várias operadoras de telecomunicações, a maioria é bloqueada[92] e o acesso nunca é requerido, pelo que são conservados e desaparecem sem qualquer implicação. O reforço da proteção destas bases de dados permite reduzir o risco de acesso ilegítimo drasticamente. Para além disso, é urgente a necessidade de compatibilizar a Lei nº 32/2008 com o RGPD e com as leis de proteção de dados que vigoram entre nós, nomeadamente no que respeita ao direito de acesso dos titulares dos dados[93], mas também tornar, finalmente, obrigatória a transmissão dos dados em causa através da aplicação que foi especificamente criada para esse efeito.

IV. A (difícil) relação entre a Lei nº32/2008 e Lei nº 109/2009

A acrescentar aos problemas inerentes à validade, e necessidade, ou não da Lei nº 32/2008, de 17 de julho, colocam-se ainda problemas relativamente à sua compatibilização com outros diplomas legais, nomeadamente com a Lei do Cibercrime. No que respeita às relações que se devem afirmar entre estes dois diplomas, surgem essencialmente duas posições. Em primeiro, e a minoritária, defende que a LC derrogou tacitamente a Lei nº 32/2008, nomeadamente no respeitante ao regime de acesso aos dados conservados – "*Aquela lei só sobrevive naquilo que não foi expressamente regulado pela lei do cibercrime"*[94]-, fundando-se no aforismo *lex posterior derogat priori* e na conceção de que

[92] Art. 7º/2 da Lei nº 32/2008, de 17 de julho.
[93] Em 2019, foram emitidas duas leis respeitantes à proteção de dados pessoais: Lei nº 58/2019 e Lei nº 59/2019. Esta última ocupa-se, especificamente, do tratamento de dados pessoais para auxílio de investigação criminal e estatui, precisamente, o direito de acesso e os fundamentos legitimadores da sua limitação (art. 15º e 16º).
[94] CORREIA, João Conde, "*A Prova Digital: as leis que temos e a lei que devíamos ter"*, p. 36

a Lei nº 32/2008 iria subsistir essencialmente no respeitante à obrigação de conservação que é imposta aos fornecedores de serviços, bem como de todos os deveres inerentes a essa que visam assegurar a proteção e segurança dos sensíveis dados em causa[95]. No sentido oposto, e correspondendo ao juízo maioritário, defende-se que entre estas leis se estabelece uma relação de complementaridade, que ressalta expressamente do artigo 11º/2 da LC. Assumindo-se a Lei do Cibercrime, atualmente, como a pedra angular[96] da obtenção de prova digital e atendendo-se às definições que elencam no seu artigo 1º, é fácil de constatar que a LC estatui um regime especial de obtenção de dados de base, de tráfego e de localização, desde que "*se tratem de dados informáticos contidos num sistema informático e esteja em causa a investigação dos crimes indicados no catálogo do artigo 11º do referido diploma legal, com as exceções contidas no catálogo especial do artigo 18º"*[97], que nem sempre é facilmente conjugado com o regime de acesso previsto na Lei nº 32/2008.

É reflexo dessa confusão de regimes o confronto entre o artigo 14º da LC, que, por sua vez, regula a injunção para apresentação ou concessão do acesso a dados, que se traduz num pedido formulado pela autoridade judiciária competente dirigido a quem tem disponibilidade ou controlo sobre os dados visando a sua junção ao processo ou permitir o seu acesso, e o artigo 4º e 9º da Lei nº 32/2008. No nº4 do referido artigo, encontra-se expresso que é aplicável aos fornecedores de serviços[98] e que estes podem, sob pena de responder criminalmente por desobediência, ter de apresentar dados relativos aos seus clientes ou assinantes, desde que não sejam respetivos a tráfego ou conteúdo. Como exposto por Carlos Pinho, de acordo com este expediente, podem ser mobilizados ao processo dados de base. Contudo, a Lei nº 32/2008 inclui, no específico catálogo de dados que regula, os dados de base, sujeitando o seu acesso e transmissão aos requisitos previstos no artigo 9º da respetiva lei. A título de lembrança, os dados de base são aqueles prévios e instrumentais a uma qualquer comunicação, incluindo o número de telefone, o endereço eletrónico e o contrato de ligação à rede[99]. Desta forma, impõem-se duas questões: se, no âmbito da investigação em curso, se achar necessário aceder a dados de base específicos integrados

[95] MESQUITA, Paulo Dá, "*Processo Penal, Prova e Sistema Judiciário"*, p. 123
[96] CORREIA, João Conde, ob. cit., p.34
[97] PINHO, Carlos, "*Problemas interpretativos resultantes da Lei nº 32/2008, de 17 de julho",* p.76
[98] "Fornecedor de serviço: qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respetivos utilizadores" (artigo 2º d) da LC)"
[99] Acórdão nº 420/2017, ponto 12 da fundamentação.

num sistema informativo de um fornecedor de serviços, deve tal pedido obedecer aos requisitos de que regime? Ao regime previsto no artigo 14º, cujo pedido pode vir a ser formulado pelo MP e fora do catálogo de crimes previsto no artigo 2º/1 g) da Lei nº 32/2008, ou ao regime instituído na Lei nº 32/2008, que subordina a transmissão desses dados à emissão de um despacho fundamentado do juiz de instrução e à indispensabilidade desse meio de prova, bem como a um restrito catálogo de crimes?

Face à confusão relativa à competência para aceder a dados de base, o Gabinete do Cibercrime do MP emitiu a Nota Prática nº8/2016[100], que visava esclarecer as autoridades relativamente aos dados que eram conservados pelos operadores de telecomunicações, bem como as entidades competentes para o seu pedido e respetivo tempo de conservação. À revelia do disposto em diversas alíneas do artigo 2º da Lei nº 32/2008, afirmou que os dados de identificação dos clientes estavam sujeitos ao regime prescrito no artigo 14º da LC e, como tal, suscetíveis de serem transmitidos para o processo penal correspondente através de um pedido do MP, relativamente a qualquer tipo de crime. Ainda neste sentido, e especificamente sobre a qualificação do endereço IP, emerge a Nota Prática nº2/2013[101] que expressa como sendo competência do MP a identificação do utilizador de um determinado IP, "aconchegando-se" de diversas decisões jurisprudenciais que foram nesse sentido. Importa, neste âmbito, referir o Acórdão do Tribunal da Relação de Lisboa de 19/06/2014[102], onde se entendeu que "*obter a identificação do utilizador de um endereço IP ... num determinado dia e hora não é suscetível de revelar informação privada ou confidencial e apenas permite confirmar que uma comunicação- que a investigação conhecia já – ocorreu"*[103], alertando, ainda, que não admitir o ofendido de aceder a este dado prejudica o seu direito de acesso ao direito, constitucionalmente consagrado no artigo 20º da CRP. Difunde-se, assim, uma prática judiciária que se afirma na penumbra do imbróglio permitido pelo legislador ao não compatibilizar expressamente os diplomas legislativos em causa.

100 https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_8_pedido_de_info_a_isp_0.pdf

101 https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_2_jurispridencia_sobre_ip.pdf

102 Processo nº 1695/09.5PJLSB.L1-9

103 Ponto 4 do acórdão em análise.

Aliás, neste sentido, afigurou-se o artigo 14º da LC como *"um dos eixos de revogação do art. 9º da Lei nº 32/2008"*[104].

Fora o problema relativo à legitimidade do acesso aos dados de base, importa atentar no artigo 18º da LC – o único expediente processual da LC que permite o acesso a dados de tráfego. Confrontando os requisitos de acesso aos dados de tráfego impostos no artigo 18º da LC e no artigo 9º da Lei nº 32/2008, as suas semelhanças são evidentes – ambos condicionam a transmissão a um despacho fundamentado do juiz de instrução e têm em vista os mesmos visados[105]. O fator dissonante entre ambos os mecanismos é, justamente, o catálogo de crimes que legitima o seu recurso, porém, não seria esta uma oportunidade de consenso e união dos regimes, visando a tão desejada unidade processual? O artigo 18º da LC legitima o acesso a este tipo de dados em todos os crimes previstos na mesma, bem como em todos aqueles em que se admitem as escutas telefónicas. O catálogo de crimes previsto no artigo 187º do CPP é composto por aqueles crimes que o legislador considera suscetíveis de abalarem a paz jurídica comunitária ao ponto de admitir o recurso a escutas telefónicas, um dos meios de prova mais intrusivos da privacidade dos cidadãos, permitindo, inclusivamente, o acesso a dados de conteúdo. Ou seja, o legislador português, aquando da transposição da Diretiva 2006/24/CE, já dispunha, no ordenamento jurídico português, de um catálogo de crimes graves, mas mesmo assim sentiu a necessidade de definir outro e, consequentemente, proceder à duplicação de regimes, o que *"(...) revelou um desconhecimento das regras processuais penais vigentes no nosso ordenamento jurídico (...)"*[106], mesmo quando ambos espelham a consciencialização da sensibilidade dos dados em causa e necessidade inerente de maior cuidado no seu acesso.

V. Conclusão

Ao longo de toda esta dissertação, salientou-se o quanto o nosso modo de viver, de pensar e de nos relacionarmos com o Mundo em geral se transformou com a crescente introdução das novas tecnologias no nosso quotidiano. Inerente à digitalização que promovemos, surgem problemas tão específicos que não se pode almejar resolvê-los sem o

[104] MESQUITA, Paulo Dá, ob. cit., p.113
[105] O nº4 do artigo 18º da LC remete, em tudo o que não contrariar o presente artigo, para os artigos referentes às escutas telefónicas, nomeadamente art. 187º, 188º e 190º do CPP. O artigo 187º/4 CPP, à semelhança do artigo 9º/3 da Lei nº 32/2008, limita o universo de visados por estes expedientes ao suspeito, arguido, intermediário e vítima de crime.
[106] PINHO, Carlos, *"Os problemas interpretativos resultantes da Lei nº 32/2008, de 17 de julho"*, p. 75.

consequente desenvolvimento de meios idóneos à sua satisfação - "*O Direito conhece, por isso, uma inevitável servidão relativamente à realidade espacial circundante, pelo que todas as evoluções do mundo social, político ou económico condicionam e influenciam o mundo jurídico"*[107].

Partimos, justamente, deste ponto: das alterações tecnológicas que revolucionaram a sociedade e a insuficiência dos expedientes tradicionais para fazer face às especificidades das novas modalidades criminológicas, nomeadamente aquelas que integram no seu *modus operandi* as novas tecnologias. Um dos instrumentos que foi criado com o objetivo de fazer face às novas dificuldades inculcadas à investigação criminal foi, justamente, a Lei nº 32/2008, de 17 de julho, que obriga à conservação indiscriminada de dados de tráfego e de localização, bem como de todos os anexos necessários à identificação do utilizador, durante o período de um ano com a mera finalidade de auxílio das investigações criminais. Porém, como é evidente, tal conservação levanta uma série de preocupações relativamente à salvaguarda efetiva dos direitos fundamentais com que confronta diretamente, desde logo no que respeita à segurança que direciona à quantidade colossal de dados cuja conservação ordena, mas, mais profundo que isso, levantam-se questões sobre a sua necessidade e proporcionalidade relativamente à finalidade que visa combater. É indubitável que o combate à criminalidade grave consubstancia um interesse comunitário de elevado relevo, porém, até que ponto devemos admitir a limitação dos nossos direitos fundamentais, enquanto cidadãos de uma sociedade democrática?

Por outro lado, encontramos os interesses inerentes às investigações criminais e necessidade de restabelecimento da paz comunitária que foi perturbada pela execução do ilícito. É tão imprescindível que a atuação do Estado se paute pelo respeito pelos direitos fundamentais, como assegurar que este esteja munido de instrumentos que permitam a efetiva realização do seu dever de administrar e realizar a justiça penal. Foi indicado que as comunidades são mais suscetíveis a aceitar limitações dos seus direitos fundamentais quando são confrontados com ataques de grande dimensão, dotados de um potencial lesivo extraordinário e cujos meios tradicionais se mostram insuficientes para reprimir. Face a estes, torna-se mais fácil aceitar as limitações aos seus direitos, mas será que nos devemos permitir ter "memória curta" e, em momentos de paz, impor um padrão de proteção dos

[107] MARQUES, Garcia e MARTINS, Lourenço, *"Direito da Informática"*, p. 76.

nossos direitos que minem a possibilidade de adoção de meios adequados ao combate desse tipo de criminalidade – que, aliás, podem anular o efeito dissuasor da instituição de determinados comportamentos como crime?

É no balanço constante entre estes dois interesses que a dissertação se desenrolou, procurando o equilíbrio constitucionalmente admissível entre dois valores fundamentais de qualquer Estado de Direito. Jorge Reis Novais, ao enunciar os parâmetros que o Tribunal Constitucional alemão considerava no âmbito da restrição de direitos fundamentais, expressa que "*quanto maior for a intensidade da restrição, tão mais significativos devem ser os valores comunitários que a justificam"*[108]. A teleologia da Lei nº 32/2008 prende-se com a necessidade de fazer face às exigências e particularidades que são suscitadas com as novas modalidades criminológicas, essencialmente, com aquelas que são levadas a cabo por delinquentes que dominam as tecnologias e que procuram minuciosamente as fragilidades do sistema processual penal com vista a beneficiar delas. O primordial perigo invocado relativamente à conservação generalizada de dados de tráfego e de localização de todos os utilizadores de comunicações eletrónicas é o risco de acesso ilegítimo, isto é, a possibilidade de terceiros dotados de específicos conhecimentos e meios técnicos acederem indevidamente àquele tipo de dados, contornando todas as medidas organizativas e técnicas que haviam sido imputadas pelo Estado por serem consideradas adequadas a manter um elevado nível de segurança. Porém, são justamente estes delinquentes que a Lei nº 32/2008 visa detetar e trazer à justiça, é relativamente a estes agentes que se acentuam as dificuldades investigativas, portanto, ao eliminar a obrigação de conservação de dados de tráfego e de localização poder-se-ia cair na infelicidade de beneficiar aqueles em detrimento da paz jurídica e segurança comunitária. A fronteira entre o mundo digital e o mundo físico assume-se cada vez mais ténue, o que expressa a crescente necessidade de adaptar e expandir os instrumentos processuais à realidade digital. O expediente em causa apura-se, portanto, como imprescindível na busca do rasto digital dos delinquentes ao mesmo tempo que é passível de ser configurado de forma a minimizar ao máximo as perdas axiológicas que derivam da limitação do direito à reserva privada e familiar e do direito à proteção de dados.

Por fim, importou analisar a complicada relação que se desenrola entre a Lei do Cibercrime e a Lei nº 32/2008, de 17 de julho, e ponderar sobre a sua efetiva necessidade.

[108] NOVAIS, Jorge Reis, *"Limites dos Direitos Fundamentais",* p. 76.

Face a uma dualidade de regimes que, em partes, parece desnecessária, urge o sentimento de que o legislador tem de se debruçar, séria e profundamente, sobre a unificação da matéria relativa à obtenção de prova em ambiente digital, desde logo porque já não estamos perante um fenómeno criminal e probatório "especial" e, como tal, justificador de regulação em legislação extravagante.

VI. Bibliografia

- ALBUQUERQUE, Paulo Pinto de, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direito do Homem*, 4ª edição, Lisboa: Universidade Católica Editora, 2011;
- ANTUNES, Maria João, *Direito Processual Penal*, 2ª Edição, Coimbra: Almedina, 2019;
- CANOTILHO, J. J. Gomes; MOREIRA, Vital, *Constituição da República Portuguesa anotada,* Volume I, 4ª edição, Coimbra: Coimbra Editora, 2007;
- CARRAPIÇO, Helena, *O Crime Organizado e as Novas Tecnologias: uma faca de dois gumes*, 3ª Série, Nº 111, Instituto da Defesa Nacional, 2005;
- CORREIA, João Conde, *Prova digital: as leis que temos e a lei que devíamos ter*, in Revista do Ministério Público, 139, 2014, p. 29-59;
- DIAS, Jorge de Figueiredo, *Direito Processual Penal,* 1ª Edição, Coimbra: Coimbra Editora, 1974;
- DIAS, Jorge de Figueiredo, *Direito Penal- Parte Geral*, Tomo I, 2ª Edição, Coimbra: Coimbra Editora, 2012;
- FIDALGO, Sónia, *A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo*, in *A Inteligência Artificial no Direito Penal* (Coord. Anabela Miranda Rodrigues), 1ª edição, Almedina, 2020, p. 129-156;
- GAMA, António et al., *Comentário Judiciário do Código de Processo Penal*, 2ª Edição, Coimbra: Almedina, 2019;
- MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática,* 2ª Edição, Coimbra: Almedina, 2006;
- MCLUHAN, Marshal, *La Galaxia Gutenberg - genesis del homo typographicus*, Madrid: Aguilar, S.A. de Ediciones, Juan Bravo, 1969;
- MIRANDA, Jorge e MEDEIROS, Rui, *Constituição Portuguesa Anotada*, Volume I, 2ª edição, Lisboa: Universidade Católica Editora, 2017;
- MESQUITA, Paulo Dá, *Prolegómenos sobre prova eletrónica e interceção de telecomunicações no Direito Processual Penal Português- o Código e a Lei do Cibercrime*, in *Processo Penal, Prova e Sistema Judiciário*, Coimbra: Coimbra Editora, 2010, p. 83-127;

- NATÁRIO, Rui Manuel Piteira, *O Combate ao Cibercrime: Anarquia e Ordem no Ciberespaço*, in Revista Militar, outubro de 2013, p. 823 – 858;
- NOVAIS, Jorge Reis, *Limites dos Direitos Fundamentais*, Coimbra: Edições Almedina, 2021.
- PINHO, Carlos, *Lei da retenção de dados de comunicações eletrónicas: aposentar ou reformar?*, in Revista do Ministério Público, Nº 154, abril – junho de 2018, pp.167-192;
- PINHO, Carlos, *Os problemas interpretativos resultantes da Lei nº 32/2008, de 17 de julho"*, in Revista do Ministério Público, Nº 128, janeiro – março de 2012, pp. 63-93;
- RAMALHO, David Silva, *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Coimbra: Edições Almedina, 2017;
- RAMALHO, David Silva e COIMBRA, José Duarte, *A declaração de invalidade da Diretiva 2006/24/CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves*, in O Direito (Diretor: Jorge Miranda), Ano 147º, IV, Lisboa: Edições Almedina, 2015, p. 997- 1045;
- RAMOS, Armando Dias, *A Prova Digital em Processo Penal: O Correio Eletrónico*, 2ª Edição, Lisboa: Chiado Editora, 2017;
- RUCZ, Melinda e KLOOSTERBOER, Sam, *Data Retention Revisited*, European Digital Rights;
- SILVA, Flávio Manuel Carneiro da, *A apreensão e utilização processual de meios de prova existentes em material informático*, no *e-book* Meios de Obtenção de Prova e Medidas Cautelares de Polícia, Centro de Estudos Judiciários, 1ª edição, 2019, p. 13- 39;
- SILVEIRA, Alessandra, e FREITAS, Pedro Miguel, *Implicações da declaração de invalidade da Diretiva 2006/24 na conservação de dados ("metadados") nos Estados-Membros da EU: uma leitura jusfundamental*, Revista de Direito, Estado e Telecomunicações, Brasília, v. 9, maio de 2017;
- VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada*, 1ª edição, Coimbra: Coimbra Editora, 2011.

Outros documentos e links relevantes:

- Nota Prática nº2/2013 – a obtenção do endereço IP- súmula da jurisprudência recente, Gabinete do Cibercrime, 3 de abril de 2013, disponível em https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_2_jurispridencia_sobre_ip.pdf consultado a 30/12/2021;
- Nota Prática nº7/2015 – retenção de dados de tráfego e Lei nº 32/2008, Gabinete do Cibercrime, 30 de dezembro de 2015, disponível em http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_7_r consultado a 29/11/2021;
- Nota Prática nº8/2016 – pedido de dados a operadores de comunicações, Gabinete do Cibercrime, 18 de fevereiro de 2016, disponível em http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_8_ consultado a 30/12/2021;
- Parecer nº 16/94/complementar da Procuradoria-Geral da República, de 02/05/1996, disponível em https://www.ministeriopublico.pt/pareceres-pgr/8833 e acedido a 03/01/2022;
- https://www.ojp.gov/pdffiles1/Digitization/189403NCJRS.pdf e consultado a 13/11/2021;
- https://www.consilium.europa.eu/pt/infographics/results-eu-fight-against-crime-2020/ e consultado a 13/11/2021;
- http://apcforenses.org/?page_id=36 e consultado a 13/11/2021;
- https://www.citius.mj.pt/portal/article.aspx?ArticleId=463 e consultado a 05/12/2021;
- Relatório de Atividade – setembro de 2015 a dezembro de 2016 – Gabinete do Cibercrime do Ministério Público, disponível em https://www.ministeriopublico.pt/sites/default/files/documentos/pdf/relatorio_anual_gabinete_cibercrime2015_02-03-2017.pdf e acedido a 07/11/2021;
- "Conclusions: 10th Meeting of Consultative Forum of Prosecutors General and Directors of Public Prosecutions of the Member States of the European Union and Workshop on Data Retention in the Fight Against Serious Crime: The Way Forward", 10 de dezembro de 2015, Haia, disponível em https://www.eurojust.europa.eu/sites/default/files/Publications/Reports/CF-2016-02-09_EN.pdf e acedido a 19/12/2021;

- Deliberação nº 1008/2017 da Comissão Nacional de Proteção de Dados, de 18 de julho de 2017, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2017&type=2&ent= e acedido a 29/01/2022;
- Deliberação nº 641/2017 da Comissão Nacional de Proteção de Dados, de 9 de maio de 2017, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2017&type=2&ent= e acedido a 29/01/2022;
- Proposta de Regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52018PC0225 e acedido a 21/12/2021;
- Recomendação nº 1/B/2019 relativa à Lei nº 32/2008, de 17 de julho, relativa à conservação de dados gerados e tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, disponível em https://www.provedor-jus.pt/documentos/Rec_1B2019_2019_01_22_Recomendacao_da_Protecao_de_dados_Ministra_Justica.pdf e acedida a 5/11/2021 e acedido pela última vez a 15/11/2021;
- Pedido de fiscalização abstrata da constitucionalidade do artigo 4º, 6º e 9º da Lei nº 32/2008, de 17 de julho, pela Provedora de Justiça, disponível em https://www.provedor-jus.pt/documentos/q-7746-2017/ e acedido pela última vez a 29/01/2022;
- Portaria nº 469/2009, de 06 de maio, disponível em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1265&tabela=lei_velhas&nversao=1&so_miolo= e acedida a 15/11/2021;
- Portaria nº 694/2010, de 16 de agosto, disponível em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?tabela=leis&nid=1267&pagina=1&ficha=1 e acedida 15/11/2021;
- Declaração da Associação de Juízes Alemães sobre o projeto de lei que introduzia uma obrigação de armazenamento e um período mínimo de retenção para dados de tráfego, nº 12/15 de maio de 2015, disponível em https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Stellungnahmen/2015/Downloads/05012015_Stellungnahme_DRB_RefE_Einfuehrung_Speicherfrist_Ho

echstspeicherfrist_Verkehrsdaten.pdf?__blob=publicationFile&v=1 e consultado a 17/12/2021;

Jurisprudência Nacional e Internacional:

- Acórdão *Digital Rights Ireland*, de 8 de abril de 2014, Proc. nº C-293 e C-594/12, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62012CJ0293&from=pt, acedido pela última vez em 22/01/2022;
- Acórdão *Tele Sverige2 AB*, de 21 de dezembro de 2016, Proc. nº C-203/15 e C-698, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62015CJ0203&from=pt , acedido pela última vez em 22/01/2022;
- Acórdão Tribunal da Relação de Lisboa, 19 de junho de 2014, nº de processo 1695/09.5PJLSB.L1-9, disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/eb1460fa14510bf380257d080036a9b9?OpenDocument e acedido a 04/01/2022
- Acórdão do Tribunal Constitucional Federal Alemão, de 2 de março de 2010, disponível em http://www.bverfg.de/e/rs20100302_1bvr025608en.html , acedido em 22/12/2021;
- Acórdão do Tribunal Europeu dos Direitos Humanos K.U. vs *Finland*, de 2 de dezembro de 2008, nº de processo 2872/02, disponível em https://hudoc.echr.coe.int/eng?i=001-89964 e acedido em 22/12/2021;
- Acórdão do Tribunal Constitucional nº 420/2017, de 13 de julho, Processo nº 917/16, disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20170420.html , acedido pela última vez a 15/01/2022;
- Acórdão do Tribunal Constitucional nº 403/2015, de 17 de setembro, Proc. nº 773/15, disponível em https://www.tribunalconstitucional.pt/tc/acordaos/20150403.html , acedido a 15/01/2022
- Acórdão do Tribunal Constitucional nº 464/2019, de 21 de outubro, Proc. nº 26/2018, disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20190464.html, acedido a 15/01/2022.