dirittifondamentali.it

**Il Tribunale costituzionale portoghese sulla conservazione dei dati di traffico e localizzazione riconducibili alle comunicazioni**
**(Tribunal Constitucional, Plenário, acórdão 19 aprile 2022 n. 268)**

Vengono dichiarati incostituzionali, per violazione degli artt. 35, commi 1 e 4, 26, comma 1, 18, comma 2 della Costituzione, gli artt. 4 e 6 della legge n. 32/2008, che prevedono che i dati di traffico e localizzazione riconducibili alle comunicazioni siano conservati dai fornitori di servizi di comunicazione elettronica o di una rete pubblica di comunicazioni, per un anno, per finalità di indagine, individuazione e perseguimento di gravi reati. Infatti, il diritto dell'interessato di controllare il trattamento dei dati che lo riguardano e l'effettività della garanzia costituzionale del controllo svolto da un'autorità amministrativa indipendente sono messi a repentaglio, dal momento che non si stabilisce che la conservazione dei dati debba essere effettuata in uno Stato membro dell'Unione europea. Inoltre, il carattere indifferenziato e generalizzato dell'obbligo di conservare tutti i dati di traffico e localizzazione comporta una limitazione sproporzionata dei diritti all'intimità della vita privata e all'autodeterminazione informativa. Viene dichiarato incostituzionale, per violazione degli artt. 35, comma 1, 20, comma 1, 18, comma 2 della Costituzione, anche l'art. 9 della legge n. 32/2008, nella parte in cui non prevede che venga notificata alla persona interessata l'avvenuta consultazione dei dati conservati da parte delle autorità di investigazione penale, una volta che tale comunicazione non sia più idonea a compromettere le indagini o la vita o l'integrità fisica di terzi: pertanto, gli interessati non possono controllare effettivamente la legittimità e la regolarità dell'accesso, risultando così violati i diritti all'autodeterminazione informativa e alla protezione giudiziaria effettiva.

***

Fonte: www.tribunalconstitucional.pt. Il testo riportato non ha carattere ufficiale.

**ACÓRDÃO N.º 268/2022**

Processo n.º 828/2019

Plenário

Relator: Conselheiro Afonso Patrão

**Acordam, em Plenário, no Tribunal Constitucional**

## I. RELATÓRIO

**1.** A Provedora de Justiça requereu, nos termos da alínea *d)* do n.º 2 do artigo 281.º da Constituição, a apreciação e declaração, com força obrigatória geral, da inconstitucionalidade das normas constantes dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de julho, por violarem o princípio da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada e familiar (n.º 1 do artigo 26.º da Constituição), ao sigilo das comunicações (n.º 1 do artigo 34.º da Constituição) e a uma tutela jurisdicional efetiva (n.º 1 do artigo 20.º da Constituição).

**2.** O pedido de declaração de inconstitucionalidade encontra-se fundamentado nos seguintes termos:

«***A. A relação entre a Lei n.º 32/2008, de 17 de julho, e o direito da União Europeia.*** *1.º. Nos termos do disposto no artigo 6.º da Lei n.º 32/2008, de 17 de julho, os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações têm o dever de conservar, pelo período de um ano, os dados de tráfego e de localização de todas as comunicações electrónicas, os quais vêm especificados no artigo 4.º do mesmo diploma.*

*2.º. Trata-se dos dados relativos às subscrições e a todas as comunicações electrónicas necessários para encontrar e identificar a fonte e o destino de uma comunicação (artigo 4.º, n.º 1, alíneas a) e b)), para determinar a data, a hora, a duração e o tipo de comunicação (artigo 4.º, n.º 1, alíneas c) e d)), para identificar o equipamento de telecomunicações dos utilizadores (artigo 4.º, n.º 1, alínea e)) e para identificar a localização do equipamento de comunicação móvel (artigo 4.º, n.º 1, alínea f)).*

*3.º. A obrigação de conservação dos dados abrange os dados gerados ou tratados no âmbito de um serviço telefónico na rede fixa, de um serviço telefónico na rede móvel, de um serviço de acesso à Internet, de um serviço de correio electrónico através da Internet bem como de um serviço de comunicações telefónicas através da Internet.*

*4.º. Esta obrigação também inclui os dados relativos às chamadas telefónicas falhadas (artigo 5.º, n.º 1).*

*5.º. Fora da obrigação de conservação dos dados estão os dados relativos ao conteúdo das comunicações, porquanto, nos termos do disposto no n.° 2 do artigo 1.º, a conservação de tais dados é expressamente proibida.*

*6.º. No que diz respeito às comunicações telefónicas na rede fixa devem ser conservados os dados relativos ao número de telefone de origem e aos números marcados, os dados relativos ao nome e endereço dos assinantes ou dos utilizadores registados (artigo 4.º, n.º 2, alínea a) e n.º 3, alínea a)), os dados relativos à data e hora do início e do fim da comunicação (artigo 4.º, n.º 4, alínea a)), os dados relativos ao serviço telefónico utilizado (artigo 4.º, n.º 5, alínea a)) e os números de telefone de origem e de destino (artigo 4.º, n.º 6, alínea a)). Relativamente às comunicações telefónicas na rede móvel, aplicam-se obrigações suplementares, tais como a conservação da Identidade Internacional de Assinante Móvel (IMSI) e da Identidade Internacional de Equipamento Móvel (IMEI) de quem telefona e do destinatário (artigo 4.º, n.º 6, alínea b)), bem como dos dados de localização do início e do fim da comunicação (artigo 4.º, n.º 7).*

*7.º. No que diz respeito aos serviços de acesso à Internet, aos serviços de correio electrónico através da Internet e às comunicações telefónicas através da Internet devem ser conservados os códigos de identificação atribuídos ao utilizador, o código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública e o nome e endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP, o código de identificação de utilizador ou o número de telefone estavam atribuídos no momento da comunicação (artigo 4.º, n.º 2, alínea b), bem como as datas e horas do início (log in) e do fim (log off) da ligação ao serviço de acesso à Internet ou da ligação, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à Internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado (artigo 4.º, n.º 4, alínea b), subalínea i) ou da ligação ao serviço de correio electrónico através da Internet (artigo 4.º, n.º 4, alínea b), subalínea ii), o serviço de Internet utilizado (artigo 4.º, n.º 5, alínea b) e ainda os dados relativos ao número de telefone que solicita o acesso por linha, a linha de assinante digital ou qualquer outro identificador terminal do autor da comunicação (artigo 4.º, n.º 6, alínea c)).*

*8.º. Em causa estão, portanto, dados que revelam a todo o momento aspectos da vida privada e familiar dos cidadãos, permitindo rastrear a localização do indivíduo ao longo do dia, todos os dias (desde que transporte o telemóvel ou outro dispositivo electrónico de acesso à Internet), e identificar com quem contacta (chamada - inclusive as tentadas e não concretizadas - por telefone ou telemóvel, envio ou recepção de SMS, MMS, de correio electrónico, ou de comunicações telefónicas através da Internet), bem como a duração e a regularidade dessas comunicações.*

*9.º. A Lei n.º 32/2008, de 17 de julho, transpôs para a ordem jurídica nacional a Directiva 2006/24/CE do Parlamento Europeu 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 electrónicas publicamente disponíveis ou de redes públicas de comunicações.*

*10.º. O Tribunal de Justiça da União Europeia (TJUE) declarou a invalidade da referida Directiva no acórdão de 8 de abril de 2014, Digital Rights Ireland Ltd e outros, C-293/12 e C-594/12.*

*11.º. A declaração de invalidade teve por fundamento a violação do princípio da proporcionalidade pela restrição que a Directiva opera dos direitos ao respeito pela vida privada e familiar e à protecção de dados pessoais, consagrados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia (Carta).*

*12.º. Com efeito, apesar de o TJUE ter reconhecido que as medidas previstas na Directiva - relativas à imposição do dever de conservação de dados de tráfego e de localização gerados no contexto de comunicações electrónicas e ao dever da sua transmissão às autoridades competentes para efeitos de investigação, detecção e repressão de crimes graves - eram, em si mesmas, medidas legítimas e adequadas ao fim visado, nem por isso deixou de concluir que as mesmas violavam o princípio da proporcionalidade, na sua dimensão de [do subprincípio da] necessidade.*

*13.º. Tratando-se de um acto de transposição de uma directiva, a Lei n. ° 32/2008, de 17 de julho, consubstancia, para efeitos do disposto no n.º 1 do artigo 51.º da Carta, um acto de aplicação do direito da União Europeia.*

*14.º. Tal significa que, embora tratando-se formalmente de legislação nacional e não de um acto adoptado pelas instituições da União Europeia, a Lei n.º 32/2008, de 17 de julho, está directamente vinculada pela Carta.*

*15.º. Nesta medida, os fundamentos invocados pelo TJUE para sustentar a declaração de invalidade do regime europeu que a Lei n.º 32/2008 pretendeu transpor não poderão deixar de ser tidos em conta, no*

*momento em que se afira da conformidade ou não conformidade em relação à Carta das normas contidas neste regime nacional.*

*16.º. Além disso, resulta do acórdão do TJUE de 21 de dezembro de 2016, Tele2 Sverige e Watson, C-203/15 e C-698/15, que qualquer legislação nacional que preveja a conservação de dados implica necessariamente a existência de disposições relativas ao acesso, por parte das autoridades nacionais competentes, aos dados que sejam conservados pelos prestadores de serviços de comunicações eletrónicas. Assim, e anda que a Directiva 2006/24 tenha sido declarada inválida pelo TJUE, nem por isso a Lei n.º 32/2008, de 17 de julho, poderá deixar de ser incluída no âmbito de aplicação da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (cfr. acórdão Tele2, n.ºs 79-81).*

*17.º. Pelo que não restam dúvidas de que a Lei n.º 32/2008, de 17 de julho, se enquadra no âmbito de aplicação do direito da União, encontrando-se, portanto, a definição pela República Portuguesa do regime legal de conservação de dados de comunicações electrónicas directamente vinculada pela Carta (artigo 51.º, n.º 1 da Carta).*

*18.º. É justamente em virtude da vinculação da legislação nacional à Carta que, no seguimento das decisões do TJUE, a Comissão Nacional de Protecção de Dados (CNPD) emitiu a Deliberação n.º 641/2017, de 9 de Maio, onde expôs a sua perspectiva sobre a Lei n.º 32/2008, considerando que a mesma contém normas que prevêem a restrição ou ingerência nos direitos fundamentais ao respeito pela vida privada e pelas comunicações e à protecção dos dados pessoais com grande amplitude e intensidade, em violação do princípio da proporcionalidade e, portanto, em violação do n.º 1 do artigo 52.º da Carta, bem como uma restrição desproporcionada dos direitos à reserva da intimidade da vida privada, à inviolabilidade das comunicações e à protecção de dados pessoais, em violação do disposto no n.º 2 do artigo 18.º da Constituição da República Portuguesa.*

*19.º. Face a esse seu entendimento, a CNPD, através da Deliberação n.º 1008/2017, de 18 de julho, decidiu desaplicar a Lei n.º 32/2008 nas situações que lhe sejam submetidas para apreciação.*

*20.º. Tendo em conta todos estes dados, poder-se-ia concluir estar-se perante legislação nacional «inteiramente determinada» - na acepção do acórdão do TJUE de 26 de fevereiro de 2013, Âkerberg Fransson, C- 617/10, n.º 29 -, pelo direito da União Europeia, o que geraria dúvidas quanto à questão de saber se caberia ainda à jurisdição constitucional nacional - e não à jurisdição própria da União Europeia - efectuar a 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.*

*21.º. Parece no entanto legítimo sustentar-se que, neste domínio, o legislador nacional definiu com certa margem de liberdade o regime instituído pela Lei n.º 32/2008, pelo que a normação nela contida não deverá ser qualificada como «acção estadual inteiramente determinada pelo Direito da União» na acepção que da expressão faz o acórdão atrás citado. Assim sendo, não estará em causa a competência da jurisdição constitucional nacional para levar a cabo o controlo de compatibilidade entre as medidas aquela legislação previstas e os direitos fundamentais em causa, nomeadamente o direito à reserva da intimidade da vida privada e à protecção dos dados pessoais.*

*22.º. Todavia, sendo embora a legislação nacional em questão «não inteiramente determinada» pelo direito da União Europeia -, e podendo, nessa medida, os órgãos jurisdicionais nacionais aplicar os padrões nacionais de proteção dos direitos fundamentais - em caso algum poderá dessa aplicação resultar um nível de protecção*

*menos elevado do que aquele garantido pela Carta (acórdãos do TJUE de 26 de fevereiro de 2013, Melloni, C-399/11, n.º 60 e Âkerberg Fransson, C-617/10, n.º 29).*

*23.º. Assim é, pelo facto de a Lei n.º 32/2008, atendendo ao que dispõe a Directiva 2002/58/CE do Parlamento e do Conselho, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, ser ainda - não obstante a declaração de invalidade da Directiva 2006/24/CE - um acto de aplicação do Direito da União, encontrando-se por isso, e como já se disse, directamente vinculada pela Carta dos Direitos Fundamentais da União Europeia (artigo 51.º, n.º 1, da Carta).*

*24.º. Ora, embora seja claro que a Lei n.º 32/2008 não padece de alguns dos vícios apontados pelo TJUE à Directiva 2006/24/CE, por outro lado, é também inequívoco que, em aspectos fundamentais do regime nele instituído, esse acto legislativo se não conforma com as exigências decorrentes do direito da União, tal como interpretado pelo TJUE.*

*25.º. O argumento principal em que se baseou o Tribunal Constitucional no acórdão n.º 420/2017, de 13 de Julho, seguindo de perto a Nota Prática n.º 7/2015 do Gabinete do Cibercrime do Ministério Público, é o de que a legislação nacional estabelece já muitas das exigências que não estavam garantidas na Directiva invalidada pelo TJUE, designadamente no que respeita aos requisitos de acesso aos dados conservados bem como no que se refere à imposição da destruição dos dados após o período de conservação.*

*26.º. No entanto, e ao contrário do que é sugerido pela interpretação feita neste aresto, resulta claramente dos acórdãos do TJUE que a circunstância de, no que respeita ao regime de acesso aos dados conservados, a lei nacional poder ir ao encontro das exigências da Carta, em nada releva para efeitos da questão da conformidade à Carta da medida de imposição legal de conservação dos dados em si mesma considerada.*

*27.º. Com efeito, o TJUE, que é o órgão jurisdicional com competência para determinar a correcta interpretação da Carta dos Direitos Fundamentais da União Europeia, nos acórdãos Digital Rights Ireland e Tele2, a que já se fez referência, parte da premissa básica segundo a qual existirão, neste domínio, dois momentos distintos e autónomos de agressão aos direitos fundamentais.*

*28.º. Num primeiro momento, logo com a imposição legal aos operadores de telecomunicações da obrigação de conservação de dados, ocorre já uma agressão – e uma agressão que, só por si, é grave (cfr. acórdão Tele2, n.ºs 99 e segs.) – aos direitos fundamentais.*

*29.º. Ou seja, mesmo que a esses dados nenhuma entidade pública viesse, posteriormente, alguma vez a aceder, já se dera uma agressão grave aos direitos individuais pela mera existência e armazenamento dos dados por parte dos operadores de telecomunicações.*

*30.º. Por sua vez, num segundo momento, que é incerto, o acesso e utilização por parte das entidades públicas competentes consubstancia um nível diferente de agressão aos direitos fundamentais, que vem, por assim dizer, acrescer à agressão – que só por si já é grave – implicada pela mera existência e armazenamento desses dados, agressão essa que, por definição, já terá ocorrido «a montante», e que tem que satisfazer, também ela, exigências decorrentes do princípio da proporcionalidade.*

*31.º. Ora, tratando-se de dois níveis diferentes de agressão aos direitos, não é possível argumentar que o facto de a Lei n.º 32/2008 satisfazer, no que respeita ao regime de acesso aos dados conservados, as exigências decorrentes da Carta, serve para salvar ou compensar a afectação dos direitos implicada na própria imposição legal de conservação de dados. Perante a existência de dois momentos autónomos de agressão aos direitos, não é de todo legítimo confundi-los de acordo com uma «lógica de compensação»*

*32.º. Pelo contrário, uma dogmática correcta de direitos fundamentais exigirá que se analise, autonomamente, a conformidade constitucional de cada uma das agressões aos direitos, em nada podendo o*

*regime de acesso e de utilização dos dados interferir na análise da conformidade constitucional, designadamente e no que respeita às exigências decorrentes do princípio da proporcionalidade, da agressão aos direitos implicada na própria imposição legal de conservação de dados.*

*33.º. No que respeita ao primeiro nível de agressão dos direitos, que se dá com a imposição legal de conservação de dados aos operadores de telecomunicações, e que consubstancia por si só uma agressão grave de liberdades fundamentais (acórdão Tele2, n.º 99 e segs.), o TJUE, nos acórdãos Digital Rights lreland e Tele2, já referidos, estabeleceu exigências claras, desde logo quanto ao âmbito da obrigação de conservação e dados, que a Lei n.º 32/2008, pura e simplesmente, não cumpre.*

*34.º. Na verdade, e quanto ao âmbito da obrigação de conservação de dados impendente sobre os operadores de telecomunicações, o legislador português acolhe a solução que o TJUE expressamente censurou: prevê uma conservação generalizada e indiferenciada de todos os dados de tráfego e dos dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação electrónica, sem limitar tal obrigação em função dos critérios indicados pelo TJUE nos termos do parágr. 106 e seguintes do acórdão Tele2.*

*35.º. Recorde-se que, tendo sido chamado a interpretar legislação nacional de Estados-Membros da União Europeia (Suécia e Reino Unido) que transpunha a Directiva 2006/24/CE, implicando a recolha massiva, indiscriminada de dados das comunicações e obrigando à sua conservação por um período compreendido entre seis meses e dois anos, o TJUE concluiu que «[u]ma regulamentação deste tipo não exige nenhuma relação entre os dados cuja conservação se encontra prevista e uma ameaça para a segurança pública. Nomeadamente, não está limitada a uma conservação que tenha por objeto dados relativos a um período temporal e/ou uma zona geográfica e/ou a um círculo de pessoas que possam estar envolvidas de uma maneira ou de outra numa infração grave, nem a pessoas que, por outros motivos, mediante a conservação dos seus dados, podiam contribuir para a luta contra a criminalidade [ ... ]» (acórdão Tele2, n.º 106).*

*36.º. Tal significa que o TJUE considera ser contrária ao direito da União Europeia qualquer legislação nacional que preveja, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e de todos os dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação electrónica, ou - dizendo o mesmo por outras palavras -, qualquer legislação nacional que obrigue os prestadores de serviços de comunicações eletrónicas a conservarem esses dados de forma sistemática, contínua e sem nenhuma exceção.*

*37.º. Entende o TJUE que tal sistema regulatório excede os limites do estritamente necessário e não pode ser considerado justificado, numa sociedade democrática, como exige o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da Carta (cfr. acórdão Tele2, n.º 97-112).*

*38.º. Ora, na medida em que o sistema estabelecido pela Lei n.º 32/2008, de 17 de julho, pressupõe justamente, em lugar de uma conservação selectiva (cfr. acórdão Tele2, n.º 108), uma conservação generalizada e indiferenciada de todos os dados de tráfego e de todos os dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação electrónica, não há qualquer dúvida de que o regime estabelecido na lei nacional viola a Carta.*

*39.º. Além dessa desconformidade fundamental, relacionada com o próprio âmbito da obrigação de conservação de dados, a lei nacional é desconforme com as exigências decorrentes da jurisprudência do TJUE em matéria de segurança e protecção dos dados conservados.*

*40.º. Com efeito, a Lei n.º 32/2008, de 17 de julho, em nenhuma das alíneas do n.º 1 do artigo 7.º, estabelece especificamente o dever de os dados relativos às comunicações electrónicas serem conservados pelas*

*operadoras de telecomunicações no território da União Europeia de modo a assegurar a efectividade da fiscalização (cfr. acórdão Digital Rights Ireland, n.º 68 e acórdão Tele2, n.º 122 e 125).*

*41.º. Por último, ao não estabelecer expressamente o dever de as autoridades competentes às quais tenha sido concedido o acesso aos dados desse facto informarem as pessoas em causa, no âmbito dos processos nacionais aplicáveis, a partir do momento em que essa comunicação não seja suscetível de comprometer as investigações levadas a cabo por essas autoridades, a Lei n.º 32/2008, de 17 de julho, viola o direito da União Europeia (cfr. acórdão Tele2, n.º 121).*

*42.º. Estando a Lei n.º 32/2008 directamente vinculada pela Carta (artigo 51.º, n.º 1, da Carta), não pode o Tribunal Constitucional aplicar padrões nacionais de proteção dos direitos fundamentais que sejam susceptíveis de comprometer o nível de proteção previsto pela Carta, e, assim, o primado, a unidade e a efetividade do direito da União (acórdãos de 26 de fevereiro de 2013, Melloni, C-399/11, n.º 60 e Âkerberg Fransson, C-617/10, n.º 29).*

*43.º. De outra maneira, verificar-se-ia a situação anómala de, em virtude da interpretação dos direitos fundamentais à luz da Constituição da República Portuguesa, se permitir que na ordem jurídica nacional vigorem normas jurídicas contrárias à Carta dos Direitos Fundamentais da União Europeia.*

*44.º. Pelo que ainda que, no plano jurídico-constitucional, a declaração pelo TJUE da invalidade da Directiva 2006/24/CE não tenha como efeito automático a invalidade da Lei n.º 32/2008, a deliberação do Tribunal Constitucional quanto à conformidade das normas constantes desse acto legislativo com a Constituição da República Portuguesa deve adoptar uma fundamentação que, tanto quanto possível, seja consistente com a do TJUE nos acórdãos Digital Rights Ireland e Tele2.*

*45.º. Em virtude da directa vinculação à Carta da Lei n.º 32/2008, tal «dever de consistência na fundamentação» retira-se do princípio da cooperação leal a que a República Portuguesa - e, portanto, todos os órgãos do Estado, inclusive de índole jurisdicional - se encontra vinculada (artigo 4.º, n.º 3, do Tratado da União Europeia).*

*46.º. Em nosso entender, tanto bastaria para que o Tribunal Constitucional declarasse com força obrigatória geral, a inconstitucionalidade dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, por violação do princípio da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1) e por violação do direito a uma tutela jurisdicional efectiva (artigo 20.º, n.º 1).*

*47.º. Todavia, e independentemente da articulação entre a ordem jurídica nacional e a ordem jurídica europeia, os artigos 4.º, 6.º e 9.º da Lei n.º 32/2008 sempre se hão de considerar inconstitucionais à luz de parâmetros exclusivamente decorrentes do texto da Constituição da República.*

***B. Da violação do direito à reserva da intimidade da vida privada e familiar (artigo 26.º, n. 1)***

***1. Da imposição legal de conservação de dados como agressão – e agressão grave – aos direitos fundamentais.***

*48.º. No acórdão n.º 403/2015, de 27 de Agosto, o Tribunal Constitucional, analisando a pertinente jurisprudência constitucional, reconhece que as circunstâncias em que as comunicações são realizadas integram o âmbito de protecção do direito à reserva da intimidade da vida privada e familiar, consagrado no artigo 26.º, n.º 1, da Constituição Ac. n.º 403/2015, AcTC, 93.º vol., 2015, pp. 45-101, pp. 60 e segs.).*

*49.º. Embora tal argumentação se dirija às questões de constitucionalidade relacionadas com o acesso pelas autoridades competentes a dados de tráfego e de localização, daí não deve retirar-se que a mesma não seja aplicável à própria imposição legal de conservação de dados. O Tribunal Constitucional apenas se não terá expressamente pronunciado sobre esta última dimensão do problema na exacta medida em que, atendendo ao objecto do pedido, tal como delimitado pelo requerente naquele processo, apenas se ocupou especificamente do regime de acesso aos dados, deixando de fora da sua análise o regime legal relativo à própria obrigação de conservação desses dados por parte das operadoras de telecomunicações.*

*50.º. O que é certo é que, argumentar-se que «[ ... ] a manipulação ilegal ou ilegítima do conteúdo e das circunstâncias da comunicação pode violar a privacidade dos interlocutores intervenientes, atentando ou pondo em risco esferas nucleares das pessoas, das suas vidas, ou dimensões do seu modo de ser e estar [.] de sorte que a possibilidade de se aceder aos dados das comunicações colide com um conjunto de valores associados à vida privada que fundamentam e legitimam a proteção jurídico-constitucional» (Ac. n.º 403/2015, AcTC, cit., p. 60), implica reconhecer que, independentemente do eventual acesso aos dados existentes, a mera imposição legal de conservação de dados integra o âmbito de protecção do direito à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1 ).*

*51.º. É isso que, em articulação com o acórdão n.º 128/92, conclui o Tribunal Constitucional: «De modo que, na jurisprudência constitucional, as comunicações privadas, englobando o conteúdo e circunstancialismos em que as mesmas têm lugar, são reconhecidas como um meio através do qual se manifestam aspetos da vida privada da pessoa e que, por isso, caem no âmbito da proteção constitucional da respetiva reserva (Ac. n.º 403/2015, AcTC, cit., p. 61).*

*52.º. Tal significa que, desde logo, a imposição às operadoras de comunicações electrónicas de conservação de dados de tráfego e de localização de todas as comunicações electrónicas consubstancia uma restrição - e uma restrição intensa ou grave - do direito à reserva da intimidade da vida privada e familiar, consagrado no artigo 26.º, n.º 1, da Constituição.*

*53.º. Na verdade, a mera existência de dados, agregados e guardados, por um período de um ano, em centros de conservação [em princípio] detidos e geridos pelas próprias empresas operadoras de telecomunicações, contendo informação extremamente sensível sobre a vida privada e familiar de milhões de cidadãos (supra, ponto 8), é um facto que gera por si só um permanente risco de violação da privacidade, ainda que tais dados nunca venham a ser acedidos, nos termos e para os efeitos legais, pelas autoridades para tal legitimadas.*

*54.º. Com efeito, por muito que se procure assegurar a sua inviolabilidade através da tecnologia a cada momento disponível, não é possível garantir em termos absolutos que não haja falhas de segurança, e que não ocorra o acesso ilegítimo, por parte de terceiros, a todo o manancial de informação que por este meio é conservado.*

*55.º. O problema assumirá ainda maior gravidade se se tiver em linha de conta que a autoridade pública competente para o controlo da aplicação das regras relativas à segurança e proteção de dados, a Comissão Nacional de Protecção de Dados (artigo 7.º, n.º 3, da Lei n.º 32/2008) - autoridade à qual a lei, no seu artigo 14.º, conferiu a competência para a instrução dos processos de contraordenação e para a aplicação das correspondentes coimas -, decidiu, através da Deliberação n.º 1008/2017, de 18 de julho, «desaplicar [a Lei n.º 32/2008] nas situações que lhe sejam submetidas para apreciação», por entender que, sendo as normas nela inscritas lesivas, de acordo com o seu juízo, da Carta dos Direitos Fundamentais da União e da Constituição da República Portuguesa, deveria agir «em cumprimento do primado do Direito da União e da prevalência da Constituição» (supra, pontos 18 e 19). Assim, e face à ausência de fiscalização por parte da*

*autoridade administrativa competente, podem agora os operadores de serviços de telecomunicações não dispor de qualquer desincentivo para incumprir as obrigações que sobre eles impendem, as quais deveriam corresponder às exigências de garantia de um «nível particularmente elevado de protecção e segurança».*

*56.º. O momento de agressão - e de agressão grave - aos direitos dá-se, portanto, logo com a obrigação, imposta às operadoras de telecomunicações, de conservação de todos estes dados. Não fora a previsão legal desta obrigação e jamais seria possível vir a verificar-se o acesso ilegítimo aos dados conservados por parte de terceiros, porquanto tais dados, pura e simplesmente, não existiriam.*

*57.º. A recondução da imposição legal de conservação de dados ao âmbito de protecção do artigo 26.º, n.º 1, é determinante no que respeita aos dados de localização fora do contexto de uma comunicação, se se partir do pressuposto segundo o qual não estarão tais dados cobertos pela garantia constitucional de sigilo das telecomunicações, consagrada no artigo 34.º, n.º 1 da CRP.*

*58.º. Ainda que se parta desse pressuposto - e se considere, como no caso do Acórdão n.º 486/2009, que relativamente a tal tipo de dados se estará sempre fora do âmbito de um acto comunicacional concreto - não poderá jamais esquecer-se 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 electrónico 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 outras pessoas, com quem esteve, onde e quando.*

*59.º. Embora seja predominante e generalizada a percepção segundo a qual a informação contida em dados de tráfego e de localização será menos invasiva da privacidade do que o conhecimento do próprio conteúdo das comunicações, o que é certo é que se invoca a sua indispensabilidade para efeitos de investigação criminal.*

*60.º. Ora, se tais dados fossem inocentes e nada revelassem sobre a vida do indivíduo em causa, então seguramente que nenhum interesse haveria em recorrer a esses dados para efeitos de investigação criminal.*

*61.º. É precisamente por serem extremamente precisos na reconstituição da vida da pessoa em causa - de uma certa perspectiva, mais até do que o próprio conteúdo das comunicações efectuadas – que tais dados se revelam preciosos para as autoridades competentes na área da investigação criminal.*

*62.º. Assim, a imposição legal de conservação, por um período de um ano, de todos os «metadados», incluindo os dados de localização fora do contexto de uma comunicação, constitui, só por si, uma agressão séria e grave do direito à reserva da intimidade da vida privada e familiar, consagrado no artigo 26.º, n.º 1, da Constituição.*

*63.º. A questão que se põe é então a de saber se tal agressão, que, só por si, é séria e grave, se encontrará constitucionalmente justificada, o que implica que se analise a medida à luz das exigências decorrentes do princípio da proporcionalidade (artigo 18.º, n.º 2).*

### *2. Da violação do princípio da proporcionalidade*

*64.º. Nos termos do disposto no artigo 3.º, n.º 1, da Lei n.º 32/2008, de 17 de julho, «a conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, detecção e repressão de crimes graves por parte das autoridades competentes». Nenhuma outra finalidade de interesse público é invocada pelo legislador como justificação para a medida que estabelece uma obrigação geral de conservação de dados.*

*65.º. Embora não haja qualquer informação de ordem quantitativa que nos dê a conhecer a dimensão exacta da realidade que, através da obrigação geral de conservação de dados, o legislador procurou combater, não restam dúvidas de que a [necessidade da] luta contra a criminalidade grave é, em si mesma, razão legítima de*

*restrição de direitos fundamentais. Não apenas por ser tarefa fundamental do Estado a garantia da paz e da segurança, esteio do exercício dos demais direitos e liberdades individuais e do respeito pelo Estado de direito democrático (artigos 9.º e 25.º); mas ainda por se mostrar especialmente adequado que os poderes públicos façam uso dos meios proporcionados pelo progresso tecnológico para levar a cabo a realização de tal tarefa estadual. Os dados de tráfego e de localização constituem pontos de referência em relação ao momento do crime, à localização de suspeitos na zona do crime ou nas suas proximidades, a comportamentos de suspeitos antes e depois do crime, às relações existentes entre os suspeitos, ao itinerário de fuga ou mesmo à indiciação de outros suspeitos. Que o acesso, por parte das autoridades públicas, a todo o acervo de informação que estes dados contêm seja uma medida adequada à prossecução das finalidades enunciadas na lei é pois algo que, em abstracto, não pode ser contestado.*

*66.º. Certo é, no entanto, que já existem na ordem jurídica medidas menos restritivas do que aquelas de que vimos falando - a conservação generalizada e indiferenciada durante todo um ano de todos os «metadados» respeitantes a todos os cidadãos - e que se mostram também elas adequadas à prossecução da finalidade que o n. o 1 do artigo 3.º da Lei n.º 32/2008 enuncia. É o que se verifica com o regime de preservação de dados (quickfreeze), tal como previsto e regulado pelo artigo 12.º da Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime, que transpõe para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa).*

*67.º. Argumentar-se-á porventura, contra o que vimos dizendo, que a eficácia revelada pelo sistema do quick freeze no combate à criminalidade grave não é em si mesma equiparável àquela que é dispensada pelo sistema de conservação generalizada e indiferenciada de todos os «metadados». Nos seus próprios termos, o quick freeze é válido apenas para o caso concreto; e só é ordenado tendo como fundamento [concreto] a verificação de uma determinada suspeita. Em contrapartida, a obrigação geral de conservação de dados, ao permitir às autoridades públicas «a leitura do passado» de quem quer que seja, mostra-se operativa para além de qualquer suspeita que já se tenha, em certo caso concreto, formado. Dizendo de outro modo: enquanto a medida de «preservação de dados» [quickfreeze] só é útil a partir do momento em que se tenha previamente identificado o suspeito da prática de um crime, obrigação geral de conservação de dados será útil bem para além desse momento, na exacta medida em que ela própria facilita a identificação [dos suspeitos]. No combate à «criminalidade grave» não pode pois equiparar-se a eficácia revelada por um e outro sistema conservação generalizada e indiferenciada de dados é bem mais eficaz do que a mera «preservação» dos mesmos (Carlos Pinho, «Lei de retenção de dados de comunicações eletrónicas: aposentar ou reformar?», Revista do Ministério Público 154,2018, pp. 167-192, 179- 185).*

*68.º. No entanto, o facto de certa medida legislativa se mostrar bem mais eficaz do que qualquer outra na realização de bens constitucionalmente protegidos não transforma tal medida em acção legítima, no quadro das restrições admissíveis a direitos e liberdades essenciais. Sendo este um postulado firme da dogmática dos direitos fundamentais, válido para qualquer acção do Estado, a sua aplicabilidade aos domínios da política criminal adquire reverberação especial: nem tudo o que se mostrar especialmente eficaz no combate à criminalidade grave será assim, e só em razão de tal eficácia, constitucionalmente justificado. Nesta medida, carecerá de reavaliação o argumento segundo o qual um sistema de conservação generalizada e indiferenciada de dados seria susceptível de superar o teste da necessidade (em que se analisa o princípio da proporcionalidade) por ser relativamente mais eficaz na luta contra a criminalidade do que um regime de preservação de dados (quick freeze)*

*69.º. Em uma ordem constitucional de liberdade, jamais pode todo e qualquer indivíduo que utilize um meio de comunicação ser tratado como um potencial criminoso em termos de ver sacrificado - e gravemente sacrificado - o seu direito fundamental à reserva da intimidade da vida privada e familiar.*

*70.º. É, no entanto, a necessidade desse mesmo sacrifício que o regime instituído pela Lei n.º 32/2008 assume, ao impor uma conservação generalizada e indiferenciada de todos os dados de tráfego e de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação electrónica. Uma obrigação geral de conservação de dados, ao não prever nenhuma diferenciação, limitação ou excepção em função do objectivo prosseguido - sendo inclusivamente aplicável a pessoas cujas comunicações estejam sujeitas a segredo profissional - afecta globalmente todas as pessoas que utilizem serviços de comunicações electrónicas, sem que essas pessoas se encontrem, ainda que indirectamente, em situação susceptível de justificar um procedimento criminal.*

*71.º. Assim, ao pressupor que todo e qualquer indivíduo deve ser, a título preventivo e de modo contínuo, intensamente vigiado, o regime instituído pela Lei n.º 32/2008 tem por efeito transformar em regra a conservação dos dados de tráfego e de localização. Todavia, de uma adequada aplicação do princípio da proporcionalidade não poderá deixar de retirar-se a ilação contrária. Sendo a intimidade da vida privada uma liberdade essencial, as restrições que os poderes públicos imponham a tal liberdade deverão ocorrer não por regra mas por excepção.*

*72.º. Tal natureza excepcional das restrições sempre poderia vir a ser garantida se o regime legal deixasse de ser absolutamente indeterminado quanto às circunstâncias e às condições em que é legítimo proceder à conservação dos dados – limitando, por hipótese, tal conservação a um período temporal e/ou uma zona geográfica e/ou a um círculo de pessoas que pudessem estar envolvidas de uma maneira ou de outra na prática de infrações graves – e definisse um período mais curto (não de um ano) para a manutenção da obrigação.*

*73.º. A este propósito, importa observar que o Tribunal Constitucional Federal alemão, na decisão de 2 de Março de 2010, que declarou a inconstitucionalidade das alterações introduzidas à Telekommunikationsgesetz e à Strafprozessordnung pela lei que transpusera a Directiva 2006/24/CE, embora tenha considerado que o prazo nela previsto para a conservação de dados, seis meses, não violava os direitos fundamentais, não deixou de observar que se estava já muito próximo daquilo que, de acordo com as exigências decorrentes do princípio da proporcionalidade, seria o limite máximo constitucionalmente admissível.*

*74.º. Elucidativo é ainda o facto de, na sequência dessa decisão, o legislador alemão ter, em 2015, voltado a aprovar uma lei a impor às operadoras de telecomunicações a conservação de dados - até então e desde 2010, com a declaração de inconstitucionalidade das alterações introduzidas à Telekommunikationsgesetz e à Strafprozessordnung pela lei que transpusera a Directiva 2006/24/CE. não havia enquadramento legal nesta matéria -, reduzindo substancialmente os limites máximos da duração da conservação de dados. Agora, na República Federal da Alemanha, e em virtude da aprovação da Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, de 10 de Dezembro de 2015, (BGBl. I S. 2218 ff.), foram introduzidas alterações à Telekommunikationsgesetz, de 22 de Junho de 2004, (BGBl. I S. 1190), prevendo-se no § 113b desta última um prazo máximo de conservação de 10 semanas no que respeita a dados de tráfego e um prazo máximo conservação de 4 semanas no que se refere a dados de localização".*

*75.º. De acordo com as motivações expressas pelo legislador, este regime procuraria responder à necessidade de dispersar, ou de pelo menos evitar uma excessiva concentração, [d]os dados conservados. Ao limitar a*

*quatro semanas o período de conservação dos dados de localização, a lei alemã não só se mostra particularmente sensível à qualidade e delicadeza da informação que este tipo de dados transmite, como procura ainda impedir que, para além desse período, se possa concentrar toda essa informação através do «cruzamento» dos dados de tráfego com os dados de localização, com a consequente largueza de conhecimentos - e, logo, de possibilidade de reconstituição do passado de cada um - que tal «cruzamento» faculta.*

*76.º. Em Portugal, a imposição legal de conservação de dados, com a amplitude, duração e indiferenciação que decorre dos artigos 4.º e 6.º, da Lei n.º 32/2008, de 17 de julho, ao aplicar a mesma disciplina jurídica a qualquer que seja a categoria de dados em causa e ao impor a conservação dos dados por um período indevidamente longo, traduz uma restrição excessiva do direito individual à privacidade. Mas comporta, do mesmo passo, o risco de lesão efectiva de outros direitos e liberdades, constitucionalmente consagrados.*

*77.º. Com efeito, a conservação de tamanha amplitude de dados respeitantes às circunstâncias de todas as comunicações efectuadas por todos os cidadãos (destinatários [pertença a determinadas categorias profissionais, instituições, associações ou grupos de representação de interesses], data, hora e localização das chamadas telefónicas), permite, ao combinar e cruzar esses dados, inferir, com precisão, informações detalhadas sobre padrões de vida individuais, círculos sociais de pertença, inclinações político-partidárias, bem como aspectos da vida pessoal, tais como rotinas, hobbies, vulnerabilidades (por exemplo, em matéria de saúde). Além da agressão que tal constitui para cada indivíduo, enquanto titular de um direito básico à reserva da privacidade, do acesso ilegítimo de terceiros a todo este manancial de informação podem resultar constrições graves ao exercício de outros direitos e liberdades, nomeadamente os que se encontram consagrados no Capítulo II do Título II da Parte Primeira da Constituição da República.*

***C. Da violação do sigilo das comunicações (artigo 34.º, n.º 1)***

*78.º. O artigo 34.º, n.º 1, consagra o sigilo das comunicações, o qual protege contra o conhecimento por parte do poder público a transmissão, com a ajuda dos meios de comunicação disponíveis, de informação a receptores individuais.*

*79.º. O sigilo das comunicações abrange não apenas o conteúdo do que é transmitido entre o emissor e o receptor mas também as circunstâncias da comunicação, designadamente se, quando, com que frequência, através de que meio de comunicação e entre quem é que são estabelecidas comunicações.*

*80.º. O Tribunal Constitucional, chamado a pronunciar-se sobre a questão, não teve qualquer dúvida em considerar que «[ ... ] a proibição de ingerência nas comunicações, constante do artigo 34.º da CRP, abrange os dados de tráfego» (Ac. n.º 403/2015, cit., p. 65).*

*81.º. Uma vez mais, importa aqui observar que, embora tal argumentação seja feita a propósito do acesso pelo Estado a dados de tráfego e de localização, daí se não deve retirar que o mesmo não seja aplicável à própria imposição legal de conservação de dados. O Tribunal Constitucional apenas se não terá expressamente pronunciado sobre essa dimensão do problema na exacta medida em que, atendendo ao objecto do pedido, tal como delimitado pelo requerente nesse processo, apenas se ocupou especificamente do regime de acesso aos dados, deixando de fora da sua análise o regime legal relativo à própria imposição legal de conservação de dados às operadoras de telecomunicações.*

*82.º. Aliás, a construção dogmática elaborada nesse aresto e que serve de suporte à construção do direito à autodeterminação comunicativa, nos termos do qual o mesmo se analisa «[ ... ] em uma dupla vertente, enquanto proteção de uma reserva da vida privada e enquanto liberdade de atuação, ou seja, uma conexão*

*entre "segredo das comunicações" e "liberdade de comunicação"» (Ac. n.º 403/2015, AcTC, cit., p. 63), densifica a protecção constitucional, tomando claro que as questões de constitucionalidade relativas ao acesso, de que especificamente se ocupa o n.º 4 do artigo 34.º, são apenas uma das múltiplas dimensões da protecção constitucional globalmente conferida por esse preceito constitucional.*

*83.º. A protecção que a Constituição confere respeita não apenas ao momento de acesso por parte das autoridades públicas, mas a cada acto do poder público susceptível de afectar o sigilo das telecomunicações.*

*84.º. O acto do legislador consistente em impor às operadoras de telecomunicações, por um período de um ano, uma conservação generalizada e indiferenciada de todos os dados de tráfego e dos dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação electrónica, consubstancia, em si mesmo considerado - e independentemente das disposições que visam regular o seu posterior eventual acesso por parte das autoridades -, uma agressão - e uma agressão grave - por parte do Estado ao sigilo das comunicações, constitucionalmente garantido no artigo 34.º, n.º 1.*

*85.º. No mesmo sentido concluiu o Tribunal Constitucional Federal alemão na já referida decisão de 2 de Março de 2010, a respeito da disposição da Lei Fundamental alemã que, em termos equivalentes ao artigo 34.º, n.º 1, da Constituição portuguesa, consagra o sigilo das comunicações.*

*86.º. A questão que se põe é, uma vez mais, a de saber se tal agressão, que, só por si, é séria e grave, será constitucionalmente justificada, o que implica que se analise a medida à luz das exigências decorrentes do princípio da proporcionalidade (artigo 18.º, n.º 2).*

*87.º. Nestes termos, serão também aqui aplicáveis as considerações feitas a propósito da desproporcionalidade da restrição do direito à reserva da intimidade da vida privada (supra, pontos 64-77).*

*88.º. Isto é assim, desde logo, em virtude da dupla vertente do direito à autodeterminação comunicativa, considerando que entre os diferentes bens-jurídico constitucionais através deste direito protegidos se encontra a reserva da intimidade da vida privada (Ac. n.º 40312015, cit., p. 62).*

*89.º. Mas também no que respeita à outra vertente do direito à autodeterminação comunicativa, centrada no domínio de actuação do indivíduo – liberdade para comunicar e liberdade para desenvolvimento das relações interpessoais – não deixam de valer as considerações anteriormente expendidas.*

*90.º. Por muito elevado que seja o peso a atribuir à razão de interesse público que sustenta a medida de conservação de dados - uma maior eficácia na luta contra a criminalidade grave -, tal peso não justifica a intensidade do sacrifício imposto ao direito ao sigilo das comunicações: o indivíduo viver com a sensação de estar a ser permanentemente vigiado e, por causa disso, retrair-se e inibir-se na comunicação com as outras pessoas para não deixar rasto do exercício de liberdades que a Constituição tem como fundamentais.*

*91.º. Pelo que deve entender-se que a imposição legal de conservação de dados, com a amplitude, duração e indiferenciação que decorrem dos artigos 4.º e 6.º, da Lei n.º 32/2008, de 17 de julho, ao aplicar a mesma disciplina jurídica a qualquer que seja a categoria de dados em causa e ao impor a conservação dos dados por um período indevidamente longo, constitui uma restrição desproporcionada do sigilo das telecomunicações, consagrado no artigo 34.º, n.º 1, da Constituição.*

***D. Da violação do direito a uma tutela jurisdicional efectiva (artigo 20.º, n.º 1)***

*92.º. A Lei n.º 32/2008, de 17 de julho, não prevê que as autoridades nacionais competentes às quais é concedido o acesso aos dados conservados informem desse facto as pessoas em causa, no âmbito dos processos aplicáveis.*

*93.º. Esse dever de comunicação ao interessado não está assegurado em nenhum outro lugar da ordem jurídica (não sendo nomeadamente previsto pelo Código de Processo Penal).*

*94.º. Não se vê, porém, como pode vir a ser cumprido o princípio constitucional da tutela jurisdicional efectiva, constante do artigo 20.º da Constituição da República, sem a consagração legal deste dever de comunicação. O artigo 9.º da Lei n° 32/2008 define o procedimento que deve ser seguido para que os dados conservados pelas operadoras possam ser transmitidos às autoridades competentes. Todavia, o facto de se não prever, em momento algum desse procedimento, a necessidade de informar o interessado (a pessoa a que se referem os dados que foram transmitidos) quanto à existência mesma do procedimento, faz com que tal existência se tome imperceptível aos olhos de quem por ela é afectado. Nestas circunstâncias, comprometidas ficam, 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 reacção e defesa contra eventuais acessos ilegítimos a essa mesma informação.*

*95.º. Porque assim é, a circunstância de, nos termos do disposto no artigo 9.º, da Lei n.º 32/2008, de 17 de julho, o eventual acesso aos dados por parte das autoridades competentes ser precedido de autorização judicial por parte do juiz de instrução em nada altera os dados da questão; como em nada os altera a circunstância de a comunicação poder vir a comprometer as investigações levadas a cabo pelas autoridades competentes. Para que o procedimento previsto no artigo 9.º da Lei n.º 32/2008 se mostre inteiramente conforme com o disposto no artigo 20.º da CRP necessário é que a comunicação à pessoa afectada se faça, ainda que tal ocorra apenas a partir do momento em que a mesma [comunicação] não seja já susceptível de comprometer as investigações (supra, ponto 41).*

*96.º. 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 a frustração da investigação ou perigo para a vida ou integridade física de terceiros. Todavia, em tais circunstâncias, a conformidade do regime legal com as exigências constitucionais que vimos mencionando exigirá que a decisão de não-comunicação, além de fundamentada, seja judicialmente validada.*

*97.º. Todavia, o regime instituído pela Lei n° 32/2008 é todo ele silente quanto a este dever de comunicação, seja ele cumprido em que momento for e tenha ele as excepções que tiver.*

*98.º. Tal confere, em nosso entender, um argumento adicional para a declaração de inconstitucionalidade do disposto nos artigos 4.º e 6.º da referida lei. A imposição legal de conservação de dados que nestes artigos se prevê, para além de infringir, pela sua amplitude, duração e indiferenciação, as normas constitucionais relativas à reserva de privacidade e ao sigilo das comunicações, não permite que o interessado tenha qualquer controlo sobre o destino dos dados que são conservados, assim se excluindo a possibilidade de defesa perante um eventual acesso ilegítimo. Nestes termos, também por este motivo será inconstitucional o regime decorrente dos artigos 4.º e 6.º da Lei n.º 32/2008.*

*99.º. No entanto, constitui por si só uma violação do disposto no artigo 20.º, n.º 1, da Constituição da República o facto de o artigo 9.º da Lei n.º 32/2008 em momento algum prever a necessária comunicação aos interessados, sempre que os dados conservados sejam, nas condições aí definidas, transmitidos às autoridades competentes. A ausência, do conteúdo prescritivo deste artigo 9.º, de uma qualquer disciplina jurídica que garanta - quiçá através da previsão de um procedimento próprio - que as pessoas possam exercer o seu direito a uma tutela jurisdicional efectiva contra acessos ilegítimos por parte das autoridades aos dados conservados, toma, em nosso entender, todo o regime naquele artigo instituído contrário à ordem constitucional portuguesa.*

*Nestes termos, requer-se ao Tribunal Constitucional que aprecie e declare, com força obrigatória geral:*
*(i) a inconstitucionalidade, por violação do princípio da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1) e ao sigilo das comunicações (artigo 34.º, n.º 1) e por violação do direito a uma tutela jurisdicional efectiva (artigo 20.º, n.º 1), do disposto nos artigos 4.º e 6.º, da Lei n.º 32/2008, de 17 de julho;*
*(ii) a inconstitucionalidade, por violação do direito a uma tutela jurisdicional efectiva (artigo 20.º, n.º 1), do disposto no artigo 9.º da Lei n.º 32/2008, de 17 de julho*».

**3.** Notificado nos termos conjugados do artigo 54.º e do n.º 3 do artigo 55.º da Lei n º 28/82, de 15 de novembro (Lei de Organização, Funcionamento e Processo no Tribunal Constitucional [LTC]), o Presidente da Assembleia da República ofereceu o merecimento dos autos. Ademais, remeteu uma nota técnica elaborada pelos serviços de apoio à Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, relativa aos trabalhos preparatórios que conduziram à aprovação da Lei n.º 32/2008, de 17 de julho, e dando conta da jurisprudência entretanto produzida sobre as normas fiscalizadas.

**4.** Discutido o memorando elaborado pelo Presidente do Tribunal, nos termos e para os efeitos do disposto no n.º 1 do artigo 63.º da LTC, e fixada a orientação do Tribunal, cumpre agora decidir em conformidade com o que então se estabeleceu.

**II. FUNDAMENTAÇÃO**

**5.** Assiste legitimidade à requerente para pedir a declaração de inconstitucionalidade de quaisquer normas, com força obrigatória geral, por força do disposto na alínea *d)* do n.º 2 do artigo 281.º da Constituição.

**6.** A Lei n.º 32/2008, de 17 de julho, transpôs para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu 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. Aquele ato legislativo regula a conservação e a transmissão dos dados de identificação, tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes.
A requerente solicita a fiscalização das normas contidas nos seus artigos 4.º, 6.º e 9.º.
O artigo 4.º identifica as categorias de dados a armazenar pelos fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações; o artigo 6.º determina a obrigação da sua conservação pelo período de um ano, a contar da data da conclusão da comunicação; e o artigo 9.º estabelece as condições de transmissão de dados armazenados ao Ministério Público ou à autoridade de polícia criminal competente:

Artigo 4.º

**Categorias de dados a conservar**

1 — Os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis ou de uma rede pública de comunicações devem conservar as seguintes categorias de dados:

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

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

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

*d*) Dados necessários para identificar o tipo de comunicação;

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

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

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

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

*i*) O número de telefone de origem;

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

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

*i*) Os códigos de identificação atribuídos ao utilizador;

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

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

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

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

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

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

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

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

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

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

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

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

*i*)A data e a hora do início *(log in)* e do fim *(log off)* da ligação ao serviço de acesso à Internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à Internet a uma comunicação, bem como o código de identificação de utilizador do subscritor ou do utilizador registado;
*ii*) A data e a hora do início e do fim da ligação ao serviço de correio eletrónico através da Internet ou de comunicações através da Internet, com base em determinado fuso horário.
5 — Para os efeitos do disposto na alínea *d*) do n.º 1, os dados necessários para identificar o tipo de comunicação são os seguintes:
*a*) No que diz respeito às comunicações telefónicas nas redes fixa e móvel, o serviço telefónico utilizado;
*b*) No que diz respeito ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet, o serviço de Internet utilizado.
6 — Para os efeitos do disposto na alínea *e*) do n.º 1, os dados necessários para identificar o equipamento de telecomunicações dos utilizadores, ou o que se considera ser o seu equipamento, são os seguintes:
*a*) No que diz respeito às comunicações telefónicas na rede fixa, os números de telefone de origem e de destino;
*b*) No que diz respeito às comunicações telefónicas na rede móvel:
*i*) Os números de telefone de origem e de destino;
*ii*) A Identidade Internacional de Assinante Móvel (*International Mobile Subscriber Identity*, ou IMSI) de quem telefona;
*iii*) A Identidade Internacional do Equipamento Móvel (*International Mobile Equipment Identity*, ou IMEI) de quem telefona;
*iv*) A IMSI do destinatário do telefonema;
*v*) A IMEI do destinatário do telefonema;
*vi*) No caso dos serviços pré-pagos de carácter anónimo, a data e a hora da ativação inicial do serviço e o identificador da célula a partir da qual o serviço foi ativado;
*c*) No que diz respeito ao acesso à Internet, ao correio eletrónico através da Internet e às comunicações telefónicas através da Internet:
*i*) O número de telefone que solicita o acesso por linha telefónica;
*ii*) A linha de assinante digital (*digital subscriber line*, ou DSL), ou qualquer outro identificador terminal do autor da comunicação.
7 — Para os efeitos do disposto na alínea *f*) do n.º 1, os dados necessários para identificar a localização do equipamento de comunicação móvel são os seguintes:
*a*) O identificador da célula no início da comunicação;
*b*) Os dados que identifiquem a situação geográfica das células, tomando como referência os respetivos identificadores de célula durante o período em que se procede à conservação de dados.

Artigo 6.º
**Período de conservação**
As entidades referidas no n.º 1 do artigo 4.º devem conservar os dados previstos no mesmo artigo pelo período de um ano a contar da data da conclusão da comunicação.

Artigo 9.º

**Transmissão dos dados**

1 — A transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada, por despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves.

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

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

*a)* Ao suspeito ou arguido;

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

*c)* A vítima de crime, mediante o respetivo consentimento, efetivo ou presumido.

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

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

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

Na Lei n.º 32/2008, de 17 de julho, são identificáveis dois regimes jurídicos em torno dos dados identificados no artigo 4.º: um relativo à *obrigação de conservação* pelos fornecedores de serviços de comunicações eletrónicas ou de uma rede pública de comunicações, essencialmente contido nos artigos 4.º a 8.º; e outro atinente ao seu *acesso* pelas autoridades competentes para a investigação e repressão criminal, estatuído nos artigos 9.º a 11.º.

A requerente solicita a fiscalização da constitucionalidade do regime jurídico da *conservação dos dados* (quanto ao seu âmbito e duração) e, bem assim, da norma que disciplina a *transmissão* dos dados às autoridades competentes para a investigação, deteção e repressão de crimes graves.

**6.1.** No que tange ao regime de *conservação dos dados,* prevê-se uma obrigação, para os fornecedores de serviços de comunicações eletrónicas ou de uma rede pública de comunicações, de preservação dos dados elencados no artigo 4.º, relativos a quaisquer utilizadores e assinantes.

O n.º 1 do artigo 4.º prescreve a conservação de dados que permitam identificar o assinante ou utilizador, a fonte, o destino, data, hora, duração e o tipo de comunicação, bem como identificar o equipamento de telecomunicações e a sua localização. A obrigação abrange os dados relativos às subscrições e a todas as comunicações eletrónicas necessários para encontrar e identificar a fonte e

o destino de uma comunicação (alíneas *a)* e *b)* do n.º 1 do artigo 4.º), para determinar a data, a hora, a duração e o tipo de comunicação (alíneas *c)* e *d)* do n.º 1 do artigo 4.º), para identificar o equipamento de telecomunicações dos utilizadores (alínea *e)* do n.º 1 do artigo 4.º) e para identificar a localização do equipamento de comunicação móvel (alínea *f)* do n.º 1 do artigo 4.º). O que compreende os dados gerados ou tratados no âmbito de serviços telefónicos na rede fixa, de serviços telefónicos na rede móvel, de serviços de acesso à internet, de serviços de correio eletrónico através da internet e de serviços de comunicações telefónicas através da internet.

A obrigação legalmente determinada para os fornecedores de serviços de comunicações eletrónicas é a de conservar tais dados por um período de um ano a contar da data da conclusão da comunicação (artigo 6.º), com a finalidade exclusiva de, se necessário, poderem ser utilizados para «*investigação, deteção e repressão de crimes graves por parte das autoridades competentes*» (n.º 1 do artigo 3.º). Em consequência, não se permite ao titular dos dados que se oponha à conservação (n.º 4 do artigo 3.º) e determina-se que os ficheiros destinados à conservação de dados estejam separados de quaisquer outros (n.º 3 do artigo 3.º). Não se prevê qualquer exceção para as comunicações que possam estar tuteladas por regimes legais de sigilo profissional; todavia, o legislador não ignorou a respetiva proteção, levando-a em consideração *no momento em que é solicitada a sua transmissão* às autoridades de investigação criminal (n.º 4 do artigo 9.º).

O legislador previu um dever de conservação *com a mesma segurança e proteção que os dados na rede* (alínea *b)* do n.º 1 do artigo 7.º da Lei n.º 32/2008, de 17 de julho) e disciplinou que a sua transmissão eletrónica às autoridades ocorresse «*nos termos das condições técnicas e de segurança fixadas em portaria conjunta dos membros do Governo responsáveis pelas áreas da administração interna, da justiça e das comunicações, que devem observar um grau de codificação e proteção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados*» (n.º 3 do artigo 7.º), subordinando o controlo dessas regras à Comissão Nacional de Proteção de Dados [CNPD], nos termos do n.º 5 do artigo 7.º. Em conformidade, a Portaria n.º 469/2009, de 6 de maio, alterada pelas Portarias n.ºs 915/2009, de 18 de agosto, e 694/2010, de 16 de agosto, estabeleceu medidas relativas às condições técnicas e de segurança dos dados conservados. O ato regulamentar incide essencialmente sobre a segurança da *transmissão dos dados* às autoridades públicas, instituindo uma aplicação informática específica e prevendo regras para todo o procedimento de transmissão. Não versa, porém, sobre os requisitos de segurança da *conservação de dados pelos operadores* — aludindo-se apenas à obrigação de os sujeitar «*à mesma segurança e proteção que os dados na rede*» (alínea *b)* do n.º 1 do artigo 7.º da Lei n.º 32/2008, de 17 de julho).

Por outro lado, as disposições relativas à conservação de dados (essencialmente contidas no artigo 7.º da Lei n.º 32/2008, de 17 de julho) não impõem que o seu armazenamento ocorra em Portugal (ou em outro Estado-Membro da União Europeia).

Os dados referidos no artigo 4.º não abrangem o conteúdo das comunicações, dizendo respeito somente às suas circunstâncias — razão pela qual são usualmente designados por *metadados* (ou dados sobre dados) — cfr. Acórdãos n.ºs 403/2015 e 420/2017:

«*Numa concreta comunicação é possível separar do núcleo duro da informação fornecida ou transmitida um conjunto de marcos ou pontos de referência que lhe dão o respetivo suporte e que permitem circunscrever a informação sob todas as formas. Tais dados são 'informações' que acrescem aos dados e que têm como objetivo*

*informar sobre eles, em princípio, para tornar mais fácil a sua organização. Sendo dados sobre dados ('informação sobre informação'), acabam por fornecer informação sobre a localização, tempo, tipo de conteúdo, origem e destino, entre outras, dos atos comunicacionais efetuados através de telecomunicações ou por outros meios de comunicação.*

*Como categoria que tem por fim um efeito jurídico é de usar a designação 'dados de tráfego' (…) porque no nosso ordenamento jurídico já há uma definição legal desse enunciado. Com efeito, o artigo 2.º, n.º 1, alínea d), da Lei n.º 41/2004, de 18 de agosto, sobre Segurança nas Telecomunicações, define 'dados de tráfego' como 'quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma'.*

*A este propósito, o Tribunal Constitucional acolheu, desde o Acórdão n.º 241/2002, de 29/05/2002, uma classificação tripartida (louvando-se, então, nos Pareceres do Conselho Consultivo da Procuradoria-Geral da República n.º 16/94, votado em 24/06/94, na base de dados da DGSI, n.º 16/94 – complementar, votado em 2/05/1996, in Pareceres, vol. VI, págs. 535 a 573, e n.º 21/2000, de 16/06/2000, no Diário da República – II Série, de 28/08/2000) dos dados resultantes do serviço de telecomunicações. Ali se distinguiram: '(…) os dados relativos à conexão à rede, ditos dados de base; os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência), dados de tráfego; dados relativos ao conteúdo da comunicação ou da mensagem, dados de conteúdo'».*

O conjunto de *metadados* elencado no artigo 4.º abrange dados de diferente natureza, categorizados na jurisprudência constitucional como *dados de base* e *dados de tráfego*. A distinção é relevante, pois a tutela constitucional não é modelada nos mesmos termos para as duas espécies.

Os *dados de base* referem-se à conexão à rede, independentemente de qualquer comunicação, permitindo a identificação do utilizador de certo equipamento — nome, morada, número de telefone (Acórdãos n.ºs 241/2002, 486/2009, 403/2015, 420/2017 e 464/2019); como se disse no Acórdão n.º 486/2009, reproduzindo os Pareceres n.ºs 16/94 e 21/2000 do Conselho Consultivo da PGR, «*Os dados de base constituem, na perspetiva dos utilizadores, os elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respetivo serviço: interessa aqui essencialmente o número e os dados através dos quais o utilizador tem acesso ao serviço*». Já os dados de tráfego são definidos como «*os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência)*» (Acórdão n.º 403/2015); «*Constituem, pois, elementos já inerentes à própria comunicação, na medida em que permitem identificar, em tempo real ou a posteriori, os utilizadores, o relacionamento direto entre uns e outros através da rede, a localização, a frequência, a data, hora e a duração da comunicação, devem participar das garantias a que está submetida a utilização do serviço, especialmente tudo quanto respeite ao sigilo das comunicações*» (Acórdão n.º 486/2009, reproduzindo os Pareceres n.ºs 16/94 e 21/2000 do Conselho Consultivo da PGR)

A norma abrange ambas as categorias de *metadados*: ao determinar a conservação de dados relativos a «*nome do assinante ou do utilizador registado*», «*códigos de identificação atribuídos ao utilizador*», «*O código de identificação do utilizador e o número de telefone atribuídos a qualquer comunicação que entre na rede telefónica pública*» e «*nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP estava atribuído*», alcançam-se os designados *dados de*

*base,* que não pressupõem qualquer comunicação (abrangendo até uma fase prévia à comunicação), visando a identificação do utilizador do aparelho que se conexiona à rede. Por outro lado, ao estabelecer a conservação de dados gerados a propósito de uma certa comunicação (dados relativos à data, hora e duração de comunicações, protocolos IP estáticos e dinâmicos, hora e data de início [*log in*] e fim [*log off*] de ligação à internet), compreendem -se os *dados de tráfego*, aqueles que são produzidos pelo estabelecimento de uma *certa comunicação* ou sua tentativa.

Importa traçar dois sublinhados no que respeita à subsunção dos dados mencionados no artigo 4.º da Lei n.º 32/2008 na categorização seguida pelo Tribunal Constitucional (*dados de base* e *dados de tráfego*).

A primeira nota refere-se aos *endereços de protocolo IP*. Estes são habitualmente inseridos na categoria de *dados de base*, por não revelarem quaisquer circunstâncias da comunicação — mas apenas a identificação do computador que se conectou à rede. Todavia, se se contrapuser a identificação de um utilizador de um *número de telefone* com a do *protocolo IP*, subjazem diferenças importantes, que o Tribunal Constitucional Federal Alemão assinalou no Acórdão do 1. Senat, de 2 março de 2010 — 1 BvR 256/08; 1 BvR 263/08; 1 BvR 586/08, §259: os números de telefone são, em princípio, caracteres *permanentes*, pelo que a identificação do sujeito a que pertencem pode ser obtida independentemente de qualquer comunicação. Pelo contrário, os protocolos IP podem ser *estáticos* (identificando permanentemente um ponto de acesso à rede) ou *dinâmicos* (sendo atribuídos a certo computador *apenas no momento em que se conexiona à rede e durante a sua ligação*). Quer isto dizer que a identificação de um protocolo IP dinâmico envolve informação da sua utilização *num determinado momento*, revelando não apenas o utilizador como também o uso da internet em certo contexto.

Neste quadro, a identificação do sujeito a que estava atribuído determinado *protocolo IP dinâmico* não permite, de forma tão clara, obedecer à divisão entre *dados de base* e *dados de tráfego*, pois certas circunstâncias da comunicação (a data e a hora) são inerentes à identificação do protocolo de IP dinâmico. Foi essa a razão pela qual o Tribunal Constitucional Federal Alemão, no Acórdão de 17 de julho de 2020 (1 BvR 1873/13 - 1 BvR 2618/13), entendeu que a identificação do titular de um *protocolo IP dinâmico*, ao pressupor uma consulta do tráfego para identificar o utilizador em dado momento, se enquadra nos *dados de tráfego*, eventualmente submetidos no âmbito do direito à inviolabilidade das comunicações (§§ 101 e 102 do Acórdão).

A segunda nota liga-se à natureza dos designados *"dados de localização"*, definidos pela alínea *c)* do artigo 2.º da Diretiva 2002/58/CE como «*quaisquer dados tratados numa rede de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas publicamente disponível*». Reconduzindo aquele conceito às categorias de metadados reconhecidas pelo Tribunal Constitucional, a informação relativa à localização do equipamento pode enquadrar-se nos *dados de base* (quando identifica a posição geográfica do aparelho, independentemente de qualquer comunicação) ou nos *dados de tráfego* (quando esta identificação está associada a uma comunicação ou tentativa de comunicação — onde estava o sujeito A quando comunicou com o sujeito B). Sucede que a primeira espécie dos dados de localização (a que não pressupõe comunicações) é residual, como notou o Tribunal Constitucional no Acórdão n.º 464/2019: «*segundo o parecer da CNPD n.º 38/2017, nos dias de hoje ocorrem comunicações mesmo quando o utilizador do equipamento de comunicação não o aciona direta e intencionalmente. É, por exemplo, o caso*

*das atualizações efetuadas pelas aplicações de correio eletrónico ou outro tipo de mensagens, o que significa que a geração e troca de dados são praticamente constantes, mesmo quando os cidadãos utilizadores dos equipamentos nada fazem»*. Por essa razão, «*tem-se considerado que os mesmos estão também incluídos no conceito mais amplo de "dados de tráfego"*» (Acórdão n.º 403/2015), ideia que aqui se reafirma.

**6.2.** No que respeita ao *acesso aos dados* pelas autoridades competentes para investigação, deteção e repressão criminal, exige-se a autorização do juiz de instrução, requerida pelo Ministério Público ou pela autoridade de polícia criminal competente, ficando subordinada à existência de «*razões para crer que a obtenção desses dados é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter no âmbito da investigação, deteção e repressão de crimes graves*» (n.ºs 1 e 2 do artigo 9.º da Lei n.º 32/2008, de 17 de julho).

Por outro lado, estabelece-se um catálogo taxativo de crimes cuja investigação ou repressão pode consentir o acesso: os «crimes graves» — «*crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima*» (alínea *g)* do n.º 1 do artigo 2.º), sendo certo que os conceitos de «criminalidade violenta» e de «criminalidade altamente organizada» são densificados no artigo 1.º do Código de Processo Penal (CPP). Trata-se, assim, de um leque de infrações mais restrito do que aquele que admite a interceção e gravação de conversações ou comunicações telefónicas, determinada pelo juiz num processo penal em curso (cfr. artigo 187.º do Código de Processo Penal). Ademais, circunscreve-se o universo subjetivo de potenciais visados ao suspeito ou arguido, à pessoa que sirva de intermediário (relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido) ou à vítima de crime, mediante o respetivo consentimento (n.º 3 do artigo 9.º).

O legislador incidiu ainda sobre as condições da transmissão dos dados às autoridades de investigação criminal, não apenas determinando a sua comunicação eletrónica (artigo 10.º) como estabelecendo a observância de condições técnicas e de segurança determinadas por ato regulamentar. Ora, na Portaria n.º 469/2009, de 6 de maio, alterada pelas Portarias n.ºs 915/2009, de 18 de agosto, e 694/2010, de 16 de agosto, previu-se (artigo 2.º) uma aplicação informática específica ("sistema de acesso ou pedido de dados às operadoras de comunicações" [SAPDOC]) através da qual «*o processo de transmissão e acesso aos dados decorre, através de ligação segura, encriptada mediante nome de utilizador e palavra passe, através de obrigação de registo eletrónico dos pedidos de dados enviados, incluindo a indicação de quem procedeu ao envio e da data e hora em que o mesmo ocorreu, bem como dos acessos a ficheiros de resposta, igualmente com indicação de quem os efetuou e da data e hora de cada acesso*» (DAVID SILVA RAMALHO e JOSÉ DUARTE COIMBRA, "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", *O Direito*, Ano 147, 2015, p. 1037). Ademais, cabe aos operadores de telecomunicações «*elaborar registos da extração dos dados transmitidos às autoridades competentes e enviá-los trimestralmente à CNPD*» (n.º 6 do artigo 9.º), comunicando assim à entidade responsável pela fiscalização *quais os dados transmitidos às autoridades de investigação criminal.*

Depois da transmissão dos dados, o legislador disciplinou a sua destruição, prevendo a sua determinação pelo juiz, oficiosamente ou a requerimento de qualquer interessado, logo que deixem de ser estritamente necessários para os fins a que se destinam — o que sucederá nos casos de arquivamento definitivo do processo penal; absolvição ou condenação transitadas em julgado; prescrição do procedimento penal; e amnistia (artigo 11.º).

Em suma, as normas fiscalizadas consagram um catálogo taxativo de infrações penais que podem dar lugar à *transmissão de dados*, condicionando-a ainda aos casos em que esta seja indispensável para a descoberta da verdade ou quando a prova seria, de outra forma, impossível ou muito difícil. O que significa que se circunscreveu decisivamente essa transmissão *ao processo penal* e apenas para investigação, deteção e investigação de *certos crimes*, regulando-se ainda as condições de segurança dessa transmissão e a destruição dos dados comunicados às autoridades públicas. Neste quadro, o legislador nacional combinou uma obrigação *generalizada* de os operadores de telecomunicações conservarem *todos* os dados de base, tráfego e localização (sem delimitar as categorias de dados ou os sujeitos afetados) com um regime vinculado quanto ao respetivo *acesso* pelas autoridades de investigação criminal.

**7.** Não restam dúvidas que as normas fiscalizadas se colocam no domínio de aplicação do Direito da União Europeia e, por isso, estão abrangidas pela Carta dos Direitos Fundamentais da União Europeia (CDFUE). Vejamos.

A Carta dos Direitos Fundamentais da União Europeia (CDFUE) constitui um catálogo de direitos fundamentais que vincula, acima de tudo, a própria União Europeia (n.º 1 do artigo 6.º do Tratado da União Europeia [TUE]; n.º 1 do artigo 51.º da CDFUE). Garante, assim, que a convenção do exercício em comum, em cooperação ou pelas instituições da União, de poderes estaduais não implica uma redução da tutela dos cidadãos, porquanto a União Europeia está, ela própria, vinculada por um catálogo de direitos fundamentais redigido à imagem dos textos constitucionais nacionais.

Simplesmente, em virtude do princípio da administração indireta, não é — em regra — a União Europeia a executar e a aplicar os seus próprios atos, cabendo tal missão às autoridades nacionais (cfr. artigo 291.º do Tratado sobre o Funcionamento da União Europeia [TFUE]). Por essa razão, a CDFUE vincula também os Estados-Membros *quando estes apliquem direito da União Europeia* (artigo 51.º CDFUE). Nessas circunstâncias — isto é, quando autoridades nacionais legiferam em aplicação direito da União Europeia —, ficam os Estados-Membros vinculados ao parâmetro europeu de proteção dos direitos fundamentais.

A jurisprudência do Tribunal de Justiça da União Europeia (TJUE) permite identificar três situações que correspondem ao pressuposto de aplicação da Carta aos Estados-Membros «*quando apliquem o direito da União*» (artigo 51.º CDFUE): a atuação dos Estados como agentes da União, efetivando as suas normas — designadamente, transpondo diretivas (i); a ação dos Estados em domínios em que as regras comunitárias conferem às autoridades nacionais margem de apreciação, *v. g.* admitindo derrogações às normas de fonte europeia (ii); atividade legiferante nacional em domínios que são já objeto de regulação comunitária (iii).

Nessa medida, as normas cuja declaração de inconstitucionalidade é pedida estão indiscutivelmente no âmbito de aplicação do direito da União Europeia e, assim, da CDFUE.

Desde logo, tais regras foram emanadas em transposição da Diretiva n.º 2006/24/CE, do Parlamento Europeu 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, ato jurídico que procurava uniformizar as medidas nacionais de conservação de dados sobre as comunicações e sua transmissão às autoridades com competências criminais — adotadas no uso da faculdade conferida pelo artigo 15.º da Diretiva 2002/58/CE.

Em segundo lugar, a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho de 2002, que disciplina o direito à privacidade no setor das telecomunicações, regula as condições em que podem os Estados-Membros adotar medidas de intrusão nos dados cuja confidencialidade é prescrita: quando «*constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas*» (artigo 15.º da Diretiva 2002/58/CE). Deste modo, concluiu o Tribunal de Justiça que as medidas nacionais de *conservação* de metadados relativos a comunicações eletrónicas se encontram sob o âmbito de aplicação do direito da União Europeia (Acórdão de 21 de dezembro de 2016, *Tele 2*, proc. C-203/15 e C-698/15, n.º 78), bem como as medidas de *transmissão* desses dados às autoridades públicas, para fins de investigação e repressão da criminalidade (Acórdão de 6 de outubro de 2020, *La quadrature du net*, procs. C-511/18, C-512/18 e C-520/18, n.º 58).

No fundo, tendo o TJUE declarado a invalidade da Diretiva n.º 2006/24/CE (Acórdão de 8 de abril de 2014, *Digital Rights Ireland*, proc. C-293/12 e C-594/12) — que harmonizava as medidas de conservação de dados relativos a comunicações e sua transmissão às autoridades com competência criminal —, nem por isso se excluíram tais medidas do âmbito de aplicação do direito europeu. Simplesmente, não mais os Estados-Membros se encontram *obrigados* a adotar as providências que aquela impunha; embora as medidas nacionais que permitam ou visem uma intromissão nas comunicações eletrónicas fiquem sujeitas às obrigações decorrentes do disposto no artigo 15.º da Diretiva 2002/58/CE, só sendo conformes ao direito europeu quando «*constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas"*» (artigo 15.º da Diretiva 2002/58/CE). Tais normas traduzem «*justamente uma concretização da exceção facultativa ao regime-regra da privacidade em matéria de comunicações eletrónicas admitida no artigo 15.º, n.º 1, da Diretiva n.º 2002/58*», razão pela qual «*nenhuma dúvida existe de que também as medidas nacionais que concedam o acesso aos dados previamente conservados se enquadram no âmbito de aplicação daquele preceito*» (Acórdão do Tribunal Constitucional n.º 464/2019).

Neste quadro, as medidas adotadas pelos Estados-Membros que estabeleçam tais intromissões — sejam elas adotadas em transposição da Diretiva 2006/24/CE, entretanto declarada inválida; ou, ao invés, ao abrigo das exceções à inviolabilidade das comunicações eletrónicas permitidas pelo artigo 15.º da Diretiva 2002/58/CE — situam-se no âmbito de aplicação do direito europeu. O que implica a conclusão de que o Estado está vinculado à norma do artigo 15.º da Diretiva 2002/58/CE e, igualmente, à CDFUE (cfr. n.º 1 do artigo 51.º da CDFUE).

**8.** Encontrando-se as normas fiscalizadas no âmbito de aplicação do direito da União Europeia, importa determinar a relevância desta ordem jurídica para o pedido de declaração de inconstitucionalidade dirigido a este Tribunal. Desde logo, importa saber de que modo é que a eventual incompatibilidade das normas fiscalizadas com a CDFUE ou com o artigo 15.º da Diretiva 2002/58/CE influi na apreciação da sua conformidade constitucional.

A Constituição determina expressamente que a aplicação do direito da União Europeia na ordem jurídica interna é feita «*nos termos definidos pelo Direito da União*» (cfr. n.º 4 do artigo 8.º da Constituição). Em consequência, sob ressalva da parte final daquela disposição, é o direito da União Europeia que determina o seu modo de relacionamento com a ordem jurídica nacional — incluindo o direito constitucional.

**8.1.** Neste quadro, pode perguntar-se se a eventual inconciliabilidade das normas fiscalizadas com regras europeias vinculativas (em concreto, os direitos consagrados nos artigos 7.º e 8.º da CDFUE; e as obrigações impostas ao Estado por força do artigo 15.º da Diretiva 2002/58/CE) gera, *nos termos definidos pelo Direito da União*, a invalidade das normas em crise. Cabendo a este Tribunal declarar a sua invalidade com fundamento na transgressão de regras e princípios de direito da União Europeia.

Assim não é. Conservando o direito da União Europeia *autonomia* face à ordem jurídica interna, a ordem jurídica nacional não é afetada, ao nível da validade, pelas normas europeias; nem a ordem jurídica europeia é, em princípio, afetada ao nível da sua validade — mesmo quando as suas normas são aplicadas ao nível interno — por contradizer as Constituições nacionais. O princípio da autonomia do direito da União Europeia concretiza-se na existência, ao nível europeu, de mecanismos próprios de interpretação, controlo e aplicação, repercutidos no sistema jurisdicional de apreciação da validade das suas normas.

Aliás, foi este princípio da autonomia do direito da União Europeia que o Tribunal Constitucional expressamente afirmou no Acórdão n.º 422/2020, ao determinar que não lhe cabe (sob ressalva da parte final do n.º 4 do artigo 8.º) aferir da conformidade constitucional de normas organicamente europeias. Como aí se concluiu, «*Uma outra perspetiva menos exigente banalizaria a intervenção do Tribunal Constitucional, num quadro onde a mesma foi constitucionalmente configurada muito restritivamente, e – consequência não menos constitucionalmente indesejada –, em aberto desafio à aceitação da projeção do DUE na ordem interna nos termos pelo próprio definidos, criaria um mecanismo interno, de fácil ativação, onde a constante discussão deste, à margem e em aberto desafio aos seus próprios termos, originaria um sistema nacional espúrio, sem qualquer respaldo no quadro constitucional de interação entre as ordens jurídicas nacional e europeia*». Por força do princípio da autonomia, só o Tribunal de Justiça é competente para apreciar a invalidade do direito europeu, por referência aos seus próprios parâmetros (cfr. Acórdão do TJUE de 22 de outubro de 1987, *Foto-Frost*, proc. 314/85, n.º 15). Simetricamente, o direito interno, ainda que adotado em cumprimento de normas europeias, vê a sua validade apreciada *apenas* pelos tribunais nacionais, não tendo o Tribunal de Justiça poderes de cognição sobre atos de direito nacional (cfr. artigo 263.º do TFUE). Assim, porque as normas fiscalizadas são organicamente *nacionais* — adotadas pela Assembleia da República — dúvidas não restam de que há plena jurisdição do Tribunal Constitucional para as apreciar.

Ora, uma das vertentes do princípio da autonomia é justamente a circunstância de, nas relações entre o direito europeu e o direito nacional, se ter renunciado «*ao paradigma da pirâmide*», pelo que o conflito normativo não provoca a nulidade ou revogação das normas nacionais, antes «*apontando para o paradigma da rede, onde nenhum ponto é privilegiado em relação a outro, e nenhum está inequivocamente subordinado a outro*» (NUNO PIÇARRA, "A justiça constitucional da União Europeia", *Estudos jurídicos e económicos em homenagem ao Prof. Doutor António de Sousa Franco*, vol. III, 2006, p. 479). Deste modo, a antinomia entre normas nacionais e europeias simultaneamente aplicáveis a dado caso concreto é solucionada ao nível da *eficácia*: são desaplicadas no caso concreto as regras nacionais que contradigam normas europeias simultaneamente mobilizáveis, sem que aquelas percam a sua validade. É este o sentido do princípio do primado ou da prevalência na aplicação do direito da União Europeia, que configura, assim, uma «*uma regra de colisão reconduzível à aplicação preferente do direito europeu (pre-emption, Vorrangsanwendung) e não como uma estrita regra de supremacia normativa eventualmente conducente à invalidade do direito interno*» (GOMES CANOTILHO e VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, vol. I, 4.ª Edição, 2007, p. 266).

É por isso que, na terminologia do Tribunal Constitucional Espanhol, o direito da União Europeia goza de *primazia* mas não de *supremacia*: trata-se de preferência aplicativa e não de qualquer causa de invalidade ou inexistência de direito nacional (cfr. Tribunal Constitucional Espanhol na Declaração nº 1/2004, de 13 de Dezembro de 2004):

*"La proclamación de la primacía del Derecho de la Unión por el art. I-6 del Tratado no contradice la supremacía de la Constitución. Primacía y supremacía son categorías que se desenvuelven en órdenes diferenciados. Aquélla, en el de la aplicación de normas válidas; ésta, en el de los procedimientos de normación. La supremacía se sustenta en el carácter jerárquico superior de una norma y, por ello, es fuente de validez de las que le están infraordenadas, con la consecuencia, pues, de la invalidez de éstas si contravienen lo dispuesto imperativamente en aquélla. La primacía, en cambio, no se sustenta necesariamente en la jerarquía, sino en la distinción entre ámbitos de aplicación de diferentes normas, en principio válidas, de las cuales, sin embargo, una o unas de ellas tienen capacidad de desplazar a otras en virtud de su aplicación preferente o prevalente debida a diferentes razones. Toda supremacía implica, en principio, primacía (de ahí su utilización en ocasiones equivalente, así en nuestra Declaración 1/1992, FJ 1), salvo que la misma norma suprema haya previsto, en algún ámbito, su propio desplazamiento o inaplicación. La supremacía de la Constitución es, pues, compatible con regímenes de aplicación que otorguen preferencia aplicativa a normas de otro Ordenamiento diferente del nacional siempre que la propia Constitución lo haya así dispuesto, que es lo que ocurre exactamente con la previsión contenida en su art. 93, mediante el cual es posible la cesión de competencias derivadas de la Constitución a favor de una institución internacional así habilitada constitucionalmente para la disposición normativa de materias hasta entonces reservadas a los poderes internos constituidos y para su aplicación a éstos".*

Neste quadro, se «*nos termos definidos pelo direito da União Europeia*» (n.º 4 do artigo 8.º da Constituição) a antinomia entre normas nacionais e europeias não provoca a invalidade das primeiras (determinando-se, ao invés, a sua *desaplicação* ao caso), o direito da União Europeia terá

necessariamente um efeito distinto para o Tribunal Constitucional, a quem compete atestar a conformidade de normas com a Constituição.

Os tribunais ordinários, perante normas nacionais e europeias simultaneamente mobilizáveis que se revelem incompatíveis, fazem atuar o princípio do primado do direito da União Europeia, desaplicando a norma nacional no caso concreto (salvo se tal puser em causa os princípios fundamentais do Estado de Direito Democrático, nos termos do n.º 4 do artigo 8.º da Constituição). É neste sentido que se diz que o destinatário do princípio do primado é o juiz nacional, porquanto é a ele que cabe a desaplicação da norma nacional em favor da regra europeia. Sendo certo que a *desaplicação da norma nacional* como efeito do princípio do primado é proclamada pelo Tribunal de Justiça desde os arestos que desvelaram aquele cânone (cfr. Acórdão de 15.07.1964, *Costa c. ENEL*, proc. 6/64; Acórdão do TJ de 9.3.1978, *Simmenthal*, proc. 106/77, n.º 17) e se mantém em jurisprudência constante (Acórdão de 5.10.2010, *Elchinov*, proc. C-173/09, n.º 31: «*o juiz nacional encarregado de aplicar, no âmbito da sua competência, as disposições do direito da União tem a obrigação de garantir a plena eficácia dessas disposições, não aplicando, se necessário e pela sua própria autoridade, qualquer disposição contrária da legislação nacional*»; Acórdão de 19.11.2009, *Krzysztof Filipiak*, proc. C-314-08, n.º 83 – «*o Tribunal de Justiça já declarou que a incompatibilidade com o direito comunitário de uma norma de direito nacional posterior não acarreta a inexistência dessa norma. Face a tal situação, o órgão jurisdicional nacional é obrigado a não aplicar essa norma*», gerando um «*efeito de exclusão exercido por uma norma de direito da União diretamente aplicável em face do direito nacional a ela contrário*» — Acórdão de 8.09.2010, *Winner Wetten GmbH*, proc. C-409/06, n.º 67).

No fundo, tendo o direito europeu chamado a si o problema do seu relacionamento com as ordens jurídicas nacionais — o que a Constituição recebe no n.º 4 do artigo 8.º — o princípio do primado do direito da União Europeia atua no domínio *por si próprio delimitado*: a incompatibilidade de normas europeias e nacionais simultaneamente mobilizáveis ao caso concreto. Pelo que a competência para desaplicar, nos casos concertos, normas nacionais contrárias a regras europeias pertence aos tribunais ordinários, estabelecendo-se uma relação direta entre aqueles e o Tribunal de Justiça em sede de reenvio prejudicial.

Em consequência, a eventual contrariedade das normas ora em crise com regras de direito da União Europeia que possam ser invocáveis no plano interno terá como resposta do sistema judicial nacional a desaplicação das normas internas — sem que estas sejam expurgadas do ordenamento jurídico ou que se gere, por esse efeito, a sua invalidade. Foi justamente o que decidiu a Comissão Nacional de Proteção de Dados (CNPD): considerando, na sua deliberação n.º 641/2017, de 9 de maio de 2017, que o regime contido na Lei n.º 32/2008 contraria o Direito da União Europeia — por transgressão desproporcionada dos artigos 7.º e 8.º da CDFUE —, deliberou desaplicar a Lei n.º 32/2008, com fundamento no primado do direito da União Europeia (Deliberação n.º 1008/2017, de 18 de julho de 2017).

Não é esse o problema que se põe ao Tribunal Constitucional nos presentes autos. O Tribunal Constitucional é chamado a apreciar a *validade* de normas jurídicas nacionais e não a resolver um problema aplicativo ao caso concreto de normas conflituantes de ordens jurídicas autónomas; nem é chamado, como sucedeu no caso que deu origem ao Acórdão n.º 422/2020, a pronunciar-se sobre a conformidade constitucional de normas *organicamente europeias.* Nessa medida, o papel do direito da União Europeia nos presentes autos será necessariamente *outro*, sendo certo que é à ordem

jurídica comunitária que cabe definir a sua missão, nos termos reconhecidos pelo n.º 4 do artigo 8.º da Constituição.

É por estas razões que o Tribunal Constitucional desde cedo excluiu a possibilidade de incluir as normas de direito europeu nos parâmetros de inconstitucionalidade. Esclareceu-se não só que «*é de rejeitar a "qualificação da incompatibilidade do direito interno com o direito comunitário como uma situação de 'inconstitucionalidade' que ao Tribunal Constitucional caiba apreciar"*» (Acórdão n.ºs 621/98) como que «*a ordem jurídica comunitária, globalmente recebida pelo direito português, por via de uma cláusula do próprio texto constitucional – nº 2 do artigo 8.º – compreende uma instância jurisdicional precipuamente vocacionada para a tutela de direito comunitário, que não funciona apenas no plano das relações interestaduais ou intergovernamentais, concentrando nessa instância a competência para velar pela aplicação uniforme e pela prevalência das respectivas normas, o que tornaria incongruente que, para o mesmo efeito, se fizesse intervir, no plano interno, uma outra instância do mesmo ou semelhante tipo, como seria o Tribunal Constitucional*» (Acórdão n.º 93/2001).

Percebe-se que assim seja. Tal solução é a única que assegura a uniformidade de aplicação da ordem jurídica europeia e que conduz à harmonização da competência do Tribunal Constitucional com a do Tribunal de Justiça, salvaguardando a autonomia do direito da União Europeia e a primazia na aplicação ao caso concreto (com eventual intervenção do TJUE em sede de reenvio prejudicial) sem que se impute a tal circunstância uma transgressão da Constituição. Na verdade, não só a própria natureza do princípio do primado se dirige a dirimir conflitos aplicativos ao nível da *eficácia* — como o Tribunal de Justiça repetidamente tem afirmado — como a recondução de uma contrariedade a normas europeias a uma questão de constitucionalidade poria em causa a uniformidade de aplicação do direito europeu, já que a desaplicação das normas nacionais contrárias a regras europeias ficaria dependente do sistema de controlo de constitucionalidade vigente nesse Estado-Membro.

Deste modo, a incompatibilidade de certa norma nacional com o direito da União Europeia não implica, de forma automática, um juízo de inconstitucionalidade; provoca, ao invés, uma afetação da sua eficácia no plano interno, na medida em que contradiga regras europeias simultaneamente mobilizáveis. E, nos *termos como o direito da União Europeia o define*, este efeito dá-se independentemente da fonte das normas conflituantes: *quer* a norma europeia conste de direito originário (como a CDFUE, nos termos do artigo 6.º do TUE) ou derivado (como uma diretiva ou um Regulamento); *quer* a norma nacional conste de ato regulamentar, de ato legislativo ou mesmo da Constituição.

Pelo que a demonstração da contradição das normas em crise com o direito da União Europeia não permite inferir uma conclusão pela respetiva inconstitucionalidade. O juízo de inconstitucionalidade — e, assim, da *invalidade* da norma nacional — depende da desconformidade das normas fiscalizadas com o seu parâmetro hierarquicamente superior — *maxime*, a Constituição.

**8.2.** Importa, pois, dilucidar a relevância do direito europeu para o pedido formulado — cabendo ao próprio direito da União Europeia estabelecê-lo, como determina o n.º 4 do artigo 8.º da Constituição. Ora, o direito da União Europeia, em decorrência do princípio da cooperação leal (cfr. n.º 3 do artigo 4.º do TUE), consagra uma imposição aos Estados-Membros de garantir o efeito

útil das normas europeias; e é de entre as suas várias refrações que se encontra o *princípio da interpretação conforme ao Direito da União Europeia.*

O *princípio da interpretação conforme* — nascido na década de 70 do século XX a propósito da obrigação de os tribunais nacionais alcançarem, através da interpretação do direito nacional, o efeito útil de diretivas insuscetíveis de produzir efeito direto (cfr., entre muitos outros, Acórdãos do TJUE *Mazzalai*, de 20.05.1976, proc. 111/75, e *Von Colson*, de 10.04.1984, proc. 14/83; *Marleasing*, de 13.11.1990, proc. 106/89) — foi sendo reconduzido a um cânone geral de interpretação do direito nacional (de *todo* o direito nacional) de modo a atingir a plena eficácia do direito da União Europeia. Determina tal princípio que os tribunais nacionais, ao aplicar o direito interno, são obrigados a interpretá-lo, na medida do possível, à luz do direito europeu: «*Esta obrigação de interpretação conforme do direito nacional é inerente ao sistema do Tratado FUE, na medida em que permite aos órgãos jurisdicionais nacionais assegurar, no âmbito das suas competências, a plena eficácia do direito da União quando decidem dos litígios que lhes são submetidos*» (Acórdão do TJUE de 24.01.2012, *Maribel Dominguez*, proc. C-282/10).

Assim, os tribunais dos Estados-Membros, na fixação do sentido das normas de direito nacional, estão vinculados ao *efeito útil* do direito europeu e devem, dentro da margem permitida pelas regras interpretativas internas, escolher a exegese que melhor se acomode às normas europeias. No fundo, no seio da obrigação de as autoridades nacionais tomarem as medidas que garantam a efetividade do direito da União, «*uma dessas medidas consiste precisamente na obrigação de os tribunais, e as restantes autoridades nacionais, interpretarem a lei nacional em conformidade com o direito da União*» (cfr. SOFIA OLIVEIRA PAIS, "Princípio da interpretação conforme", *Princípios Fundamentais de Direito da União Europeia*, 3.ª Edição, Almedina, 2016, p. 96). Trata-se, pois, de uma garantia de eficácia do direito europeu plenamente recebida pelo disposto no n.º 4 do artigo 8.º da Constituição.

Ora, pedindo-se ao Tribunal Constitucional a fiscalização de normas *organicamente nacionais* por referência ao seu parâmetro hierárquico de validade, é na interpretação *da Constituição* que intervém o Direito da União Europeia (incluindo a Carta dos Direitos Fundamentais da União Europeia [CDFUE]). Vejamos.

No quadro da proteção dos direitos fundamentais, verifica-se uma congruência tendencial entre a ordem jurídica europeia e a ordem jurídica nacional. O que se compreende, atendendo à *rede de proteção constitucional* gerada pela comunicação constante entre as ordens jurídicas nacional e europeia. O ordenamento jus-europeu alimenta-se dos catálogos nacionais, uma vez que o Tratado recebe, «*enquanto princípios gerais, os direitos fundamentais tal como os garante a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais e tal como resultam das tradições constitucionais comuns aos Estados-Membros*» (n.º 3 do artigo 6.º do TUE) e a União Europeia está vinculada, ela própria, à CDFUE, que contém um catálogo de direitos fundamentais redigido à imagem das constituições nacionais. É esta, segundo FREITAS DO AMARAL e NUNO PIÇARRA, a «*contrapartida do princípio do primado: a garantia de congruência material entre a ordem jurídica da União Europeia as ordens jurídicas nacionais quanto aos princípios constitucionais fundamentais*» ("O Tratado de Lisboa e o princípio do primado do direito da União Europeia: uma «evolução na continuidade»", *Revista de Direito Público*, n.º 1, 2009). O que decorre, de forma muito clara, da absorção para o acervo comunitário das «*tradições constitucionais comuns aos Estados*

*membros*» em matéria de direitos fundamentais enquanto padrão de interpretação da própria Carta (n.º 4 do artigo 52.º CDFUE).

Simplesmente, a articulação *multinível* não ocorre apenas nesta direção. Na verdade, *nos termos definidos pelo direito da União Europeia*, a interpretação do direito nacional (em qualquer das suas fontes) tem em conta o direito europeu: «*Cabe ao tribunal nacional dar à lei interna, em toda a medida em que uma margem de apreciação lhe seja concedida pelo respectivo direito interno, uma interpretação e uma aplicação em conformidade com as exigências do direito comunitário*» (Acórdão do TJUE de 4 de Fevereiro de 1988, *Murphy*, proc. 157/86). É o que sucede no domínio de direitos fundamentais que estejam simultaneamente previstos na Constituição e na CDFUE, sobretudo quando nesta última se preveja um nível de proteção mais elevado (cfr. artigo 53.º da CDFUE). Operando-se uma *ponderação* das fontes internacionais de direitos fundamentais no momento da aplicação das normas e princípios constitucionais internos.

Daqui decorre que, quando o Estado atua no domínio de aplicação do direito da União Europeia (n.º 1 do artigo 51.º da CDFUE), o sentido a dar aos direitos fundamentais que parametrizam a validade das normas internas deve privilegiar uma consonância com as normas europeias a que o Estado se encontra vinculado, estabelecendo-se uma relação interativa, mais do que hierárquica. E, caso ocorram conflitos entre os parâmetros, a solução será procurada *"by seeking to interpret the Constitution according to Community law"* (RUI MOURA RAMOS, "The adaptation of the Portuguese Constitutional Order to Community Law", *Boletim da Faculdade de Direito*, vol. 76, 2000, p. 8).

Bem se compreende que assim seja. No quadro da rede comunicante de proteção dos direitos fundamentais, a uniformidade de aplicação do direito da União pelos Estados-Membros estaria em causa se os parâmetros fossem díspares, fixando um nível de proteção inferior àquele que é garantido pela CDFUE (Acórdãos do TJUE de 26 de fevereiro de 2013, *Melloni*, C-399/11, n.º 60 e *Åkerberg Fransson*, C-617/10, n.º 29). Por esta razão, «*A congruência constitucional implica que, no respeito pelos princípios hermenêuticos pertinentes, se procure sempre obter uma interpretação das normas nacionais que seja conforme com o direito da UE*» (MIGUEL GORJÃO-HENRIQUES, "Compreensões e pré-compreensões sobre o primado na aplicação do direito da União: breves notas jurídico-constitucionais relativamente ao Tratado de Lisboa", *Estudos em Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho*, vol. III, 2012, p. 369).

A atuação do princípio de interpretação conforme alastra às condições de *restrição* dos direitos fundamentais: o juízo de proporcionalidade na limitação dos direitos fundamentais assegurados pela CDFUE não se desliga daquele que é operado pelo Tribunal de Justiça. No fundo, ainda que o parâmetro de validade das normas de direito interno seja encontrado na Constituição, a reflexão constitucional deixa de ter como horizonte exclusivo de referência o quadro nacional, pelo que a multiplicidade de fontes de proteção dos direitos fundamentais — associada à diversidade de instâncias jurisdicionais de tutela, inseridas em ordenamentos jurídicos distintos e entre os quais não existe uma relação de hierarquia — implica uma concordância prática entre os parâmetros convocados. Que é assegurada, justamente, pelo cânone da *interpretação conforme*. Aliás, a articulação do texto constitucional com os parâmetros europeus é exercida pelo próprio legislador constituinte, que vai moldando o conteúdo dos preceitos da Lei Fundamental aos padrões de

proteção comunitários — o que é especialmente claro nas sucessivas revisões do artigo 35.º da Constituição, relativo à utilização da informática.

Por estas razões, situando-se as normas fiscalizadas no domínio de aplicação do direito da União Europeia, a interpretação dos parâmetros constitucionais a que as regras em crise se submetem tem em conta o sentido das normas europeias, procurando-se estabelecer a interpretação mais próxima do direito europeu. É, aliás, o que a requerente sustenta nos artigos 42.º a 45.º do pedido, solicitando ao Tribunal Constitucional que interprete os parâmetros da Constituição portuguesa à luz da Carta. E foi justamente o que o Tribunal Constitucional concluiu no Acórdão n.º 464/2019: «*por força das normas do artigo 8.º da Constituição que estabelecem a relevância do Direito Internacional e do Direito da União na ordem jurídica interna e, também, da cláusula aberta no domínio dos direitos fundamentais consagrada no artigo 16.º da Constituição, este Tribunal não pode deixar de considerar os direitos fundamentais consagrados na CDFUE e na referida Convenção, devendo igualmente ter em conta, numa perspetiva de diálogo interjurisdicional, a interpretação que dos mesmos tem vindo a ser feita pelas instâncias competentes para a sua aplicação, nomeadamente o Tribunal de Justiça da União Europeia ("TJUE") e o Tribunal Europeu dos Direitos Humanos ("TEDH")*».

**9.** Definidos os termos de influência do direito da União Europeia para o presente pedido, importa agora determinar o conteúdo das normas comunitárias nesta matéria. Sendo certo que a fixação do respetivo sentido (incluindo as disposições da CDFUE, enquanto integrante do direito da União Europeia nos termos do artigo 6.º do TUE), cabe ao Tribunal de Justiça da União Europeia (artigo 267.º do TFUE), pelo que a respetiva jurisprudência é o ponto axial da densificação dos seus conceitos.

No que respeita à CDFUE, assumem relevância, desde logo, as normas contidas nos artigos 7.º e 8.º da Carta, relativos, respetivamente, ao respeito da vida privada e familiar e à proteção de dados pessoais:

Artigo 7.º

**Respeito pela vida privada e familiar**

Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.

Artigo 8.º

**Proteção de dados pessoais**

1. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente

De acordo com o Tribunal de Justiça, as medidas de conservação de dados de tráfego e de localização pelos fornecedores de serviços de comunicações eletrónicas são abrangidas por ambas

as disposições, na medida em que possam ser ligados à identificação de uma pessoa. Não só porque os direitos estão indissociavelmente ligados (Acórdão de 9 de novembro de 2010, *Volker*, procs. C-92/09 e C-93/09, n.º 47), como também porque a «*conservação dos dados está abrangida pelo âmbito de aplicação do artigo 8.º desta, uma vez que constitui um tratamento de dados pessoais na aceção deste artigo e deve, assim, necessariamente, respeitar as exigências de proteção de dados resultantes deste artigo*» — Acórdão *Digital Rights Ireland, cit.*, n.º 29.

Com efeito, o artigo 7.º da CDFUE, relativo ao respeito pela vida privada e familiar, ao domicílio e às comunicações, é decalcado no disposto no artigo 8.º da CEDH, devendo ser interpretado com o mesmo sentido e alcance (n.º 3 do artigo 52.º da CDFUE). O que implica que o regime das suas restrições seja idêntico, como concluiu o Tribunal de Justiça no Acórdão de 15 de novembro de 2011, *Dereci*, proc. C-256/11, n.º 70: «*o artigo 7.° da Carta dos Direitos Fundamentais da União Europeia (a seguir «Carta»), relativo ao direito ao respeito da vida privada e familiar, consagra direitos correspondentes aos que são garantidos pelo artigo 8.°, n.º 1, da CEDH e que se deve, portanto, dar ao artigo 7.° da Carta o mesmo sentido e o mesmo alcance que o sentido e o alcance dados ao artigo 8.°, n.º 1, da CEDH, conforme interpretado pela jurisprudência do Tribunal Europeu dos Direitos do Homem*». Neste quadro, mobilizou-se, para densificação do artigo 7.º da CDFUE, o regime do n.º 2 do artigo 8.º da CEDH: «*Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros*». Simplesmente, diferentemente do que sucede na CEDH, a Carta autonomizou o direito à proteção de dados pessoais (no artigo 8.º da CDFUE), sem deixar de reconhecer uma relação indissociável entre ambos (Acórdão *Volker, cit.*, n.º 47).

Com estes parâmetros, o sentido dos direitos fundamentais consagrados na Carta foi densificado pelo Juiz comunitário, quer a propósito da confrontação dos atos adotados pela União Europeia com aqueles parâmetros quer, por outro lado, pela análise da sua conciliabilidade com os regimes nacionais adotados *em aplicação do direito da União Europeia.* E no seu âmbito de proteção abrangeram-se não apenas os dados de identificação de uma pessoa como aqueles que permitam chegar a essa identificação (como número de telefone, os endereços de correio eletrónico e de IP do computador).

**9.1.** Desde logo, tendo o legislador comunitário disciplinado diretamente a matéria da conservação de dados no quadro das comunicações eletrónicas, o TJUE teve oportunidade de se pronunciar sobre a validade daqueles atos europeus, por confrontação direta com a CDFUE.

A Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas, positiva um *direito à confidencialidade*, um *direito à anonimização ou eliminação dos dados de tráfego* e a *proteção dos dados de localização* (artigos 5.º, 6.º e 9.º). Todavia, aí se previu a viabilidade e as condições de admissibilidade de os Estados-Membros derrogarem aquele nível de proteção: «*Os Estados-Membros podem adotar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos nos artigos 5.º e 6.º, nos n.os 1 a 4 do artigo 8.º e no artigo 9.º da presente diretiva sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para*

*salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas, tal como referido no n.º 1 do artigo 13.º da Diretiva 95/46/CE. Para o efeito, os Estados-Membros podem designadamente adotar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões enunciadas no presente número*» (artigo 15.º). Ora, em 2006 — invocando a disparidade das medidas derrogatórias aprovadas pelos Estados-Membros no uso da faculdade prevista pelo artigo 15.º da Diretiva n.º 2002/58/CE — foi aprovada a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março de 2006 (cfr. Considerando n.º 6).

A abordagem do legislador europeu de 2006 aparta-se da que havia sido seguida na Diretiva 2002/58/CE: em vez de *permitir* aos Estados-Membros restringir os direitos inerentes à privacidade das comunicações eletrónicas, *impôs aos Estados a obrigação de operar tal restrição* (artigo 3.º da Diretiva n.º 2006/24/CE), estabelecendo o dever de conservação de certas categorias de dados (excluindo o conteúdo das comunicações [artigo 5.º], por «*períodos não inferiores a seis meses e não superiores a dois anos, no máximo, a contar da data da comunicação*» [artigo 6.º]) e determinando que o acesso aos dados pelas autoridades nacionais competentes só deveria ocorrer para efeitos de investigação, deteção e repressão de crimes graves (n.º 1 do artigo 1.º), «*de acordo com os requisitos da necessidade e da proporcionalidade devem ser definidos por cada Estado-Membro no respetivo direito nacional, sob reserva das disposições pertinentes do Direito da União Europeia ou do Direito Internacional Público, nomeadamente a CEDH na interpretação que lhe é dada pelo Tribunal Europeu dos Direitos do Homem*» (artigo 4.º). Em conformidade, aditou-se um novo número (1-A) ao artigo 15.º da Diretiva n.º 2002/58/CE, nos termos do qual os dados cuja conservação fosse expressamente determinada pela Diretiva n.º 2006/24/CE ficariam subtraídos ao disposto no n.º 1 do artigo 15.º da Diretiva n.º 2002/58/CE.

Ora, chamado a pronunciar-se prejudicialmente, o TJUE concluiu pela invalidade das normas da diretiva de 2006, por implicarem uma restrição desproporcionada aos direitos ao respeito pela vida privada e familiar e à proteção de dados pessoais, consagrados, respetivamente, nos artigos 7.º e 8.º da CDFUE e por estabelecerem de forma indeterminada o leque de crimes cuja investigação ou repressão pode admitir o acesso aos dados conservados (Acórdão *Digital Rights Ireland, cit.*, n.ºs 26 a 29; e 41 a 43). Sendo o direito derivado da União Europeia parametrizado pelo respetivo direito primário — e que a CDFUE assume justamente esse valor (cfr. n.º 1 do artigo 6.º do TUE) —, concluiu o Juiz europeu não estarem preenchidos os pressupostos da sua restrição (n.º 1 do artigo 52.º da CDFUE).

O TJUE considerou violado o princípio da proporcionalidade. *Por um lado,* face ao excessivo âmbito de aplicação da medida de conservação dos dados, quer quanto ao universo *objetivo* (ao englobar todos os meios de comunicação eletrónica), quer *subjetivo* (ao abranger todas as pessoas, todos os meios de comunicação eletrónica e todos os dados de tráfego sem criar qualquer diferenciação, limitação ou exceção em função do objetivo ou do risco e sem exigir qualquer relação entre a conservação dos dados e uma ameaça para a segurança pública) — n.ºs 56 ss do Acórdão *Digital Rights*. *Por outro lado,* pela inexistência de critérios ou requisitos de acesso das autoridades nacionais aos dados conservados — designadamente, controlo jurisdicional prévio —, limitando-se a remeter para as infrações graves tal como definidas no direito nacional de cada

Estado-Membro (n.º 60). *Em terceiro lugar*, pelo facto de a duração de conservação de dados se situar «*entre um mínimo de seis meses e um máximo de vinte e quatro meses, sem que se especifique que a determinação do período de conservação se deve basear em critérios objetivos a fim de garantir que se limita ao estritamente necessário*» (n.º 64). *Por fim*, por não se estabelecerem garantias de proteção eficaz contra os riscos de abuso e contra qualquer acesso e sua utilização ilícita ou sequer que os dados fiquem conservados no território da União, de modo a assegurar que a fiscalização da segurança do armazenamento e transmissão dos dados se faça *com base no direito da União* (n.ºs 66 a 68).
O Acórdão *Digital Rights Ireland* permite, assim, delimitar o parâmetro comunitário de admissibilidade das medidas de conservação dos dados de tráfego e de localização: à luz da Carta, é possível a sua estatuição (sendo adequadas à proteção de um interesse geral relevante), embora a regulamentação deva restringir a sua aplicação ao indispensável para aquele objetivo, mediante definição seletiva do universo de dados e de titulares afetados (i), o estabelecimento de garantias no acesso das autoridades a essas informações (ii), a estatuição de critérios objetivos de duração da conservação por atenção aos objetivos visados (iii) e a criação de mecanismos de segurança de proteção eficaz desses dados contra abusos, utilização e acesso ilícitos (iv) (Acórdão *Digital Rights Ireland, cit.*, n.ºs 51 e 56 a 59).

**9.2.** A declaração de invalidade da Diretiva n.º 2006/24/CE pelo Tribunal de Justiça — enquanto órgão jurisdicional competente para a apreciação da validade do direito derivado da União Europeia (cfr. Acórdão *Foto-Frost, cit.*; e, igualmente, Acórdão do Tribunal Constitucional n.º 422/2020) não implica, como efeito automático, a invalidade da Lei n.º 32/2008, de 17 de julho. Como se explicou no Acórdão n.º 420/2017, «*A declaração de invalidade de uma diretiva não tem uma consequência automática sobre a validade de um ato legislativo português que a transponha. O ato legislativo nacional, embora tendo como objetivo o cumprimento do dever de transposição de uma diretiva, decorrente do Direito da UE (artigo 4.º, n.º 3, do Tratado da UE, artigo 288.º, 3.º parágrafo, do Tratado sobre o Funcionamento da UE e artigo 112.º, n.º 8, da Constituição), tem uma fonte autónoma de validade e legitimidade. O Tribunal de Justiça não tem jurisdição para apreciar a validade dos atos de direito nacional dos Estados-Membros, sendo que a sua análise apenas incidiu sobre o texto da diretiva. A validade da Lei n.º 32/2008, de 17 de julho, não pode ser posta em causa apenas devido ao facto de este ato normativo da União ter sido declarado inválido*».
Estas considerações não implicam que seja irrelevante, para os presentes autos, o conteúdo do direito da União Europeia e a sua eventual incompatibilidade com as normas sob fiscalização. Não pode olvidar-se que os padrões constitucionais se submetem, eles próprios, a uma interpretação conforme ao direito da União Europeia. Em consequência, atendendo à comunhão de conteúdos entre a Constituição e a CDFUE, se o ato de transposição se revelar contrário às normas europeias cuja ofensa implicou a invalidade da Diretiva, é plausível que transgrida igualmente a Constituição, interpretada em conformidade com aquelas. Importa, pois, saber em que medida as medidas nacionais sob fiscalização conflituam com as normas europeias em causa.
A primeira decisão do Tribunal de Justiça sobre a compatibilidade com a CDFUE de regimes nacionais adotados em transposição da Diretiva 2006/24/CE (entretanto declarada inválida) foi o Acórdão de 21 de dezembro de 2016, *Tele2*, proc. C-203/15 e C-698/15. Aí se considerou que o estabelecimento, pelo legislador nacional, de uma obrigação de conservação de *todos os dados de*

*tráfego* de *todos os utilizadores e assinantes* padecia da mesma incompatibilidade com a CDFUE que havia sido assacada à diretiva em que se baseou. Em consequência, o Tribunal de Justiça indicou, por via da interpretação do artigo 15.º da Diretiva n.º 2002/58/CE, o figurino da legislação nacional que pode ter-se por compatível com os direitos garantidos pela Carta, cumprindo os requisitos de restrição estabelecidos no seu artigo 52.º: a norma do artigo 15.º da Diretiva n.º 2002/58/CE, conjugada com o disposto nos artigos 7.º, 8.º e 52.º da Carta, *«(…) não se opõe a que um Estado-Membro adote uma regulamentação que permita, a título preventivo, a conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos de luta contra a criminalidade grave, desde que a conservação dos dados seja limitada ao estritamente necessário, no que se refere às categorias de dados a conservar, aos equipamentos de comunicação visados, às pessoas em causa e à duração de conservação fixada»* (n.º 108). O que impõe, por isso, a previsão de *«normas claras e precisas que regulem o âmbito e a aplicação dessa medida de conservação dos dados e que imponham exigências mínimas, de modo a que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso»* (n.º 109), que subordine a conservação de dados *«a critérios objetivos, que estabeleçam uma relação entre os dados a conservar e o objetivo prosseguido»* (n.º 110) e que opere uma delimitação do universo de pessoas e de situações por ela abrangidas, que *«deve basear-se em elementos objetivos que permitam visar um público cujos dados sejam suscetíveis de revelar uma relação, pelo menos indireta, com atos de criminalidade grave, de contribuir de uma maneira ou outra para a luta contra a criminalidade grave ou de prevenir um risco grave para a segurança pública»* (n.º 111).

Já no que respeita ao *acesso aos dados* pelas autoridades nacionais competentes para deteção, prevenção e combate à criminalidade, concluiu-se que o normativo comunitário implica a previsão de controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente, na sequência de um pedido formulado pela autoridade nacional competente (i), a definição de critérios e condições de admissão desse acesso (ii), a obrigação de informar as pessoas visadas (a partir do momento em que essa comunicação não seja suscetível de comprometer a investigação), para que possam exercer o direito de recurso a que se refere o n.º 2 do artigo 15.º da Diretiva (iii) e a previsão de obrigação armazenamento dos dados no território da União, bem como a sua destruição no termo do respetivo período de conservação (iv) (Acórdão *Tele 2*, n.ºs 119 a 122).

Em outubro de 2020, o Tribunal de Justiça voltou a pronunciar-se sobre a compatibilidade do disposto no artigo 15.º da Diretiva 2002/58/CE, conjugado com os artigos 7.º e 8.º da CDFUE, com regimes jurídicos nacionais que prevejam uma obrigação generalizada da conservação de metadados pelos operadores de telecomunicações com vista a serem transmitidos às autoridades competentes para a ação penal (Acórdão *La quadrature du net, cit.*). Reiterando a jurisprudência do Acórdão *Tele2* quanto aos dados de tráfego e de localização — e considerando, por isso, incompatível com o direito da União Europeia um regime nacional que prescreva a obrigação indiferenciada de dados de tráfego, por restringir desproporcionadamente os direitos consagrados nos artigos 7.º e 8.º da CDFUE (n.ºs 112 a 133) —, pronunciou-se separadamente sobre a obrigação de conservação generalizada de *dados de base* e de *endereços de protocolo IP dinâmicos que indiquem a fonte de uma comunicação* (aqueles que pressupõem uma análise do contexto das comunicações e que, por isso, é duvidosa a sua qualificação como *dados de base* ou *dados de tráfego*). Quanto a estes, e

independentemente da questão de saber qual a sua categorização correta, admitiu a compatibilidade com a CDFUE da sua conservação geral pelo período de um ano (n.ºs 154 a 159).

**9.3.** Uma interpretação dos parâmetros constitucionais em conformidade com o direito da União Europeia deve ainda ter em conta a disciplina do Regulamento Geral sobre a Proteção de Dados (Regulamento UE 2016/679 — RGPD) quanto à proteção conferida *às pessoas singulares* a respeito do tratamento de dados pessoais. Com efeito, os dados de base, de tráfego e de localização, na medida em que permitam identificar uma *pessoa singular* (n.º 1 do artigo 4.º do RGPD), ficam sujeitos à disciplina europeia de tratamento de dados pessoais. Em consequência, tais dados apenas podem ser *recolhidos para satisfazer finalidades determinadas, explícitas e legítimas, e não podem ser tratados posteriormente de uma forma incompatível com essas finalidades* (alínea *b)* do n.º 1 do artigo 5.º do RGDP) e a sua conservação de forma a poder identificar os titulares só pode ocorrer *durante o período necessário para as finalidades para as quais são tratados* (alínea *e)* do n.º 1 do artigo 5.º do RGDP). Sendo certo que o RGPD abrange qualquer tratamento de dados feitos por estabelecimentos situados no território da União (artigo 3.º do RGPD), abarcando assim o tratamento de dados pessoais operado pelos fornecedores de comunicações eletrónicas em Portugal.
Ora, decorre das regras do RGPD (que, enquanto Regulamento da União Europeia, vincula todos os sujeitos públicos e privados, em toda a União — artigo 288.º TFUE) que os dados pessoais que venham a ser objeto de tratamento não podem ser *transferidos* para Estados terceiros, salvo nas condições fixadas nos artigos 44.º a 40.º do RGPD: a existência de uma decisão de adequação pela Comissão Europeia (artigo 45.º) ou, nos demais casos, de uma atuação fiscalizadora pela autoridade nacional de controlo (artigos 46.º e seguintes), quando se garanta um nível de proteção similar àquele que é garantido pelo normativo europeu.

**10.** Determinados o conteúdo e a relevância do direito da União Europeia para os presentes autos, importa agora apreciar a conformidade constitucional das normas fiscalizadas. Começar-se-á, assim, por apurar o concreto sentido dos padrões constitucionais mobilizáveis — interpretando-os, como se viu *supra,* à luz do direito da União Europeia, face ao disposto no n.º 4 do artigo 8.º da Constituição. O que não implica que o direito da União Europeia constitua o único instrumento a influir na interpretação dos parâmetros constitucionais convocados, como se sublinhou no Acórdão n.º 403/2015, por força do disposto no artigo 16.º da Constituição:
«o artigo 12.º da Declaração Universal dos Direitos do Homem declara que "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência (…)". A mesma redação é retomada pelo artigo 17.º do Pacto Internacional relativo aos Direitos Civis e Políticos. Ambos os textos prescrevem que o indivíduo tem direito à proteção da lei contra tais intervenções ou tais atentados.
O artigo 8.º da Convenção Europeia dos Direitos do Homem (CEDH), por seu turno, estabelece que "qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência". Nos termos do n.º 2, "não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a

segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros". O Tribunal Europeu dos Direitos do Homem (TEDH) tem desenvolvido uma ampla jurisprudência sobre a proteção do acesso a dados de comunicações, afirmando expressamente que os mesmos se encontram abrangidos pela proteção de "vida privada e familiar" ínsita no n.º 1 do artigo 8.º da CEDH. Assim, no caso Malone c. Reino Unido, referiu que o acesso e uso de dados respeitantes a tráfego de comunicações constituem matéria que é abrangida pelo âmbito de proteção do n.º 1 do artigo 8.º da CEDH (Acórdão de 02/08/1984, queixa n.º 8691/79)».

Sustenta a requerente que as normas dos artigos 4.º e 6.º da Lei n.º 32/2008, de 17 de julho — atinentes ao regime da conservação dos dados — restringem de modo desproporcionado os direitos à reserva da intimidade da vida familiar (n.º 1 do artigo 26.º da Constituição) e à inviolabilidade das comunicações (n.º 1 do artigo 34.º da Constituição), interpretados à luz da Carta dos Direitos Fundamentais da União Europeia, enfermando por isso de inconstitucionalidade material. Já quanto à norma contida no artigo 9.º da Lei n.º 32/2008, de 17 de julho, que consagra o regime da transmissão e acesso dos dados às autoridades competentes para a investigação, deteção e repressão dos crimes graves, a requerente imputa a desconformidade constitucional ao facto de, nos termos da regra fiscalizada, o visado não ser informado de que os dados que é titular foram transmitidos e tratados pelas autoridades de polícia criminal, postergando-lhe a discussão judicial da legalidade da medida e atentando, assim, contra o direito a uma tutela jurisdicional efetiva, consagrado no artigo 20.º da Constituição.

Ora, de acordo com a jurisprudência deste Tribunal, a tutela constitucional dos *metadados* das comunicações (dados que não abrangem o conteúdo das comunicações, mas dizem respeito somente às suas circunstâncias) não é uniforme: a distinção entre *dados de base*, relativos à identificação dos sujeitos que se conectam à rede, e *dados de tráfego — «os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência)»* — tem refração nos parâmetros convocáveis. Deste modo, o padrão invocado pela requerente (o direito à inviolabilidade das comunicações, consagrado no artigo 34.º da Constituição) não protege os *dados de base*, como se concluiu nos Acórdãos n.ºs 486/2009 e 403/2015, e se reiterou no Acórdão n.º 463/2019:

*«Assim, quer os dados de base, quer os dados de localização de equipamento, a que se refere o artigo 3.º da Lei Orgânica, n.º 4/2017, não devem ser considerados como dados atinentes a uma comunicação, já que tanto nuns quanto noutros inexiste qualquer dimensão subjetiva inerente à comunicação. Os primeiros são, nos termos da alínea a) do n.º 2 do artigo 2.º da mesma Lei, dados escritos atinentes a uma relação contratual entre uma pessoa e uma empresa operadora de telecomunicações, referindo-se à identificação e morada do titular e ao próprio contrato de ligação à rede; os segundos abrangem a deteção de dados de localização a partir de um telefone ligado, mas em stand by, e/ou através do sistema de satélite GPS ou outro (ver, neste sentido, Manuel da Costa Andrade, "Comentário ao artigo 194.º do Código Penal", in J. Figueiredo Dias (direção), Comentário Conimbricense do Código Penal — Tomo I, 2.ª Edição, Coimbra Editora, 2012, pág. 1104)».*

Neste contexto, *nem todos* os dados a que se refere o artigo 4.º da Lei n.º 32/2008, de 17 de julho, estão protegidos pelo disposto nos números 1 e 4 do artigo 34.º da Constituição. De acordo com a jurisprudência reiterada deste Tribunal, aquele parâmetro abrange os *dados de tráfego* quando *pressuponham uma comunicação entre pessoas*, mas já não os dados que, independentemente de qualquer comunicação, sejam atinentes à conexão de certo equipamento a uma rede de comunicações ou à mera identificação de um utilizador a quem estava atribuído um determinado número de telefone ou um endereço de protocolo IP estático (*dados de base* — cfr. Acórdão n.º 420/2017); nem os *dados de tráfego* gerados pela comunicação entre um sujeito e uma máquina — *v. g.*, a consulta de sítios da internet.

Simplesmente, o princípio do pedido não obsta a que o Tribunal Constitucional possa declarar a inconstitucionalidade das normas cuja apreciação foi requerida com fundamento diverso daqueles cuja violação foi invocada (n.º 5 do artigo 51.º da LTC). O que implica a consideração da proteção constitucional da conservação de *todos os metadados* identificados nas normas fiscalizadas — independentemente da categoria em que se insiram (dados de base / dados de tráfego) e de darem ou não suporte a comunicações intersubjetivas.

Ora, a conservação e acesso a todos os metadados a que se referem as normas fiscalizadas — *dados de base, dados de tráfego que não pressupõem uma comunicação interpessoal* e *dados de tráfego relativos a comunicações interpessoais* —, porque são aptos a revelar aspetos relevantes da vida privada e familiar dos cidadãos, submete-se a outras garantias constitucionais — designadamente, os direitos à reserva da intimidade da vida privada e ao livre desenvolvimento da personalidade (n.º 1 do artigo 26.º da Constituição) e o direito à autodeterminação informativa (n.ºs 1 e 4 do artigo 35.º da Constituição). O tratamento de todos estes dados, ao manter o rastreio dos passos dos utilizadores, seja quanto à sua localização, seja quanto à utilização que faz da internet, seja quanto às pessoas com quem contacta ou tenta contactar, por telefone, correio eletrónico, mensagens escritas ou através da internet, é suscetível de comprimir os direitos à reserva da intimidade da vida privada, ao livre desenvolvimento da personalidade e à autodeterminação informativa. Como sublinha a requerente no artigo 8.º do pedido, permitem rastrear a sua localização «*ao longo do dia, todos os dias (desde que transporte o telemóvel ou outro dispositivo eletrónico de acesso a Internet), e identificar com quem contacta (chamada — inclusive as tentadas e não concretizadas — por telefone ou telemóvel, envio ou receção de SMS, MMS, de correio eletrónico, ou de comunicações telefónicas através da Internet), bem como a duração e a regularidade dessas comunicações*». Razão pela qual se concluiu no Acórdão n.º 403/2015:

«*a manipulação ilegal ou ilegítima do conteúdo e das circunstâncias da comunicação pode violar a privacidade dos interlocutores intervenientes, atentando ou pondo em risco esferas nucleares das pessoas, das suas vidas, ou dimensões do seu modo de ser e estar. De sorte que a possibilidade de se aceder aos dados das comunicações colide com um conjunto de valores associados à vida privada que fundamentam e legitimam a proteção jurídico-constitucional.*

*Desde logo, a liberdade de ação, enquanto vertente do direito ao desenvolvimento da personalidade, de acordo com a qual, na interação com os outros, a condução da vida de cada um é autoconformada pela sua atuação, o que pressupõe, como referem Gomes Canotilho e Vital Moreira "a exigência de proibição de ingerências dos*

*poderes públicos (...) como, por exemplo, (...) 'o direito a não ser espiado' " (Constituição da República Portuguesa Anotada, 2. ed., Vol. I, pág. 465).*
*Depois, com a esfera íntima e a esfera privada da pessoa humana, seja enquanto pretensão de isolamento, tranquilidade e exclusão do acesso dos outros a si próprio (direito à solidão), seja, enquanto impedimento à ingerência dos outros (direito ao anonimato), seja ainda, mais modernamente, e perante a insuficiência protetora das referidas dimensões, enquanto controlo das informações que lhe dizem respeito e de subtração ao conhecimento dos outros os factos reveladores do modo de ser do sujeito na condução da sua vida privada (autodeterminação informacional). Como refere Joaquim Sousa Ribeiro, esta última dimensão, hoje a de maior relevo, «impede que o "eu" seja objeto de apropriação pelos outros, como matéria de comunicação na esfera pública. Nela conjuga-se o direito ao segredo (à intromissão dos outros na esfera privada, com tomada de conhecimento de aspetos a ela referentes) e um direito à reserva (proibição de revelação)» – cfr. A Tutela de bens da personalidade na Constituição e na Jurisprudência constitucional portuguesas, in Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho, Vol. III, Coimbra Editora, pág. 853).*
*Estes direitos encontram-se hoje expressamente consagrados no artigo 26.º da CRP e são intimamente interligados, constituindo a reserva da intimidade da vida privada uma dimensão do direito, mais amplo, referente ao desenvolvimento da personalidade».*

Deste modo, nos termos do n.º 5 do artigo 51.º da LTC, a ponderação da conformidade constitucional das normas dos artigos 4.º e 6.º da Lei n.º 32/2008, de 17 de julho, far-se-á, em primeira linha, à luz dos direitos fundamentais que parametrizam todas as categorias de dados identificadas nas normas indicadas pela requerente — concretamente os direitos ao livre de desenvolvimento da personalidade e à autodeterminação informativa.

**11.** É reconhecido que o direito ao livre desenvolvimento da personalidade abrange a faculdade de comunicar com segurança, enquanto parte da sua liberdade de ação e de realização pessoal. Com efeito, aquele constitui um direito de muito largo espectro, expressando a tutela geral de uma esfera de liberdade pessoal. Em consonância, no Acórdão n.º 464/2019, concluiu-se que «*uma das dimensões da liberdade de ação inerente ao desenvolvimento da personalidade consiste na liberdade de comunicar, tuteladora da comunicação interpessoal: "a comunicação que se destina a um recetor individual ou a um círculo de destinatários previamente determinado" (Acórdão n.º 403/2015, ponto 13). Tal liberdade abrange, deste modo, "a faculdade de comunicar com segurança e confiança e o domínio e autocontrole sobre a comunicação, enquanto expressão e exteriorização da própria pessoa" (v. ibidem)*». É neste contexto de que se pode falar «*de um "direito à autodeterminação comunicativa" que serve para defender vários bens jurídico-constitucionais, entre eles: o direito ao desenvolvimento da personalidade e o direito à reserva da intimidade da vida privada*» (Acórdão n.º 403/2015). Como se disse neste aresto:
*«Na vertente de defesa da reserva da intimidade da vida privada, o direito à autodeterminação comunicativa protege a esfera pessoal perante as ingerências públicas ou privadas, ou seja, o interesse das pessoas que comunicam em impedir ou em controlar a tomada de conhecimento, a divulgação e circulação do conteúdo e circunstâncias da comunicação. Neste sentido, os interlocutores intervenientes têm direito a um ato negativo: à não intervenção de terceiros na comunicação e nas circunstâncias que a acompanham. Trata-se de uma garantia de que devem beneficiar, prima facie, todas as comunicações privadas, independentemente de as*

*mesmas dizerem ou não respeito à intimidade dos intervenientes (cfr. Lucrecio Rebollo Delgado, El Secreto de las Comunicaciones: Problemas Actuales, Revista de Derecho Político, n.º 48-49, 2000, pág. 363).*
*No entanto, o direito à autodeterminação comunicativa abrange ainda esferas de proteção mais amplas que a da simples reserva da vida privada. É que o progresso tecnológico, ao facilitar a acumulação, conservação, circulação e interconexão de dados referentes às comunicações, aumentou as possibilidades de devassa. Agora é o próprio domínio de atuação do individuo que é posto em causa, pois já não tem meios para assegurar a confidencialidade da comunicação. A liberdade de, à distância, trocar com os destinatários livremente escolhidos por cada um, informações, notícias, pensamentos e opiniões está comprometida com as inimagináveis possibilidades da sua afronta pelos avanços tecnológicos. Por isso, é necessário assegurar que a comunicação à distância entre privados se processe como se os mesmos se encontrassem presentes, i.e., que as comunicações entre emissor e recetor, bem como o seu circunstancialismo, se tenham como uma comunicação fechada, em que os sujeitos se autodeterminam quanto à realização da mesma e esperam, legitimamente, que a comunidade proteja o circunstancialismo daquela pretendida comunicação. Ora, como a interação entre pessoas que se encontram à distância tem de ser feita através da mediação necessária de um terceiro, de um fornecedor de serviços de comunicação, exige-se que esse operador e o Estado regulador também garantam a integridade e confidencialidade dos sistemas de comunicação.*
*Neste contexto, o direito à autodeterminação comunicativa assume-se como um direito de liberdade, de liberdade para comunicar, sem receio ou constrangimentos de que a comunicação ou as circunstâncias em que a mesma é realizada possam ser investigadas ou divulgadas. Sem essa confiança, o indivíduo sentir-se-á coartado na liberdade de poder comunicar com quem quiser, quando quiser, pelo tempo que quiser e quantas vezes quiser. Trata-se, pois, de permitir um livre desenvolvimento das relações interpessoais e, ao mesmo tempo, de proteger a confiança que os indivíduos depositam nas suas comunicações privadas e no prestador de serviços das mesmas».*

Ademais, mesmo fora do domínio das comunicações, o direito ao livre desenvolvimento da personalidade abrange o direito ao sigilo dos *dados pessoais* — que, como se viu, não compreende somente aqueles que diretamente identificam uma pessoa, mas também aqueles que, sem esforço excessivo, permitam chegar a essa identificação — como se concluiu no Acórdão n.º 464/2019:
*«Pode, na verdade, afirmar-se que o segredo dos dados pessoais e o poder de controlo do sujeito sobre os mesmos constituem uma garantia do direito ao livre desenvolvimento da personalidade enquanto possibilidade de «interiorização autónoma» da pessoa ou o direito a «autoafirmação» em relação a si mesmo, contra quaisquer imposições heterónomas (de terceiros ou dos poderes públicos). Este direito à "autoafirmação" dá guarida a vários «direitos de personalidade inominados mesmo que não especificamente positivados na Constituição, como por exemplo, o direito aos documentos pessoais e o direito à autodeterminação informativa quanto a dados pessoais constantes de ficheiros manuais ou informáticos, o direito à confidencialidade de dados pessoais constantes de atos ou decisões públicas respeitantes ao estado civil, o direito de não ser espiado no desenvolvimento de atividades lícitas (cf. Gomes Canotilho/Vital Moreira, Vol. I, ob. cit., pp. 464-465».*

Ora, a *proibição de ingerência* de terceiros na esfera de autonomia pessoal é indispensável à autoconformação da identidade. Garantindo a liberdade de cada sujeito, já que privacidade e liberdade se relacionam intimamente: a *vida privada* tutelada decorre da liberdade de condução da

vida do titular. O que justifica a previsão autónoma (n.º 1 do artigo 26.º), no seio do direito ao livre desenvolvimento da personalidade (como uma das suas dimensões, mas sem nele se esgotar), do direito à reserva da intimidade da vida privada; e cuja proteção alastra aos dados relativos às comunicações, como se concluiu no Acórdão n.º 403/2015:
*«O Tribunal Constitucional formulou, pela primeira vez, uma definição do conteúdo do direito à reserva da vida privada no Acórdão n.º 128/92, como constituindo o direito de cada um a ver protegido o espaço interior ou familiar da pessoa ou do seu lar contra intromissões alheias, i.e., como um direito a uma esfera privada onde ninguém pode penetrar sem autorização do respetivo titular. No entender do Tribunal, esse direito compreende, por um lado, a autonomia, ou seja, o direito a ser o próprio a regular, livre de ingerências estatais e sociais, essa esfera de intimidade e, por outro, o direito a não ver difundido o que é próprio dessa esfera de intimidade, a não ser mediante autorização do interessado ("direito ao segredo do ser"). E no que toca aos lugares da vida onde a vida privada pode ser manifestada, o Tribunal afirmou ainda que ela abrange «a vida pessoal, a vida familiar, a relação com outras esferas de privacidade (…) o lugar próprio da vida pessoal ou familiar (…) e, bem assim, os meios de expressão e de comunicações privados (a correspondência, o telefone, as conversas orais, etc». De modo que, na jurisprudência constitucional, as comunicações privadas, englobando o conteúdo e circunstancialismos em que as mesmas têm lugar, são reconhecidas como um meio através do qual se manifestam aspetos da vida privada da pessoa e que, por isso, caem no âmbito da proteção constitucional da respetiva reserva».*

Dito de outro modo: o direito à reserva da intimidade da vida tutela os indivíduos contra o acesso a um conjunto de informações que dizem respeito apenas aos próprios (por onde circulam, em que momento, em que contextos), envolvendo a proteção constitucional dos dados que permitem retirar conclusões sobre essas circunstâncias, como se concluiu no Acórdão n.º 464/2019:
*«Na forma específica de proibição de acesso por terceiros, o direito à proteção de dados apresenta-se como um direito de garantia de um conjunto de valores fundamentais individuais — a liberdade e a privacidade — bens jurídicos englobados na autodeterminação individual, abrangendo duas dimensões: a dimensão negativa ou de abstenção do Estado de ingerência na esfera jurídica dos cidadãos e a dimensão positiva enquanto função ativa do Estado para prevenir tal ingerência por parte de terceiros. Na vertente da proibição de tratamento de dados pessoais suscetíveis de gerar discriminação, este direito fundamental está ainda diretamente ligado à garantia da igualdade entre os cidadãos, «[...] demonstrando que a proteção de dados pessoais não tem em si mesmo apenas um objetivo de tutela da privacidade, mas também uma importante função social de garantia da igualdade» (cf. Filipa Urbano Calvão, ob. cit., pág. 90)».*

É neste quadro que se reconhece «*um direito fundamental à autodeterminação informativa, traduzido num conjunto de direitos relacionados com o tratamento automático das informações pessoais dos cidadãos, que visam, simultaneamente, protegê-las perante ameaças de recolha e de divulgação, assim como de outras utilizações possibilitadas pelas novas tecnologias, e, também, assegurar aos respetivos titulares um conjunto de poderes de escolha nesse âmbito*» (CATARINA SARMENTO E CASTRO, "40 Anos de «Utilização da Informática» — O artigo 35.º da Constituição da República Portuguesa", *e-Pública*, vol. 3, n.º 3, 2016, p. 44). A sua consagração expressa, no artigo 35.º da Constituição, assegura ao titular o poder de decidir sobre o uso e divulgação dos seus dados pessoais; o poder de controlar a informação disponível a seu respeito.

Este direito, ainda que possa ser modelado como *direito-garantia* do direito à reserva da intimidade da vida privada — estabelecendo uma defesa do cidadão contra intromissões não autorizadas de terceiros e do Estado quanto às informações que lhe respeitem — tem um âmbito mais amplo do que aquele: visa impedir que o indivíduo se torne um objeto de informação, garantindo-lhe o domínio sobre os seus próprios dados. É por isso que o direito à autodeterminação informativa é densificado num feixe de posições jurídicas subjetivas estatuídas no artigo 35.º da Constituição: «*(a) direito de acesso das pessoas aos registos informáticos para conhecimento dos seus dados pessoais deles constantes (n.º 1), bem como a rectificação e complementação dos mesmos; (b) direito ao sigilo em relação aos responsáveis de ficheiros automatizados e a terceiros dos dados pessoais informatizados e direito à sua não interconexão (n.º 4); (c) direito ao não tratamento informático de certos tipos de dados pessoais (n.º 3)*». (GOMES CANOTILHO e VITAL MOREIRA, *cit.*, p. 551).

E, note-se, o direito à autodeterminação informativa não depende de qualquer processo comunicacional, como se afirmou no Acórdão n.º 403/2015:

«*E nisto se distingue do direito à autodeterminação informativa consagrado no artigo 35.º da CRP, com vista à proteção das pessoas perante o tratamento de dados pessoais informatizados. O objeto de proteção do direito à autodeterminação comunicativa reporta-se a comunicações individuais efetivamente realizadas ou tentadas e só essas é que estão cobertas pelo sigilo de comunicações. Naquele outro direito protege-se as informações pessoais recolhidas e tratadas por entidades públicas e privadas, cuja forma de tratamento e divulgação pode propiciar ofensas à privacidade das pessoas a que digam respeito. Como refere Maria Eduarda Gonçalves, neste caso, o problema não está na existência ou na quantidade de dados, mas na qualidade, "entendida esta, em termos amplos, como o conjunto das condições da recolha dos dados, seu tratamento e comunicação, bem como as características desses dados, isto é, a sua exatidão, a sua adequação aos fins prosseguidos" (cfr. Direito Da Informação, Almedina, pág. 84). Neste caso, pretende-se impedir que as informações prestadas a um particular ou a uma entidade possam por estes ser divulgadas a outras pessoas ou entidades, ou seja, que a pessoa se torne "simples objeto de informações", face a todos os registos informáticos que vai deixando no seu dia a dia. A proibição de ingerência ou devassa neste domínio implica não apenas a proibição de acesso a terceiros aos dados pessoais, mas ainda a proibição de divulgação ou mesmo de interconexão de ficheiros com dados da mesma natureza (cfr. Gomes Canotilho e Vital Moreira, ob. cit., pág. 554)*»

**12.** A Constituição não ficou, todavia, pela afirmação destas posições jurídicas subjetivas. Fez-lhes acrescer garantias de controlo, assentes no *direito de o visado controlar o tratamento dos dados* e no *dever de o Estado proteger* o direito atribuído. Em conformidade, cometeu ao legislador a previsão de garantias de segurança, impondo a adoção de medidas de proteção dos dados contra perda, destruição e acesso de terceiros. Como se afirmou no Acórdão n.º 464/2019, «*as pessoas têm não apenas o direito de saber o que a seu respeito consta dos registos informáticos, mas também o direito de que esses dados sejam salvaguardados contra a devassa ou difusão. Por sua vez, este último direito engloba vários direitos específicos: (a) a proibição de acesso de terceiros a dados pessoais (artigo 35.º, n.º 4, da Constituição); (b) proibição da interconexão de ficheiros de bases e bancos de dados pessoais (artigo 35.º, n.º 2, da Constituição)*». Onde se inclui, aliás, um *direito ao esquecimento*, garantindo-se ao titular dos dados que a sua conservação e tratamento apenas pode ocorrer por um período de tempo, devendo ser destruídos ou cancelados uma vez obtida a finalidade a que tendiam.

As *garantias de efetividade* — que cabe ao legislador prever — assentam em duas dimensões.

Em primeiro lugar, no seio do direito à autodeterminação informativa, encontra-se o poder de supervisionar essa informação, prevenindo e corrigindo lesões da liberdade individual. O titular goza do direito a conhecer não só que dados pessoais estão a ser *recolhidos e conservados* como também como são *utilizados, comunicados, para que finalidade e para quem* (seja ele do setor público ou privado). Só dessa forma pode o sujeito exercer a faculdade de, designadamente, exigir a eliminação de dados tratados em violação de regras ou princípios constitucionais; e de reagir contra arbitrariedades no seu tratamento: uma vez que a Constituição impede «*que a pessoa se transforme em "simples objeto de informações"*» (Acórdão n.º 355/97), goza o titular do direito de reação em caso de violação dos seus direitos em matéria de tratamento de dados pessoais.

Ora, para que o controlo se torne efetivo, é imperioso que os cidadãos conheçam que os seus dados foram acedidos; que possam eficazmente controlar o modo como são alcançados, controlados e tratados; e que possam recorrer aos tribunais para reagir contra a sua utilização indevida. O que, de resto, o TEDH enfatizou no Acórdão *Big Brother Watch, cit.*, §310: «*after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers*». É isso, de resto, que se consagra na legislação processual penal de alguns países, informando-se o visado de medidas de interceção das comunicações (veja-se o §101 da legislação processual penal alemã [Strafprozeßordnung] que determina a comunicação ao visado de quaisquer meios ocultos de investigação de que tenha sido alvo, a partir do momento em que tal notificação não ponha em causa o sucesso da investigação). Pelo que a autodeterminação informativa implica *o direito de o próprio titular dos dados conhecer* a quem foram transmitidos, por que razões e qual o tratamento desenvolvido; sendo certo que a sua inclusão no catálogo dos direitos, liberdades e garantias envolve a submissão das restrições ao regime dos n.ºs 2 e 3 do artigo 18.º da Constituição.

Em segundo lugar, decorre do n.º 2 do artigo 35.º um controlo da proteção e tratamento dos dados *por uma autoridade administrativa independente,* cuja intervenção é constitucionalmente determinada com funções garantísticas dos particulares. Trata-se de uma dimensão da autodeterminação informativa que o legislador tem de concretizar; e de que encontramos reflexos, na lei ora fiscalizada, na obrigação de os operadores de comunicações que transmitam dados às autoridades de investigação criminal elaborarem registos dessas operações, enviando-os trimestralmente à CNPD (n.º 6 do artigo 9.º da Lei n.º 32/2008, de 17 de julho). No fundo, ao remeter para lei a definição do regime jurídico de proteção dos particulares em matéria de «*tratamento automatizado, conexão, transmissão e utilização*» (n.º 2 do artigo 35.º da Constituição), a Constituição contém uma *imposição legiferante* segundo a qual deve o legislador a assegurar não só o controlo pelo próprio visado (o que implica o conhecimento de que os seus dados foram acedidos) como também a atuação de uma autoridade administrativa independente que assevere a efetividade dos direitos constitucionalmente garantidos em matéria de conservação e tratamento dos dados pessoais. À semelhança, de resto, do que prevê o n.º 3 do artigo 8.º da CDFUE.

Estas duas dimensões têm óbvio reflexo quanto ao local de armazenamento dos dados. Com efeito, a intervenção da *autoridade administrativa independente* a que se refere a Constituição não é compatível com a conservação dos dados em jurisdições subtraídas à respetiva atuação; e o exercício dos poderes de auditoria pelos próprios sujeitos visados não é viável se os dados forem

armazenados em países cujos ordenamentos não ofereçam similares garantias. Nessa medida, a efetividade dos direitos conferidos pelos n.ºs 1 e 2 do artigo 35.º — incluindo a garantia de fiscalização por autoridade administrativa independente — depende do local da sua conservação, assacando-se ao legislador a obrigação de previsão do seu armazenamento em local compatível com o exercício das garantias constitucionais de proteção e com a intervenção da autoridade administrativa independente (n.º 2 do artigo 35.º da Constituição).

Similar conclusão foi, de resto, extraída pelo Tribunal de Justiça da União Europeia, ao determinar que as garantias de segurança a que se refere o n.º 3 do artigo 8.º da CDFUE dependem do local de conservação dos dados. Ao declarar a invalidade da Diretiva n.º 2006/24/CE, considerou o Juiz comunitário que «*a referida diretiva não impõe que os dados em causa sejam conservados no território da União, pelo que não se pode considerar que esteja plenamente garantida a fiscalização, por uma entidade independente, expressamente exigida pelo artigo 8.º, n.º 3, da Carta, do respeito das exigências de proteção e de segurança, tal como referidas nos dois números anteriores. Ora, semelhante fiscalização, efetuada com base no direito da União, constitui um elemento essencial do respeito da proteção das pessoas relativamente ao tratamento dos dados pessoais*» (Acórdão *Digital Rights*, n.º 68). O que se reiterou no Acórdão *Tele 2* (*cit.*):

«*122 (…) Tendo em conta a quantidade de dados conservados, o caráter sensível desses dados bem como o risco de acesso ilícito aos mesmos, os prestadores de serviços de comunicações eletrónicas devem, para assegurar a plena integridade e a confidencialidade dos referidos dados, garantir um nível particularmente elevado de proteção e de segurança através de medidas técnicas e de organização adequadas. Em especial, a regulamentação nacional deve prever a conservação no território da União bem como a destruição definitiva dos dados no termo do respetivo período de conservação (v., por analogia, no que se refere à Diretiva 2006/24, acórdão Digital Rights, n.ºs 66 a 68).*

*123 Seja como for, os Estados-Membros devem garantir o controlo, por parte de uma autoridade independente, do respeito do nível de proteção garantido pelo direito da União em matéria de proteção das pessoas singulares relativamente ao tratamento dos dados pessoais, sendo esse controlo explicitamente exigido pelo artigo 8.º, n.º 3, da Carta e constituindo, em conformidade com jurisprudência constante do Tribunal de Justiça, um elemento essencial do respeito da proteção das pessoas relativamente ao tratamento dos dados pessoais. Se assim não fosse, as pessoas cujos dados pessoais estivessem conservados ficariam privadas do direito, garantido pelo artigo 8.º, n.ºs 1 e 3, da Carta, de apresentar pedidos às autoridades nacionais de controlo para efeitos da proteção dos seus dados (v., neste sentido, acórdão Digital Rights, n.º 68, e de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.ºs 41 e 58)».*

Daqui decorre a conclusão de que as garantias contidas no direito à autodeterminação informativa dependem da estatuição legal de armazenamento dos dados pessoais num *Estado-Membro da União Europeia*: é nessas jurisdições que vigoram os padrões de proteção constitucionalmente impostos — plasmados quer nas Constituições nacionais, quer na CDFUE, quer nas normas de direito europeu derivado (designadamente, o RGPD) — e se assegura a atuação da autoridade administrativa independente (mesmo transfronteiriça), por atenção à *rede de autoridades de controlo* prevista no sistema de proteção europeu de dados pessoais (que remonta, de resto, à Diretiva n.º 95/46/CE; e que se encontra atualmente consagrada nos artigos 52.º e seguintes

do RGPD; e no artigo 2.º da Lei n.º 43/2004, de 18 de agosto, na redação que lhe foi dada pela Lei n.º 58/2019, de 9 de agosto).

Aliás, é esta mesma injunção que estará subjacente à opção do legislador relativa à *transferência* para Estados terceiros de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais (artigos 37.º e seguintes da Lei n.º 59/2019, de 8 de agosto; e artigos 35.º e seguintes da Diretiva UE 2016/680, de 27 de abril de 2016); e ao regime geral de proteção de dados pessoais de pessoas singulares, (artigos 44.º e seguintes do RGPD). Em todos estes diplomas se estabelece uma regra de proibição de *transferência* de dados para Estados terceiros, salvo se não puser em causa a vigência das garantias jusfundamentais associadas ao direito à autodeterminação informativa.

Nessa medida, o disposto no artigo 35.º da Constituição, interpretado em conformidade com os artigos 7.º e 8.º da CDFUE, impõe ao legislador, como condição de efetividade das garantias nele consagradas, a previsão da obrigatoriedade de armazenamento dos dados pessoais num Estado-Membro da União Europeia.

**13.** No que respeita à norma contida no artigo 9.º da Lei n.º 32/2008, de 17 de julho, invoca a requerente a violação do direito à tutela jurisdicional efetiva consagrado no n.º 1 do artigo 20.º da Constituição: porque se não prevê um qualquer mecanismo que permita que os sujeitos conheçam que os seus dados foram transmitidos às autoridades públicas — designadamente não se estabelecendo um dever de notificação aos visados das medidas de transmissão — impossibilita-se, na prática, reação e defesa judiciais contra acessos ilegítimos aos dados transmitidos. Isto é, o facto de se não disciplinar na lei a notificação aos sujeitos cujos dados retidos foram efetivamente acedidos coartará os interessados de mecanismos jurisdicionais de defesa sobre essa interceção.

No fundo, porque no conteúdo do direito à tutela jurisdicional efetiva se encontra o acesso a juízo para sustentar as pretensões subjetivas de que o interessado é titular, impõe a Constituição que os interesses jurídicos dignos de tutela possam ser defendidos em tribunal. Ora, se o legislador não tiver previsto mecanismos que tornem exequível o controlo *judicial* de certo direito (legal ou constitucionalmente atribuído), ocorre a violação reflexa do direito que o interessado visava proteger pela via judiciária. O que sucederá não apenas no caso de ausência de mecanismos processuais, como também quando o legislador estabeleça limitações substanciais ao seu exercício. Nessa medida, a *inexistência de notificação ao visado de que os seus dados foram acedidos* depois de terminada a sua utilidade para o processo penal implicará, segundo a requerente, a preclusão do seu direito à justiça e aos tribunais. A questão foi posta justamente deste modo pelo TEDH no Acórdão *Big Brother Watch, cit.*, §310: «*after the surveillance has been terminated, the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers*».

O direito de acesso aos tribunais, revestindo uma dimensão *prestacional* (cometendo ao Estado a criação de um aparelho judiciário e a definição das condições para o respetivo acesso), inclui simultaneamente uma vertente garantística, ao assegurar que ninguém pode ser privado de aceder à justiça. É por isso que o Tribunal Constitucional, nos Acórdãos n.os 364/2004 e 301/2009, concluiu ser-lhe aplicável o regime específico dos direitos, liberdades e garantias, por ter natureza análoga aos enunciados no título II da Constituição (artigo 17.º da Constituição): «*Na verdade, o Estado*

*encontra-se constitucionalmente vinculado a uma actividade prestativa que satisfaça o direito dos cidadãos de acesso à justiça (artigo 20.º da CRP). Este direito corresponde a um direito fundamental dotado da força jurídica própria dos direitos, liberdades e garantias, pelo que o princípio da proporcionalidade, sempre vigente, como princípio básico do Estado de direito, em qualquer campo de actuação estadual que contenda com interesses dos particulares, encontra aqui uma qualificada expressão aplicativa (artigo 18.º, n.º 2, da CRP)*». Neste contexto, as respetivas restrições submetem-se aos requisitos do artigo 18.º da Constituição.

**14.** Apurado o conteúdo dos parâmetros constitucionais que balizam as normas fiscalizadas — que, como se viu, incidem *por um lado* num regime de conservação generalizada pelos fornecedores de comunicações eletrónicas dos metadados identificados no artigo 4.º e, *por outro*, na disciplina da sua transmissão às autoridades de investigação criminal (essencialmente contida no artigo 9.º) — importa agora proceder à apreciação da sua conformidade constitucional.

Pode pôr-se a questão de saber se deve apreciar-se isoladamente a constitucionalidade dos dois regimes ou se a conformidade constitucional das normas fiscalizadas implica a análise do regime global estabelecido pelo legislador. Isto é, se deve o Tribunal Constitucional apreciar o regime da *conservação dos dados* pelos operadores de telecomunicações sem considerar a disciplina estabelecida para a sua transmissão às autoridades de investigação criminal ou se, pelo contrário, a ponderação desta é relevante para o juízo de constitucionalidade que é pedido.

A favor da apreciação separada da constitucionalidade dos dois regimes pronunciou-se a requerente, nos artigos 31.º e seguintes do pedido: «*tratando-se de dois níveis diferentes de agressão aos direitos, não é possível argumentar que o facto de a Lei n.º 32/2008 satisfazer, no que respeita ao regime de acesso aos dados conservados, as exigências decorrentes da Carta, serve para salvar ou compensar a afetação dos direitos implicada na própria imposição legal de conservação de dados. Perante a existência de dois momentos autónomos de agressão aos direitos, não é de todo legítimo confundi-los de acordo com uma "lógica de compensação". Pelo contrário, uma dogmática correcta de direitos fundamentais exigirá que se analise, autonomamente, a conformidade constitucional de cada uma das agressões aos direitos, em nada podendo o regime de acesso e de utilização dos dados interferir na análise da conformidade constitucional, designadamente e no que respeita as exigências decorrentes do princípio da proporcionalidade, da agressão aos direitos implicada na própria imposição legal de conservação de dados*». Segundo esta linha de raciocínio, porque a medida legislativa de conservação de dados implica em si mesma uma restrição ao direito fundamental à reserva da intimidade da vida privada — ainda que nunca sejam transmitidos às autoridades de polícia criminal —, o facto de o regime do seu *acesso pelas autoridades públicas* ser eventualmente conforme aos pressupostos constitucionais de restrição não pode influir no juízo de constitucionalidade relativo à *conservação*.

A requerente invoca ainda que, no plano europeu, o Tribunal de Justiça rejeitou expressamente, no Acórdão *Tele2* (*cit.*), a tese de apreciação do regime da conservação dos dados à luz das garantias fixadas para o seu acesso — que havia sido proposta pelo Advogado-Geral (Conclusões de 19 de julho de 2016, n.ºs 192 a 215). Com efeito, o Acórdão *Tele 2* (*cit.*) analisa separadamente a conformidade com a CDFUE dos regimes de conservação de dados (n.ºs 62 a 112) e do acesso aos dados (n.º 113 e seguintes), ideia que o TJUE reiterou no Acórdão *La quadrature du net* (*cit.*), n.º 116: «*É igualmente irrelevante que os dados conservados sejam ou não utilizados posteriormente (v., por*

*analogia, no que diz respeito ao artigo 8.º da CEDH, TEDH, 16 de fevereiro de 2000, Amann c. Suíça, CE:ECHR:2000:0216JUD002779895, § 69, e de 13 de fevereiro de 2020, Trjakovski e Chipovski c. Macedónia do Norte, CE:ECHR:2020:0213JUD005320513, § 51), uma vez que o acesso a tais dados constitui, independentemente da utilização que deles seja feita posteriormente, uma ingerência distinta nos direitos fundamentais referidos no número anterior».*

Parece, aliás, ter sido esse o caminho seguido pelo Tribunal Constitucional da Roménia no Acórdão 440/2014, de 8 de julho de 2014 (disponível na internet, em língua romena, via https://privacy.apti.ro/decizia-curtii-constitutionale-date-trafic/), quando no §60 separa o juízo de constitucionalidade relativo ao regime da conservação de metadados e ao regime de acesso aos dados armazenados.

Importa tomar posição sobre o problema.

Não é decisivo que o Tribunal de Justiça haja estruturado a apreciação da conformidade com a CDFUE do regime da conservação dos dados sem considerar os termos em que o acesso aos dados era disciplinado. Com efeito, como se concluiu no Acórdão n.º 420/2017, o Tribunal Constitucional faz um juízo autónomo da constitucionalidade das normas nacionais, tendo sempre em conta o efeito útil do direito da União Europeia e a interpretação dos parâmetros nacionais em conformidade com os europeus.

Ora, mesmo sem pôr em causa que a mera conservação dos dados e a sua transmissão às autoridades de polícia criminal constituem restrições *distintas* aos direitos fundamentais à reserva da intimidade da vida privada e à autodeterminação informativa, o exame dos pressupostos constitucionais da limitação — com especial relevância para o princípio da proporcionalidade — implica a consideração dos seus efeitos na posição subjetiva dos cidadãos. Com efeito, um maior rigor do legislador no acesso e na transmissão dos dados conservados pode, em abstrato, autorizar uma maior amplitude no domínio da sua conservação pelos operadores, contanto se garanta a sua segurança. Isto é, ainda que a medida de conservação constitua *em si mesma* uma compressão de direitos fundamentais constitucionalmente consagrada — e, assim, passível de um juízo autónomo de censura — do ponto de vista da proporcionalidade da restrição aos direitos à reserva da intimidade da vida privada e à autodeterminação informativa (sobretudo nos cânones da *necessidade* e da *proporcionalidade em sentido estrito*), não é indiferente a consideração das condições de análise, tratamento e transmissão às autoridades públicas dos dados conservados. Apesar de a sua simples conservação constituir, por si só, uma limitação daqueles direitos, a intensidade da restrição depende em boa medida das garantias inerentes à transmissão e acesso a esses dados.

Foi esta a opção tomada por este Tribunal no Acórdão n.º 420/2017, quando apreciou a constitucionalidade da obrigação de conservação dos *dados de base* pelos operadores de telecomunicações, consagrada no artigo 4.º da Lei n.º 32/2008: «*Também é de ter em atenção o regime previsto para o acesso a estes dados, com limitação do universo de titulares de dados sujeitos à transmissão (artigo 9.º, n.º 3, da Lei n.º 32/2008), e impondo a necessidade de autorização prévia, por despacho fundamentado do juiz de instrução, que deve respeitar os princípios da adequação, necessidade e proporcionalidade, a requerimento do Ministério Público ou da autoridade de polícia criminal competente (artigo 9.º, n. 1, 2 e 4, da Lei n.º 32/2008)*». Igualmente, foi o *iter* seguido pelo TEDH no Acórdão *Breyer, cit.*, a propósito da conformidade com o artigo 8.º da CEDH do regime de

conservação dos dados de base relativos aos cartões SIM: para concluir que a obrigação de conservação desses dados *não viola* a CEDH, por obedecer ao princípio da proporcionalidade, o Tribunal de Estrasburgo levou em consideração o regime da transmissão daqueles dados às autoridades públicas (§§100 e 101), bem como as condições de que dispõem os sujeitos visados para controlar o acesso a tais dados pelos órgãos de investigação criminal (§103).
Ora, tendo em conta que o direito da União Europeia, tal como recebido pelo n.º 4 do artigo 8.º da Constituição, prescreve uma interpretação dos parâmetros constitucionais em conformidade com as normas europeias, de modo a alcançar o seu pleno efeito útil (cfr. *supra,* ponto 8.), a modificação da metodologia já seguida pelo Tribunal Constitucional apenas se imporia caso redundasse em proteção jusfundamental incompatível com os parâmetros extraíveis da CDFUE. No fundo, só se dessa forma se concluísse por um juízo de *não inconstitucionalidade* e se as normas fiscalizadas fossem tidas por incompatíveis com o direito da União Europeia seria necessário apurar se a ponderação isolada das normas fiscalizadas implicaria conclusão diversa que, assim, pudesse ter-se como mais adequada à plena eficácia do direito da União Europeia.
Deste modo, razões não há para que, *prima facie,* se altere a orientação seguida por este Tribunal no Acórdão n.º 420/2017.

**15.** Ao determinar a conservação e o armazenamento dos dados pessoais aí elencados pelo período de um ano, as normas dos artigos 4.º e 6.º da Lei n.º 32/2008, de 17 de julho, constringem, pelo menos, os direitos à reserva da intimidade da vida privada, ao livre desenvolvimento da personalidade e à autodeterminação informativa. Com efeito, o excurso precedido (cfr. ponto 12.) demonstra que aquela normação afeta o conteúdo das garantias constitucionais.
Deste modo, o problema que é posto ao Tribunal é o de saber se estão preenchidos os pressupostos para a legitimidade constitucional da compressão. O que depende, atenta a natureza de *direitos, liberdades e garantias* dos direitos restringidos, da necessidade de salvaguardar outros direitos ou interesses constitucionalmente protegidos e do estrito cumprimento do princípio da proporcionalidade.
Não parecem restar dúvidas que a investigação, prevenção e repressão de crimes graves, definidos como «*crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima*» (alínea *g)* do n.º 1 do artigo 2.º da Lei n.º 32/2008) — finalidade elencada no n.º 1 do artigo 1.º da Lei n.º 32/2008 — assume relevo constitucional, por se dirigir à salvaguarda da legalidade democrática e da ação penal. Isso mesmo, aliás, foi reconhecido no Acórdão do Tribunal Constitucional n.º 420/2017 e está em consonância com a conclusão do Tribunal de Justiça, no Acórdão *Digital Rights,* segundo a qual a luta contra a criminalidade grave e o terrorismo constituem objetivos de interesse geral da União (n.ºs 41 a 43).
Nestes termos, há que apurar se as medidas em causa, enquanto restrições a direitos, liberdades e garantias, cumprem os demais pressupostos constitucionais a que se sujeitam.

**16.** No seguimento das conclusões precedentes, e ainda antes de quaisquer ponderações de proporcionalidade, é desde logo evidente que as normas fiscalizadas não obedecem a uma das

condições de que depende a conformidade constitucional das medidas legislativas relativas à conservação de dados pessoais: o legislador não prescreveu a necessidade de o armazenamento dos dados ocorrer no território da União Europeia, pondo em causa a efetividade dos direitos avalizados pelos n.ºs 1 e 4 do artigo 35.º da Constituição, interpretados em conformidade com o disposto nos artigos 7.º e 8.º da CDFUE.

Ao admitir que tais dados possam ser conservados em países subtraídos à fiscalização por autoridade administrativa independente e aos direitos de auditoria dos visados, o legislador transgride a injunção de previsão do seu armazenamento em local em que sejam efetivas as garantias constitucionais de proteção e a intervenção da autoridade administrativa independente (n.º 2 do artigo 35.º da Constituição), falecendo a garantia de proteção destes dados contra a devassa ou difusão. Com efeito, o ordenamento apenas tutelou a *transferência* para Estados terceiros de tais dados pessoais e somente no que respeita a pessoas singulares; não tendo determinado, como resultava da injunção constitucional, a obrigação de armazenamento desses dados num Estado-Membro da União Europeia.

É quanto basta para concluir pela inconstitucionalidade, por violação do direito à autodeterminação informativa, consagrado nos n.ºs 1 e 4 do artigo 35.º da Constituição, interpretado em conformidade com o disposto nos artigos 7.º e 8.º da CDFUE, das normas contidas nos artigos 4.º e 6.º da Lei n.º 38/2008, de 17 de julho.

**17.** Sucede, no entanto, que não seria suficiente cumprir aquela injunção para que se pudesse concluir pela solvência constitucional de tais normas. Com efeito, mesmo que o legislador tivesse previsto tal obrigação, as normas fiscalizadas sempre envolveriam — pelo menos quanto aos dados de tráfego — uma restrição desproporcionada aos direitos consagrados nos n.ºs 1 e 4 do artigo 35.º da Constituição, em conjugação com o n.º 1 do artigo 26.º, interpretados em conformidade com o disposto nos artigos 7.º e 8.º da CDFUE. Vejamos.

**17.1.** Quanto aos dados de base (cfr. *supra*, ponto 6.1.), o problema não é totalmente inédito para o Tribunal Constitucional. No Acórdão n.º 420/2017, este Tribunal debruçou-se sobre a conformidade constitucional da obrigação de conservação de um dos *dados de base* pelos fornecedores de serviços de comunicações eletrónicas ou de uma rede pública de comunicações: *o nome e endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP está atribuído* (artigo 4.º, n.º 1, alínea *a)*, 2.ª parte, e artigo 4.º, n.º 2, alínea *b)*, subalínea *iii)*, da Lei n.º 32/2008). Quanto a estes, e só quanto a estes, o Tribunal Constitucional — ponderando as garantias da lei em matéria de *acesso* e *transmissão* dos dados conservados às autoridades com competência criminal — concluiu pela conformidade constitucional do regime de conservação:

*«Neste juízo é necessário ponderar, de um lado, a natureza relativamente pouco invasiva da privacidade dos dados em questão (dados de base), dizendo respeito à identidade do utilizador, e o período temporal de conservação (um ano) – após o qual os dados são destruídos (artigo 7.º, n.º 1, alínea e), da Lei n.º 32/2008), tendo em conta, por outro lado, a natureza especialmente grave dos crimes em questão e a centralidade destes dados para a condução da investigação criminal. Também é de ter em atenção o regime previsto para o acesso a estes dados, com limitação do universo de titulares de dados sujeitos à transmissão (artigo 9.º, n.º 3, da Lei n.º 32/2008), e impondo a necessidade de autorização prévia, por despacho fundamentado do juiz de*

*instrução, que deve respeitar os princípios da adequação, necessidade e proporcionalidade, a requerimento do Ministério Público ou da autoridade de polícia criminal competente (artigo 9.º, n. 1, 2 e 4, da Lei n.º 32/2008). Por esses motivos, a norma objeto do presente recurso não viola o princípio da proporcionalidade decorrente do artigo 18.º, n.º 2, da Constituição».*

Resta saber se os pressupostos de que a Constituição faz depender a restrição ao direito à reserva da intimidade da vida privada e à autodeterminação informativa — sobretudo elencados nos n.ºs 2 e 3 do artigo 18.º — se verificarão quanto aos demais dados de base elencados no artigo 4.º da Lei n.º 32/2008, de 17 de julho. E, constando a restrição de lei parlamentar, o problema jurídico central radicará na proporcionalidade da medida, importando saber se o juízo de conformidade constitucional que decorre do Acórdão n.º 420/2017 (relativo à identificação do utilizador a que está atribuído um determinado endereço de IP — o endereço numérico do computador, identificável pela sua atribuição a cada momento pelo gestor de rede ou pelo fornecedor de acesso à internet) pode ser estendido à obrigação de conservação de todos os *dados de base* elencados no artigo 4.º da Lei n.º 38/2008, pelo período temporal de um ano.

Com relevo para a apreciação deste problema, deve frisar-se que, do ponto de vista estrutural, os dados de base (que são, como se viu, *dados pessoais)* não têm todos natureza equivalente. Com efeito, a identificação de um utilizador de um *número de telefone* ou de um *endereço de protocolo IP dinâmico* é bastante distinta: o primeiro é *permanente*, esteja ou não em utilização; o segundo envolve informação da sua utilização *num determinado momento*, revelando por isso não apenas o utilizador como também a utilização da internet num determinado contexto. Razão pela qual o Tribunal Constitucional Federal Alemão (Acórdão de 17 de julho de 2020 [1 BvR 1873/13 - 1 BvR 2618/13], §§ 101 e 102) sustentou dever ser classificado como *dado de tráfego.*

Não foi esta a orientação fixada por este Tribunal, no Acórdão n.º 420/2017. Aí se concluiu que obrigação de conservar os dados relativos ao «*nome e o endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP» estava atribuído "no momento da comunicação"* constitui um dos *dados de base: «Atendendo ao enquadramento descrito, a questão de inconstitucionalidade a analisar diz respeito a apenas um dos referidos tipos de "metadados": os dados de base. Assim é, pois trata-se de "os elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respetivo serviço: interessa aqui essencialmente o número e os dados através dos quais o utilizador tem acesso ao serviço" (cfr. Acórdão n.º 486/2009, ponto 2.2)».* Razão pela qual o Tribunal Constitucional mobilizou, quanto a estes dados, a jurisprudência desenvolvida em matéria de *dados de base.*

Não parece dever mudar-se a orientação de que o regime jurídico-constitucional relevante para a apreciação da medida de conservação dos endereços de protocolo de IP dinâmicos que identificam a *fonte* da comunicação deve ser o dos *dados de base*. Na verdade, ainda que seja discutível a respetiva categorização (porquanto o apuramento do endereço de protocolo IP dinâmico pressupõe a análise do momento em que se realizou *uma concreta comunicação*), a intensidade de agressão aos direitos à reserva da intimidade da vida privada e à autodeterminação informativa é, neste domínio, similar ao dos demais dados de base. Com efeito, o apuramento da identidade do utilizador *da fonte da comunicação* a quem estava atribuído o protocolo IP *em certo momento* não revela as circunstâncias da comunicação, a sua duração, a pessoa com quem se comunica ou

os *sites* consultados; limita-se a identificar, tal como nos demais dados de base, o utilizador daquele computador.

Esta conclusão é, de resto, condicente com a orientação seguida pelo Tribunal de Justiça no Acórdão *La quadrature du net, cit.* n.º 152: «*Importa observar que os endereços IP, apesar de fazerem parte dos dados de tráfego, são gerados sem estarem ligados a uma comunicação específica e servem principalmente para identificar, por intermédio dos prestadores de serviços de comunicações eletrónicas, a pessoa singular proprietária de um equipamento terminal a partir do qual é efetuada uma comunicação através da Internet. Assim, em matéria de correio eletrónico e de telefonia através da Internet, desde que apenas sejam conservados os endereços IP da fonte da comunicação e não os do seu destinatário, esses endereços não revelam, enquanto tais, nenhuma informação sobre terceiros que tenham estado em contacto com a pessoa que está na origem da comunicação. Por conseguinte, esta categoria de dados tem um grau de sensibilidade menor que o dos outros dados de tráfego*».

**17.2.** Resta verificar se a obrigação de conservação dos *dados de base* (e, independentemente da sua classificação, dos endereços de protocolo IP dinâmicos que identificam a *fonte* de uma comunicação), enquanto medida restritiva dos direitos à reserva da intimidade da vida privada e à autodeterminação informativa, respeita o princípio da proporcionalidade.

No que toca à adequação às finalidades de interesse geral de prevenção, deteção e repressão de crimes graves, a conservação temporal daqueles dados constitui instrumento adequado à identificação do utilizador. Com efeito, apesar de atingir direitos fundamentais tão iminentes como a privacidade, a intimidade e a autodeterminação informativa (na sua dimensão de confidencialidade de dados pessoais), ela tende à proteção de valores constitucionalmente protegidos — a segurança interna, a legalidade democrática e o exercício da ação penal no combate à criminalidade —, potenciando a eficácia da atividade estadual de investigação e repressão de crimes graves. Ideia que, aliás, é consonante com o juízo do Tribunal de Justiça no Acórdão *Digital Rights Ireland* relativo à obrigação de conservação destes dados que constava da Diretiva 2006/24/CE: «*No que respeita à questão de saber se a conservação dos dados é adequada à realização do objetivo prosseguido pela Diretiva 2006/24, cumpre observar que, tendo em conta a crescente importância dos meios de comunicação eletrónica, os dados que devem ser conservados em aplicação desta diretiva permitem às autoridades nacionais competentes em matéria penal dispor de possibilidades suplementares de elucidação das infrações graves e, portanto, nesta perspetiva, constituem um instrumento útil nas investigações penais. Assim, a conservação desses dados pode ser considerada adequada à realização do objetivo prosseguido pela dita diretiva*». E que encontra, aliás, suporte direto na jurisprudência do TEDH, no Acórdão *Breyer, cit.*, §87.

Note-se que, nos termos da jurisprudência consolidada do Tribunal Constitucional, não há que garantir — no que respeita à adequação — se a medida fiscalizada é a *mais eficaz* na persecução do objetivo a que tende, mas apenas a sua vocação para as finalidades subjacentes. Tem-se entendido que uma medida é considerada idónea desde que se revele apta a atingir o seu objetivo, mesmo que o faça de forma pouco eficiente. Nestes termos, ainda que a providência de conservação dos dados de base possa não lograr o seu objetivo quando os utilizadores utilizem SIMs anónimos ou operadores situados fora da Europa através de *roaming* — preocupações reveladas pelo Tribunal Constitucional da República Checa, em *obiter dictum* (Acórdão de 22 de Março de 2001, proc. Pl. ÚS

24/10, §56) —, o subprincípio da adequação não se tem por violado se aquela medida, em abstrato, propender à identificação dos sujeitos envolvidos em crimes graves.

**17.3.** Menos evidente é o cumprimento dos demais crivos (da exigibilidade e da proporcionalidade em sentido estrito), no que respeita a saber se a medida ultrapassa o estritamente necessário para as finalidades que visa alcançar e se, ainda que assim não seja, a agressão aos direitos fundamentais protegidos é contrapesada pelos efeitos alcançados. A questão põe-se não só quanto à definição do prazo da sua conservação — que estará, também ele, sujeito à demonstração da sua *exigibilidade,* limitando-se ao estritamente necessário para os objetivos visados — como no que tange ao universo de dados abrangido pela medida de conservação.

A fixação do período temporal de conservação (um ano) pode questionar-se atendendo à circunstância de ter o legislador fixado um período geral, aplicável a todas as categorias de dados elencadas no artigo 4.º e independentemente da sua diferente natureza (cfr. n.º 64 do Acórdão *Digital Rights Ireland*). Independentemente do mérito da observação, a circunstância de a conservação das diferentes categorias de metadados reclamar um juízo de constitucionalidade independente (por consubstanciarem níveis diferentes de intensidade na agressão aos direitos fundamentais em causa), implica que, nesta sede, se cinja a apreciação à proporcionalidade da medida de conservação de *dados de base* pelo período de um ano.

Ora, no que concerne aos *dados de base,* o período de conservação de um ano não é desrazoável, não se demonstrando que a previsão de um prazo de conservação mais curto pudesse garantir similar eficácia. É crível que a investigação criminal possa necessitar de dados de identificação dos utilizadores do ano imediatamente anterior ao momento em que a informação é tida por essencial. Sobretudo, tendo em conta que a investigação dos *crimes graves* em cujo âmbito o acesso pode ser pedido é previsivelmente complexa e demorada, sendo pouco provável que imediatamente após a prática da infração criminal estejam identificados os dados cujo acesso é imprescindível à descoberta da verdade. Não se vislumbrando, de resto, qualquer meio menos lesivo que permita equivalente eficácia na realização dos objetivos a que a medida se destina. A isto acresce que o grau de agressão ao direito à intimidade da vida privada pela conservação dos *dados de base* é menos gravoso do que os demais metadados elencados no artigo 4.º da Lei n.º 32/2008, de 17 de julho (pois apenas identificam o utilizador do meio de comunicação em causa), o que é balanceado pelos efeitos positivos em matéria de ação penal.

A questão mais problemática reside no universo de sujeitos e dados abrangidos, tendo em consideração que a norma fiscalizada postula uma conservação generalizada dos dados de *todos* os utilizadores e assinantes. Ainda que não sejam conjeturáveis medidas menos intrusivas que apresentem similar eficácia, pode questionar-se se a delimitação do universo pessoal e material da obrigação de retenção (todos os dados de todos os utilizadores e assinantes) não constituirá uma solução desproporcionada por referência àquelas finalidades. Com efeito, sendo certo que a restrição da obrigação de conservação a um âmbito limitado de visados reduziria a eficácia da investigação criminal — porquanto ficariam por preservar dados que, a final, se viriam a considerar relevantes — há que saber se se verifica um equilíbrio razoável entre a eficiência acrescida decorrente da obrigação generalizada de conservação de todos os metadados de todas as

pessoas e a afetação dos direitos à reserva da intimidade da vida privada e à autodeterminação informativa.

O legislador nacional, quanto à conservação de outros dados relevantes para a investigação criminal (que são *dados pessoais* na aceção do artigo 35.º da Constituição) tomou opções distintas, não havendo estabelecido um universo indiferenciado de visados. Pense-se, por exemplo, na base de dados de perfis de ADN, em que se não determinou a conservação de todos os dados de todos os cidadãos — mas apenas de um leque circunscrito de sujeitos (voluntários, pessoas condenadas em processo criminal; arguidos em processo criminal; etc. — artigo 15.º da Lei n.º 5/2008, de 12 de fevereiro, na versão que lhe foi conferida pela Lei n.º 90/2017, de 22 de agosto). Ou, ainda, no regime estatuído pelo artigo 12.º da Lei do Cibercrime (Lei n.º 109/2009, de 15 de setembro), que plasma uma possibilidade de *quick-freeze*, admitindo que a autoridade judiciária (ou o órgão de polícia criminal, nos casos do n.º 2) requeira ao fornecedor do serviço a preservação e conservação dos dados determinados como necessários à produção da prova, a partir do momento em que é feito o pedido. Em contraste, nas normas fiscalizadas, consagrou-se uma solução que indiscutivelmente apresenta maior eficácia, abrangendo todos os dados de todos os utilizadores.

O juízo quanto à proporcionalidade da medida restritiva não é, neste domínio, desligado do Direito da União Europeia: como se viu, está-se no seu âmbito — em concreto, o disposto no n.º 1 do artigo 15.º da Diretiva 2002/58/CE — pelo que a proteção conferida pela CDFUE, tal como interpretada pelo TJUE, influirá na apreciação levada a cabo pelo Tribunal Constitucional. Ora, a resposta à questão de saber se o regime da conservação destes dados, considerados isoladamente, contraria a CDFUE foi dada pelo Tribunal de Justiça no dia 6 de outubro de 2020, no citado Acórdão *La quadrature du net*. Neste aresto, a compatibilidade com a CDFUE das medidas nacionais (francesas) de conservação de metadados pelos fornecedores de comunicações eletrónicas foram analisadas de modo distinto quanto à medida de conservação *dos endereços de protocolo IP que identificam a fonte da comunicação* e à medida de conservação dos demais *dados de tráfego e localização*. Com efeito, como *supra* se viu, independentemente da categorização dos endereços de protocolo IP dinâmicos que identificam a fonte de uma comunicação, concluiu o TJUE que as medidas nacionais que estabeleçam a sua conservação generalizada, mesmo restringindo os direitos consagrados nos artigos 7.º e 8.º da CDFUE (respeito pela vida privada e familiar; proteção de dados pessoais), deve ter-se por compatível com o direito da União Europeia, por cumprir o crivo da proporcionalidade (Acórdão *La quadrature du net, cit.*, n.º 152). Tendo em conta a mais baixa intensidade da agressão aos direitos fundamentais, e subordinando a medida da conservação ao princípio da proporcionalidade, o Tribunal de Justiça concluiu pela viabilidade, à luz do quadro jusfundamental da União Europeia, da imposição generalizada de conservação daqueles dados (endereços de protocolos de IP e demais dados de base — identidade civil dos titulares de números de telefone e de endereços de correio eletrónico) pelo período de um ano:

*«154. Ora, para efeitos da necessária ponderação dos direitos e dos interesses em causa exigida pela jurisprudência referida no n.º 130 do presente acórdão, há que ter em conta o facto de, no caso de uma infração cometida em linha, o endereço IP poder constituir o único meio de investigação que permite a identificação da pessoa à qual esse endereço estava atribuído no momento da prática dessa infração. A isto acresce o facto de a conservação dos endereços IP pelos prestadores de serviços de comunicações eletrónicas para lá do período de atribuição destes dados não se afigurar, em princípio, necessária para efeitos da*

*faturação dos serviços em causa, pelo que a deteção das infrações cometidas em linha pode, por esse motivo, como referiram vários Governos nas suas observações apresentadas ao Tribunal de Justiça, revelar-se impossível sem recurso a uma medida legislativa nos termos do artigo 15.º, n.º 1, da Diretiva 2002/58. Isto pode ocorrer, como alegaram esses Governos, com infrações particularmente graves em matéria de pornografia infantil, como a aquisição, a difusão, a transmissão ou a colocação à disposição em linha de pornografia infantil, na aceção do artigo 2.o, alínea c), da Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho (JO 2011, L 335, p. 1).*

*155. Nestas condições, embora seja verdade que uma medida legislativa que prevê a conservação dos endereços IP de todas as pessoas singulares proprietárias de um equipamento terminal a partir do qual pode ser efetuado um acesso à Internet visa pessoas que, à primeira vista, não têm uma relação, na aceção da jurisprudência referida no n.º 133 do presente acórdão, com os objetivos prosseguidos e que os internautas são titulares, conforme referido no n.º 109 do presente acórdão, do direito de esperar, por força dos artigos 7.o e 8.o da Carta, que a sua identidade não seja, em princípio, revelada, uma medida legislativa que prevê a conservação generalizada e indiferenciada apenas dos endereços IP atribuídos à fonte de uma ligação não se afigura, em princípio, contrária ao artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, desde que essa possibilidade esteja sujeita ao estrito respeito das condições materiais e processuais que devem reger a utilização desses dados.*

*156. Tendo em conta o caráter grave da ingerência nos direitos fundamentais consagrados nos artigos 7.º e 8.º da Carta que esta conservação comporta, só a luta contra a criminalidade grave e a prevenção das ameaças graves contra a segurança pública são suscetíveis, à semelhança da salvaguarda da segurança nacional, de justificar essa ingerência. Além disso, o período de conservação não pode exceder o estritamente necessário à luz do objetivo prosseguido. Por último, uma medida desta natureza deve prever requisitos e garantias estritas quanto à exploração desses dados, nomeadamente através de um rastreio das comunicações e atividades efetuadas em linha pelas pessoas em causa.*

*157. No que diz respeito, por último, aos dados relativos à identidade civil dos utilizadores dos meios de comunicações eletrónicos, estes dados não permitem, por si só, conhecer a data, a hora, a duração e os destinatários das comunicações efetuadas, nem os locais onde estas comunicações decorreram ou a frequência das mesmas com determinadas pessoas durante um determinado período, de modo que não fornecem, com exceção das coordenadas destes, tais como os seus endereços, nenhuma informação sobre as comunicações efetuadas nem, consequentemente, sobre a sua vida privada. Assim, a ingerência que comporta uma conservação destes dados não pode, em princípio, ser qualificada de grave (v., neste sentido, Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.ºs 59 e 60).*

*158. Daqui decorre que, em conformidade com o que foi referido no n.º 140 do presente acórdão, as medidas legislativas que visam o tratamento desses dados enquanto tais, nomeadamente a sua conservação e o acesso a estes apenas para efeitos da identificação do utilizador em causa, e sem que os referidos dados possam ser associados a informações relativas às comunicações efetuadas, podem ser justificadas pelo objetivo de prevenção, de investigação, de deteção e de repressão de infrações penais em geral, a que se refere o artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58 (v., neste sentido, Acórdão de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, n.º 62).*

*159. Nestas condições, tendo em conta a necessária ponderação dos direitos e interesses em causa e pelas razões que figuram nos n.ºs 131 e 158 do presente acórdão, há que considerar que, mesmo na falta de ligação*

*entre todos os utilizadores dos meios de comunicações eletrónicos e os objetivos prosseguidos, o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, não se opõe a uma medida legislativa que impõe, sem prazo específico, aos prestadores de serviços de comunicações eletrónicas a conservação de dados relativos à identidade civil de todos os utilizadores de meios de comunicações eletrónicos para efeitos de prevenção, investigação, deteção e repressão de infrações penais, assim como da salvaguarda da segurança pública, não sendo necessário que as infrações penais ou que as ameaças ou as ofensas à segurança pública sejam graves».*

Quer isto dizer que, no que respeita aos *dados de base* (e aos endereços de protocolo IP que identificam a fonte da comunicação, independentemente da sua classificação), o direito da União Europeia não põe em causa a ponderação de proporcionalidade feita pelo Tribunal Constitucional no Acórdão n.º 420/2017, sendo esta *conforme* ao parâmetro europeu, cujo sentido foi já clarificado pela jurisprudência do Tribunal de Justiça. Em consequência, concluindo-se pela bondade constitucional da conservação dos endereços do protocolo IP da fonte da comunicação — enquanto dado que pode espelhar uma agressão mais intensa no direito à intimidade da vida privada, por pressupor um tratamento do *momento do acesso à internet*, no caso dos endereços dinâmicos — por maioria de razão será igualmente conforme aos requisitos do n.º 2 do artigo 18.º a conservação de dados de base *que não pressupõem a análise de quaisquer comunicações* (números de telefone, endereços de correio eletrónico, etc.).

Para esta conclusão concorre, ainda, o facto de a transmissão destes dados às autoridades competentes para a investigação criminal ser particularmente estrita, prevendo o legislador um leque de garantias que asseguram que apenas serão acedidos em situações de estrita necessidade para a ação penal em crimes graves. Como se disse no Acórdão n.º 420/2017:

*«O princípio da proporcionalidade em sentido estrito veda a adoção de medidas que se apresentem como excessivas (desproporcionadas) para atingir os fins visados. Neste juízo é necessário ponderar, de um lado, a natureza relativamente pouco invasiva da privacidade dos dados em questão (dados de base), dizendo respeito à identidade do utilizador, e o período temporal de conservação (um ano) – após o qual os dados são destruídos (artigo 7.º, n.º 1, alínea e), da Lei n.º 32/2008), tendo em conta, por outro lado, a natureza especialmente grave dos crimes em questão e a centralidade destes dados para a condução da investigação criminal. Também é de ter em atenção o regime previsto para o acesso a estes dados, com limitação do universo de titulares de dados sujeitos à transmissão (artigo 9.º, n.º 3, da Lei n.º 32/2008), e impondo a necessidade de autorização prévia, por despacho fundamentado do juiz de instrução, que deve respeitar os princípios da adequação, necessidade e proporcionalidade, a requerimento do Ministério Público ou da autoridade de polícia criminal competente (artigo 9.º, n. 1, 2 e 4, da Lei n.º 32/2008). Por esses motivos, a norma objeto do presente recurso não viola o princípio da proporcionalidade decorrente do artigo 18.º, n.º 2, da Constituição».*

**17.4.** Este juízo de conformidade constitucional é igualmente válido quanto aos *dados de base* que conduzam à identificação de pessoas coletivas — que estão excluídos do âmbito de aplicação do RGPD (n.º 1 do artigo 1.º) e da Lei n.º 59/2019, de 8 de agosto (artigo 1.º), mas expressamente abrangidos pelas normas fiscalizadas (artigo 4.º, em conjugação com o artigo 1.º da Lei n.º 32/2008, de 17 de julho).

Desde logo, é controvertida a atribuição às pessoas coletivas dos direitos fundamentais restringidos pelas normas fiscalizadas, tendo em conta que a Constituição apenas lhes outorga os direitos *compatíveis com a sua natureza* (n.º 2 do artigo 12.º). A norma do n.º 2 do artigo 12.º da Constituição implica, como se afirmou no Acórdão do Tribunal Constitucional n.º 279/2009, que «*as pessoas coletivas não são equiparadas às pessoas singulares. Na verdade, "as pessoas coletivas só têm os direitos compatíveis com a sua natureza, ao passo que as pessoas singulares têm todos os direitos, salvo os especificamente concedidos apenas a pessoas coletivas (v.g., o direito de antena). E tem de reconhecer-se que, ainda quando certo direito fundamental seja compatível com essa natureza e, portanto, suscetível de titularidade 'coletiva' (hoc sensu), daí não se segue que a sua aplicabilidade nesse domínio vá operar exatamente nos mesmos termos e com a mesma amplitude com que decorre relativamente às pessoas singulares"*». Em consequência, a titularidade de direitos fundamentais pelas pessoas coletivas depende de um fator circunscritivo — a compatibilidade com a sua natureza —, critério que obriga a uma aferição em cada uma das posições jusfundamentais. O que implica apurar se os direitos à reserva da intimidade da vida privada e à autodeterminação informativa são compatíveis com a natureza *coletiva* da pessoa moral, de modo a determinar se tais entidades jurídicas *deles são titulares* e, nesse caso, *se têm o mesmo conteúdo e amplitude* que revestem no quadro das pessoas singulares.

No que respeita aos direitos à reserva da vida privada e ao livre desenvolvimento da personalidade (consagrados no artigo 26.º da Constituição), embora a sua raiz na dignidade *humana* pareça conduzir à conclusão da respetiva incompatibilidade com a natureza das pessoas coletivas, não se exclui que alguns dos direitos aí consagrados possam receber tutela constitucional (e, no domínio de aplicação do direito da União Europeia, proteção pela CDFUE), na medida em que não sejam inseparáveis da personalidade singular.

Simplesmente, o seu sentido tutelador não é já o da tutela da dignidade da pessoa humana, mas a prevenção de danos patrimoniais indiretos, uma vez que a razão do seu amparo se liga à sua atuação, restrita às respetivas atribuições. A esfera de sigilo das pessoas coletivas (compreendendo o sigilo de correspondência, o desenho de organização, funcionamento e *know-how*, e o «segredo de negócio») implicará uma amplitude necessariamente distinta, como o Tribunal Constitucional vem confirmando: «*a "aplicação" dos direitos fundamentais às pessoas colectivas não pode deixar de levar em conta a particular natureza destas — e de tal modo que seguramente tem de reconhecer-se que ainda quando certo direito fundamental seja compatível com essa natureza, e portanto suscetível de titularidade "coletiva" (hoc sensu), daí não se segue que a sua aplicabilidade nesse domínio se vá operar exactamente nos mesmos termos e com a mesma amplitude com que decorre relativamente às pessoas singulares*» (Acórdão n.º 198/85). Ora, este raciocínio, desenvolvido pelo Tribunal Constitucional quanto à *inviolabilidade da correspondência das pessoas coletivas*, pode estender-se às demais dimensões do direito à reserva da vida privada — sendo certo que não estará aqui a "vida familiar" mas a "vida privada da pessoa coletiva", abrangendo o *segredo de negócio.* Aliás, no quadro europeu, ainda em momento anterior à CDFUE, o Acórdão do Tribunal de Justiça de 22 de outubro de 2002, *Roquette Frères*, proc. C-94/00, declarava a existência de um «*princípio geral de direito comunitário que consagra a proteção contra as intervenções arbitrárias e desproporcionadas do poder público na esfera da atividade privada de uma pessoa singular ou coletiva*», aceitando por isso, pelo menos do ponto de vista abstrato, a titularidade desses direitos por parte de pessoas coletivas.

Também no quadro do direito à autodeterminação informativa, essencialmente contido no artigo 35.º da Constituição, se tradicionalmente se entendia que a natureza *pessoal* dos dados indica uma tutela restrita às pessoas singulares, a verdade é que Constituição não veda a atribuição do direito a pessoas coletivas, pelo menos quanto às dimensões que sejam compatíveis com a sua natureza. É esta, de resto, a posição da CNPD, que sustenta ser «*cada vez mais duvidoso que possa continuar a considerar-se como exclusivo destinatário das medidas de protecção em matéria de dados pessoais as pessoas singulares, esquecendo as pessoas colectivas*» (Parecer n.º 18/2000). Simplesmente, ainda que se admita a atribuição do direito à autodeterminação informativa a pessoas coletivas, o seu escopo é necessariamente distinto: sendo esta construída como direito-garantia de outros direitos fundamentais, a sua relevância no domínio das pessoas coletivas funcionará como tutela de não divulgação e tratamento automatizado dos seus elementos individualizadores (designadamente, modelo organizacional, o segredo de negócio e informações comerciais e industriais).

Deste modo, ainda que os direitos pessoais consagrados nos artigos 26.º e 35.º da Constituição sejam encabeçados por pessoas coletivas, eles podem ser restringidos de modo mais amplo como, no plano da tutela conferida pela CDFUE, é expressamente reconhecido pelo Tribunal de Justiça (Acórdão de 9 de novembro de 2010, *Volker e Markus Schecke*, procs. C-92/09 e C-93/09, n.º 87: «*a gravidade da violação do direito à proteção dos dados pessoais difere consoante estejam em causa pessoas singulares ou coletivas*»), pois o seu âmbito de proteção é menor. Ora, o leque de dados ora analisado (os dados de base) não é apto a revelar qualquer segredo de negócio, de laboração ou qualquer informação comercial ou industrial. Apenas está em causa a informação de que dado número de telefone, endereço de correio eletrónico ou endereço de protocolo IP está atribuído a certa pessoa coletiva quando fonte de uma comunicação. Razão pela qual, *no domínio dos dados de base,* não custa admitir que se esteja fora do domínio de aplicação do direito à autodeterminação informativa às pessoas coletivas, por não estarem em causa os direitos *ao segredo do negócio* que são indiretamente tutelados por este direito.

Esta conclusão é, aliás, conforme ao direito da União Europeia, pois o TJUE, no Acórdão *Tele2*, *cit.*, n.º 123, concluiu que a exigência de armazenamento de dados no território da União apenas se liga à proteção de dados pessoais *relativos a pessoa singulares*, excluindo expressamente os dados relativos a pessoas coletivas: «*os Estados-Membros devem garantir o controlo, por parte de uma autoridade independente, do respeito do nível de proteção garantido pelo direito da União em matéria de proteção das pessoas singulares relativamente ao tratamento dos dados pessoais*» (sublinhado aditado).

Razão pela qual a obrigação de conservação de *dados de base* (e de endereços de protocolo IP dinâmicos relativos à *fonte* de uma comunicação, independentemente da respetiva categorização) pelo período de um ano, constante da conjugação das normas dos artigos 4.º e 6.º da Lei n.º 32/2008, de 17 de julho, não seria *em si mesma* inconstitucional, se o legislador houvesse cumprido a injunção de prever o seu armazenamento no território da União Europeia.

**18.** O mesmo não pode concluir-se quanto à obrigação de conservação dos *dados de tráfego,* gerados a propósito de uma específica comunicação, com especial relevância para os *dados de localização.*

A conservação dos dados de localização, ainda que não sejam gerados em virtude de uma comunicação pessoal, materializam uma agressão mais intensa à intimidade da vida privada dos sujeitos privados do que a preservação dos dados de base, ao permitirem identificar, a todo o

tempo, a posição e os movimentos dos utilizadores. O mesmo se diga quanto aos dados de tráfego, mesmo quando não pressupõem uma comunicação (ou sua tentativa) interpessoal, como os sítios da internet consultados, por quanto tempo, em que momento e a quantidade de tráfego gerado. Estes dados permitem traçar um perfil do utilizador, identificar os seus interesses e mesmo reconhecer, em certos casos, o tipo de conteúdos consultados. Como se disse no Acórdão n.º 464/2019, «*Esta segunda categoria de dados de tráfego de internet, embora não envolva comunicação intersubjetiva, exprime vários aspetos da personalidade e do comportamento dos utilizadores, pertencendo a cada pessoa o direito de escolha quanto à partilha, ou não, destas informações com terceiros, bem como o poder de vedar o acesso de terceiros a estes dados e de controlar quem tem acesso a eles e em que momento. Por isso mesmo, estes dados de tráfego encontram-se incluídos no âmbito objetivo de proteção das normas constitucionais atinentes à reserva de intimidade da vida privada e à autodeterminação informativa, protegidas pelos artigos 26.º, n.º 1, e 35.º da CRP*».

Note-se que, se as normas em crise parecem apenas determinar a conservação de dados relativos a *comunicações*, no que respeita aos dados de tráfego «*necessários para identificar a data, a hora e a duração de uma comunicação*» (alínea *c)* do n.º 1 do artigo 4.º), determina-se a conservação de dados que são gerados pela simples utilização da internet, independentemente de qualquer comunicação intersubjetiva (alínea *b)* do n.º 4 do artigo 4.º: «*A data e a hora do início (log in) e do fim (log off) da ligação ao serviço de acesso à Internet com base em determinado fuso horário, juntamente com o endereço do protocolo IP, dinâmico ou estático, atribuído pelo fornecedor do serviço de acesso à Internet a uma comunicação*». Ora, a conservação destes dados de navegação, mesmo que não abranja os conteúdos consultados, afeta a privacidade e a proteção dos dados pessoais de modo particularmente intenso. Como se concluiu no Acórdão n.º 464/2019, «*o tratamento não consentido dos respetivos dados de tráfego põe em causa valores e interesses do utilizador, tais como (i) a confiança que tem na segurança e reserva dos sistemas informáticos do fornecedor do serviço de acesso à internet; (ii) o interesse em decidir, ele mesmo, acerca da utilização que poderá ser efetuada das suas informações pessoais; (iii) o interesse em não ser sujeito a decisões exclusivamente automatizadas dos seus dados; (iv) o interesse em conhecer, dispor, controlar, atualizar, corrigir ou apagar os dados pessoais que lhe digam respeito; (v) o interesse em conhecer a finalidade do tratamento dos seus dados (vi) o interesse na não divulgação de dados objeto de tratamento*».

O facto de a conservação destes dados materializar uma agressão mais intensa dos direitos fundamentais à intimidade da vida privada tem reflexos na proporcionalidade da restrição. Como sublinhou o Tribunal de Justiça no Acórdão *La quadrature du net* (*cit.*), n.º 131, «*decorre da jurisprudência do Tribunal de Justiça que a possibilidade de os Estados-Membros justificarem uma limitação aos direitos e às obrigações previstos, nomeadamente, nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58 deve ser apreciada através da medição da gravidade da ingerência que tal limitação implica e da verificação de que a importância do objetivo de interesse geral prosseguido por esta limitação está relacionada com essa gravidade*».

Ora, a restrição aos direitos fundamentais agredidos com esta regulamentação não obedece às exigências de proporcionalidade, desde logo por atenção ao âmbito alargado da medida. O que, de resto, coincide com a conclusão do Tribunal de Justiça — versando *apenas* sobre os dados que, entre nós, são classificados como *dados de tráfego* e *dados de localização* — sobre o carácter manifestamente excessivo da conservação generalizada destes dados quanto a todos os utilizadores e assinantes, no Acórdão *La quadrature du net*, *cit.*, n.ºs 141 a 144:

*«141. Uma regulamentação nacional que prevê a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização, com vista a lutar contra a criminalidade grave, excede os limites do estritamente necessário e não pode ser considerada justificada, numa sociedade democrática, como exige o artigo 15.º, n.º 1, da Diretiva 2002/58, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta (v., neste sentido, Acórdão de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.o 107).*

*142. Com efeito, tendo em conta o caráter sensível das informações que os dados de tráfego e os dados de localização podem fornecer, a sua confidencialidade é essencial para o direito ao respeito da vida privada. Assim, e tendo em conta, por um lado, os efeitos dissuasivos no exercício dos direitos fundamentais consagrados nos artigos 7.º e 11.º da Carta, referidos no n.º 118 do presente acórdão, que a conservação desses dados pode produzir e, por outro, a gravidade da ingerência que tal conservação implica, é necessário, numa sociedade democrática, que esta seja a exceção e não a regra, como prevê o sistema instituído pela Diretiva 2002/58, e que esses dados não possam ser objeto de uma conservação sistemática e contínua. Esta conclusão impõe-se mesmo em relação aos objetivos de luta contra a criminalidade grave e de prevenção das ameaças graves contra a segurança pública, bem como à importância que lhes deve ser reconhecida.*

*143. Além disso, o Tribunal de Justiça sublinhou que uma regulamentação que prevê a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização abrange as comunicações eletrónicas de quase toda a população sem que seja estabelecida nenhuma diferenciação, limitação ou exceção em função do objetivo prosseguido. Tal regulamentação, contrariamente à exigência recordada no n.º 133 do presente acórdão, afeta globalmente todas as pessoas que utilizam serviços de comunicações eletrónicas, sem que essas pessoas se encontrem, mesmo indiretamente, numa situação suscetível de justificar um procedimento penal. Por conseguinte, aplica-se inclusivamente a pessoas em relação às quais não haja indícios que levem a acreditar que o seu comportamento possa ter um nexo, ainda que indireto ou longínquo, com este objetivo de luta contra os atos de criminalidade grave e, em particular, sem que se estabeleça uma relação entre os dados cuja conservação se encontra prevista e uma ameaça para a segurança pública (v., neste sentido, Acórdãos de 8 de abril de 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, n.ºs 57 e 58, e de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.o 105).*

*144. Em particular, como já declarou o Tribunal de Justiça, tal regulamentação não está limitada a uma conservação que tenha por objeto dados relativos a um período temporal e/ou uma zona geográfica e/ou a um círculo de pessoas que possam estar envolvidas de alguma forma numa infração grave, nem a pessoas que, por outros motivos, mediante a conservação dos seus dados, podiam contribuir para a luta contra a criminalidade grave (v., neste sentido, Acórdãos de 8 de abril de 2014, Digital Rights, C-293/12 e C-594/12, EU:C:2014:238, n.º 59, e de 21 de dezembro de 2016, Tele2, C-203/15 e C-698/15, EU:C:2016:970, n.o 106)»*

Interpretando os direitos à reserva da intimidade da vida privada e à autodeterminação informativa à luz dos parâmetros europeus aqui convocáveis, há que reafirmar este juízo no plano constitucional. Com efeito, ainda que não se configurem medidas com a mesma eficácia do que a conservação de todos os dados de todas as pessoas, a ponderação de uma agressão tão grave com os efeitos positivos que se alcançam conduz à conclusão de que se trata de uma solução legislativa desequilibrada, por atingir sujeitos relativamente aos quais não há qualquer suspeita de atividade criminosa. Ao conservar todos os dados de localização e de tráfego de todos os assinantes, abrangem-se as comunicações eletrónicas da quase totalidade da população, sem qualquer

diferenciação, exceção ou ponderação face ao objetivo perseguido. O legislador adota aqui um âmbito muito mais alargado (seja quanto às categorias de dados, seja quanto ao âmbito subjetivo) do que o crivo que foi seguido em outros ambientes normativos — cfr. a opção legislativa em matéria de base de dados de ADN, de criminalidade informática (*quick-freeze*), a que *supra* se aludiu — abrangendo a agressão daqueles direitos fundamentais em situações que, num juízo de ponderação, não são contrapesadas pelos efeitos positivos no combate à criminalidade.

No fundo, se a medida de conservação de dados de tráfego e de localização *em si mesma* pode ser tida como adequada e necessária para os fins de interesse público que visa salvaguardar, a definição do leque de sujeitos visados só não transgride os limites da proporcionalidade na medida em que se dirija, de forma direta, às situações em que a agressão aos direitos fundamentais em causa possa ter-se por orientada à perseguição dos objetivos da ação penal. Neste quadro, por se ultrapassarem na medida fiscalizada os limites da proporcionalidade no que concerne ao respetivo âmbito subjetivo, viola-se o n.º 2 do artigo 18.º da Constituição na restrição aos direitos fundamentais à reserva da intimidade da vida privada e à autodeterminação informativa (artigos 26.º, n.º 1, e 35.º, n.º 1, da Constituição), perdendo relevância a questão de saber se os demais elementos de que dependeria a proporcionalidade da medida (o ajustamento do prazo de conservação ao estritamente necessário para os fins a alcançar; e a imposição de condições de segurança do respetivo armazenamento) são preenchidos pela regulamentação fiscalizada.

Razão pela qual deve ter-se por inconstitucional, por violação dos n.ºs 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o artigo n.º 18.º, n.º 2, da Constituição, a medida de conservação por um ano dos dados de tráfego e dos dados de localização, decorrente da conjugação do disposto do artigo 4.º com o artigo 6.º da Lei n.º 32/2008, de 17 de julho.

**19.** Resta, por fim, apreciar a conformidade constitucional da norma do artigo 9.º da Lei n.º 32/2008, de 17 de julho, relativa ao regime de acesso aos dados pelas autoridades competentes em matéria de investigação criminal.

Também neste domínio, o regime nacional de transmissão dos dados conservados às autoridades nacionais está no âmbito de aplicação do direito da União Europeia, como de resto foi expressamente determinado pelo Tribunal de Justiça no Acórdão *Tele2:*

«76. Também se enquadra no referido âmbito de aplicação uma medida legislativa que tem por objeto [...] o acesso das autoridades nacionais aos dados conservados pelos prestadores de serviços de comunicações eletrónicas.

77. Com efeito, a proteção da confidencialidade das comunicações eletrónicas e dos dados de tráfego com elas relacionados, garantida no artigo 5.º, n.º 1, da Diretiva 2002/58, aplica -se às medidas tomadas por todas as pessoas que não sejam os utilizadores, independentemente de se tratar de pessoas singulares ou de entidades privadas ou públicas. Como confirma o considerando 21 desta diretiva, esta tem como objetivo impedir «o acesso» não autorizado às comunicações, incluindo a «quaisquer dados com elas relacionados», para proteger a confidencialidade das comunicações eletrónicas.

78. Nestas condições, uma medida legislativa através da qual um Estado-Membro impõe, com fundamento no artigo 15.º, n.º 1, da Diretiva 2002/58, aos prestadores de serviços de comunicações eletrónicas, para os efeitos mencionados nesta disposição, a obrigação de conceder às autoridades

nacionais, nas condições previstas nessa medida, o acesso aos dados conservados pelos referidos prestadores tem por objeto o tratamento de dados pessoais por parte destes últimos, tratamento que se enquadra no âmbito de aplicação desta diretiva».

Ora, na interpretação do disposto no artigo 15.º da Diretiva 2002/58/CE, à luz do estatuído nos artigos 7.º, 8.º e 52.º da CDFUE, o Tribunal de Justiça, no Acórdão *Tele2,* concluiu que a conformidade do regime de acesso aos dados pelas autoridades públicas com os direitos garantidos pela CDFUE depende, essencialmente, de três condições: estar limitado ao estritamente necessário para a prevenção, investigação, deteção e repressão de *criminalidade grave* (n.ºs 115 a 119); depender de um controlo judicial ou de entidade administrativa independente (n.º 120); ser comunicado o acesso às pessoas abrangidas, a partir do momento em que essa comunicação não seja suscetível de comprometer as investigações criminais (n.º 121). Requisitos que, aliás, condizem com a jurisprudência do Tribunal Europeu dos Direitos do Homem (TEDH), como se deu conta no Acórdão n.º 403/2015:
«um processo de acesso a dados, porque não sujeito ao escrutínio dos indivíduos visados, tem de ser compensado por uma lei suficientemente tuteladora dos direitos fundamentais (Acórdão de 06/06/2006, *Segerstedt-Wiberg e outros c. Suécia*, queixa n.º 62332/2000); que essa lei deve empregar termos suficientemente claros para possibilitar a todos os cidadãos terem conhecimento das circunstâncias e dos requisitos que permitem ao poder público fazer uso de uma medida secreta que lesa o direito à vida privada pessoal e familiar e à correspondência (Acórdão de 02/08/1984, *Malone c. Reino Unido*, queixa n.º 8691/79); que seria contrária às exigências do artigo 8.º, n.º 2, da CEDH se a ingerência nas telecomunicações fosse conferida aos poderes públicos através de um poder amplo e discricionário, e que são necessárias regras claras e detalhadas, especialmente devido ao facto de a tecnologia disponível se tornar cada vez mais sofisticada, a fim de garantir uma proteção adequada contra ingerências arbitrárias (Acórdão de 16/02/2000, *Amann c. Suíça*, queixa n.º 27798/95); e nos casos *Valenzuela c. Espanha* (Acórdão de 30/07/1998, queixa n.º 27671/95) e *Prado Bugallo c. Espanha* (Acórdão de 18/02/2003, queixa n.º 58496/00), chegou à mesma conclusão, afirmando que a lei que permitia a ingerência nas comunicações não era suficientemente clara e precisa, não mencionando a natureza das infrações que podem dar lugar às mesmas, a fixação de um limite de duração da medida, as condições de acesso aos dados e a eliminação dos mesmos».

Aliás, o TEDH pronunciou-se especificamente sobre o regime de interceção e acesso a dados de tráfego no Acórdão *Big Brother Watch, cit.*, considerando tais medidas como uma interferência na vida privada das pessoas e, por isso, fixando pressupostos para a respetiva compatibilidade com o artigo 8.º da CEDH, como este Tribunal deu nota no Acórdão 464/2019:
«Relativamente à aquisição de dados previamente armazenados, o TEDH, no caso *Big Brother Watch*, estabelece os seguintes critérios de conformidade destas medidas ao artigo 8.º da CEDH (§§464 a 467): (1) o regime deve estar de acordo com a lei, no sentido de esta ser clara, acessível e de efeitos previsíveis para os cidadãos; (2) deve prosseguir um objetivo legítimo, (3) e ser necessário numa sociedade democrática, restringindo-se ao combate à criminalidade grave; (4) o

acesso deve estar sujeito a uma autorização prévia decidida por um tribunal ou por uma entidade administrativa independente; (5) a lei deve providenciar garantias adequadas contra a arbitrariedade».

Ora, de acordo com a requerente (artigo 31.º do pedido), o regime de acesso aos dados armazenados pelas autoridades de investigação criminal obedece aos parâmetros desvelados pelo Tribunal de Justiça da CDFUE em sede de definição subjetiva e objetiva das circunstâncias em que pode a medida ser decretada. Todavia, não se prevê na Lei n.º 32/2008 a notificação aos sujeitos visados de que os dados relativos às suas comunicações foram transmitidos às autoridades públicas; condição expressamente enunciada como necessária para que se conclua pela compatibilidade com o artigo 15.º da Diretiva n.º 2002/52/CE, de acordo com o n.º 121 do citado Acórdão *Tele2: «importa que as autoridades nacionais competentes às quais foi concedido o acesso aos dados conservados informem desse facto as pessoas em causa, no âmbito dos processos nacionais aplicáveis, a partir do momento em que essa comunicação não seja suscetível comprometer as investigações levadas a cabo por essas autoridades. Com efeito, essa informação é, de facto, necessária para permitir que essas pessoas exerçam, nomeadamente, o direito de recurso, explicitamente previsto no artigo 15.º, n.º 2, da Diretiva 2002/58, lido em conjugação com o artigo 22.º da Diretiva 95/46, em caso de violação dos seus direitos (v., por analogia, acórdãos de 7 de maio de 2009, Rijkeboer, C-553/07, EU:C:2009:293, n.º 52, e de 6 de outubro de 2015, Schrems, C-362/14, EU:C:2015:650, n.º 95)».*

A inexistência da notificação aos visados de que os seus dados foram acedidos pelos órgãos competentes pela investigação criminal (uma vez terminado o processo em que tal tenha ocorrido) impedirá que estes possam exercer um controlo jurisdicional da legalidade daquela transmissão. O que é configurado como uma violação do direito de acesso à via judiciária efetiva, uma vez que se impede, na prática, o exercício de ação judicial contra eventuais arbitrariedades ou abusos naquele acesso: servindo a tutela jurisdicional efetiva para a salvaguarda dos direitos fundamentais, a impossibilidade da sua defesa materializará uma violação do direito à tutela jurisdicional efetiva.

**19.1.** Ainda que assim seja, duas notas prévias devem sublinhar-se.

Em primeiro lugar, a eventual lesão do direito à tutela jurisdicional efetiva depende do reconhecimento de um direito ou interesse legalmente protegido (o direito de os sujeitos visados controlarem a transmissão dos dados às autoridades de investigação criminal) para cuja proteção a via judiciária deve dar resposta. E se tal direito for atribuído pela Constituição, os parâmetros constitucionais relevantes serão não apenas o feixe de posições jurídicas consagradas no artigo 20.º, mas também a pretensão substantiva constitucionalmente outorgada. A tal não obsta o princípio do pedido, que não vincula o Tribunal Constitucional quanto ao fundamento da inconstitucionalidade (n.º 5 do artigo 51.º da LTC) — nada impedindo que a norma do artigo 9.º da Lei n.º 32/2008, de 17 de julho, na medida em que não prevê *«em momento algum desse procedimento, a necessidade de informar o interessado (a pessoa a que se referem os dados que foram transmitidos) quanto à existência mesma do procedimento»*, possa ver a constitucionalidade declarada à luz de normas ou princípios constitucionais diferentes daqueles que a requerente indicou.

Ora, como *supra* se viu, o direito à autodeterminação informativa, consagrado no artigo 35.º da Constituição, abrange a faculdade de controlo efetivo, pelo titular, dos dados pessoais tratados.

Assim, a eventual inoperância de mecanismos de fiscalização da utilização conferida aos dados conservados — a dificultando o controlo pelo titular — materializará também uma compressão do direito à autodeterminação informativa.

Em segundo lugar, olhando o ordenamento jurídico no seu todo, não pode concluir-se pela *inexistência* de mecanismos que permitam ao visado conhecer os termos do acesso das autoridades de investigação criminal aos seus dados e, se necessário, reagir judicialmente.

Desde logo, o RGPD expressamente prevê o direito de o titular obter dos fornecedores de comunicações eletrónicas a informação de que os seus dados foram objeto de tratamento, no n.º 1 do artigo 15.º: «*o titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações: (…) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais*».

A isto acresce que o legislador pátrio, em transposição da Diretiva (UE) 2016/680, previu expedientes que permitem aos visados conhecer as medidas de transmissão, podendo desse modo exercer o controlo da respetiva legalidade. Com efeito, a Lei n.º 59/2019, de 8 de agosto, determina que o responsável pelo armazenamento dos dados é obrigado a facultar ao titular dos dados pessoais retidos, a seu pedido, informações sobre a sua transmissão (artigo 13.º e alínea *c)* do n.º 2 do artigo 15.º), bem como a apresentar queixa à autoridade de controlo de eventuais violações do regime jurídico (alínea *f)* do n.º 2 do artigo 15.º da Lei n.º 59/2019, de 8 de agosto). O que explica, aliás, a obrigação de os fornecedores de serviços de comunicações eletrónicas elaborarem «*registos da extração dos dados transmitidos às autoridades competentes e enviá-los trimestralmente à CNPD*» (n.º 5 do artigo 9.º da Lei n.º 32/2008, de 17 de julho). Em conformidade, a informação de que os dados foram transmitidos só pode ser recusada para evitar prejuízos para investigações criminais, execução de sanções penais, proteção da segurança pública ou proteção de direitos, liberdades e garantias de terceiros (n.º 1 do artigo 16.º da Lei n.º 59/2019, de 8 de agosto), caso em que a rejeição da prestação dessa informação é judicialmente controlável, mediante ação judicial especialmente prevista e de cuja existência é o visado informado (n.º 2 do artigo 16.º e artigo 18.º, todos da Lei n.º 59/2019, de 8 de agosto).

Nessa medida, o ordenamento vigente atribui ao titular dos dados o direito a *conhecer* que estes foram transmitidos às autoridades de investigação criminal quando essa informação não seja já necessária às investigações criminais em curso. Prevendo-se mecanismos judiciais (artigo 18.º, n.º 3 da Lei n.º 59/2019, de 8 de agosto) e administrativos (artigo 18.º, n.º 2 da Lei n.º 59/2019, de 8 de agosto) de controlo de eventuais recusas dessa transmissão.

**19.2.** É neste contexto que deve analisar-se se a ausência de uma *notificação ao visado* de que os seus dados foram acedidos comprime, de forma desproporcionada, os direitos à autodeterminação informativa (nas suas dimensões de *faculdade de conhecer que os seus dados foram tratados e difundidos a terceiros;* e de *exercer um controlo efetivo* sobre os dados pessoais) e a uma tutela jurisdicional efetiva. Sendo certo que, por se estar no âmbito de aplicação do direito da União Europeia, o juízo de proporcionalidade da restrição não pode desligar-se daquele que, no domínio comunitário, parametriza as restrições aos direitos garantidos pelos artigos 7.º e 8.º da CDFUE.

O sistema vigente permite ao titular dos dados *indagar* se houve acessos pelas autoridades competentes para a ação penal, passando para o interessado a responsabilidade de pesquisar — de *motu proprio* e independentemente de qualquer notícia de que tenha sido investigado pela prática de crimes graves — a informação sobre a transmissão dos metadados. Dito de outro modo, o controlo efetivo do indivíduo sobre a transmissão dos dados ocorrerá apenas quando o sujeito visado tiver uma intuição ou pressentimento de que possa ter sido investigado, cabendo-lhe então solicitar aos fornecedores de comunicações um esclarecimento sobre a ocorrência de um acesso das autoridades de investigação criminal aos dados pessoais.

Ora, ainda que se permita *uma possibilidade de conhecimento*, certo é que, do ponto de vista pragmático, este figurino é menos eficaz do que se o visado fosse notificado que as entidades competentes para a ação penal conheceram os dados armazenados — criando-lhe, desse modo, condições efetivas para não só *saber* da difusão dos seus dados como de *exercer um controlo* sobre a licitude e regularidade daquele acesso. Assim não sendo, o escrutínio efetivo da transmissão de dados dependerá de um ónus de, periodicamente, o indivíduo se interessar pela questão de saber se tais informações foram acedidas.

Em consequência, um regime jurídico como aquele que é fiscalizado é menos infalível na prevenção de abusos ou acessos indevidos aos dados armazenados, por comparação com um sistema que informasse o visado de que aquela intromissão existiu. E, sobretudo, limita de forma bastante maior o *conhecimento efetivo* da difusão de dados pessoais a terceiros: a generalidade dos cidadãos não utilizará a faculdade de pedir ao fornecedor de comunicações eletrónicas a informação sobre a transmissão dos dados (artigo 15.º da Lei n.º 59/2019, de 8 de agosto), pelo que a grande maioria dos acessos aos dados pelos órgãos de investigação criminal ocorrerá sem que o visado possa alguma vez dela aperceber-se. Como sustenta a requerente no artigo 94.º do pedido, «*o facto de se não prever, em momento algum desse procedimento, a necessidade de informar o interessado (a pessoa a que se referem os dados que foram transmitidos) quanto à existência mesma do procedimento, faz com que tal existência se tome imperceptível aos olhos de quem por ela é afectado. Nestas circunstâncias, comprometidas ficam, 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 reacção e defesa contra eventuais acessos ilegítimos a essa mesma informação*».

Neste quadro, o direito à autodeterminação informativa — na sua dimensão de garantia de controlo efetivo dos dados pessoais — está a ser objeto, pela norma em crise, de uma limitação. Restando saber se obedece aos requisitos de proporcionalidade que decorrem do artigo 18.º da Constituição.

Assim não é. Desde logo, porque ainda que o visado não esteja desprotegido (estando ao seu alcance o poder de questionar, de *motu proprio*, se ocorreu o acesso aos seus dados por terceiros, no âmbito da deteção, investigação ou repressão de crimes graves) não se descobre qualquer motivo constitucionalmente relevante que legitime a inexistência de uma notificação ao titular dos dados, *uma vez concluindo-se pela sua desnecessidade para o processo penal*, de que eles foram transmitidos às autoridades de investigação criminal.

Mas ainda que a medida se revelasse adequada à proteção de outro valor constitucionalmente relevante, certo é que a restrição ao direito de controlo dos dados pessoais não é *necessária*, por existirem alternativas mais tuteladoras do direito à autodeterminação informativa que deixariam

intocadas os eventuais efeitos positivos da medida. Com efeito, a *notificação ao visado* de que tal transmissão ocorreu — a partir do momento em que tal comunicação não seja já suscetível de comprometer as investigações ou de constituir risco para a integridade física ou vida de terceiros — constituiria opção menos restritiva, sem que se vislumbre qualquer redução de eficácia face aos expedientes vigentes. Ora, a viabilidade de alternativas menos limitativas e similarmente eficazes ao direito de controlo sobre os dados pessoais conduz, inelutavelmente, à conclusão pela *desnecessidade* ou *inexigibilidade* da restrição.

Note-se que não parece ser determinante que o procedimento de transmissão de dados dependa de um controlo do juiz de instrução (número 1 do artigo 9.º da Lei n.º 32/2008) — artigo 95.º do pedido. Essa garantia reduz, é certo, os riscos de arbitrariedade no acesso de terceiros a dados pessoais; mas nada acrescenta no exercício do direito fundamental que aqui se restringe: o direito de ser o *titular dos dados* a conhecer o tratamento que lhes é dado e a poder controlar a respetiva utilização.

Esta conclusão é ainda suportada pelo facto de, estando-se no domínio de aplicação do direito da União Europeia, o juízo de proporcionalidade na restrição não se desligar daquele que decorre do parâmetro europeu, sendo a jurisprudência do Tribunal de Justiça particularmente inequívoca (Acórdão *Tele2*, *cit.*, n.º 121): «*importa que as autoridades nacionais competentes às quais foi concedido o acesso aos dados conservados informem desse facto as pessoas em causa, no âmbito dos processos nacionais aplicáveis, a partir do momento em que essa comunicação não seja suscetível comprometer as investigações levadas a cabo por essas autoridades. Com efeito, essa informação é, de facto, necessária para permitir que essas pessoas exerçam, nomeadamente, o direito de recurso, explicitamente previsto no artigo 15.º, n.º 2, da Diretiva 2002/58, lido em conjugação com o artigo 22.º da Diretiva 95/46, em caso de violação dos seus direitos*» (sublinhado aditado).

Ao não se prever tal notificação restringe-se de modo desproporcionado o direito à autodeterminação informativa, consagrado no artigo 35.º, n.º 1, da Constituição (na dimensão de controlo do acesso de terceiros a dados pessoais) afetando, igualmente, o direito a uma tutela jurisdicional efetiva (artigo 20.º, n.º 1, da Constituição), por prejudicar a viabilidade prática de exercício de controlo judicial de acessos abusivos ou ilícitos aos dados conservados.

**III. DECISÃO**

Pelos fundamentos expostos, o Tribunal Constitucional decide:

*a)* Declarar a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4.º da Lei n.º 32/2008, de 17 de julho, conjugada com o artigo 6.º da mesma lei, por violação do disposto nos números 1 e 4 do artigo 35.º e do n.º 1 do artigo 26.º, em conjugação com o n.º 2 do artigo n.º 18.º, todos da Constituição;

*b)* Declarar a inconstitucionalidade, com força obrigatória geral, da norma do artigo 9.º da Lei n.º 32/2008, de 17 de julho, relativa à transmissão de dados armazenados às autoridades competentes para investigação, deteção e repressão de crimes graves, na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros, por violação do

disposto no n.º 1 do artigo 35.º e do n.º 1 do artigo 20.º, em conjugação com o n.º 2 do artigo 18.º, todos da Constituição.

Lisboa, 19 de abril de 2022 – *Afonso Patrão* (Subscrevendo Declaração de voto Conjunta) - *José João Abrantes* (Subscrevo Declaração de Voto Conjunta) – *José Teles Pereira* (subscrevo Declaração de Voto conjunta) - *José Eduardo Figueiredo Dias - Pedro Machete* (Pedro Machete (Subscrevo declaração de voto conjunta.

Quanto à alínea a) do dispositivo, penso que na lógica argumentativa do presente acórdão - da qual todavia me afasto nos termos e pelos fundamentos da citada declaração -, continuando a seguir a jurisprudência dos Acórdãos n.ºs 403/2015 e 463/2019, os números 1 e 4 do artigo 34 da Constituição também deveria ser mobilizado como parâmetro do juízo de inconstitucionalidade) - *Assunção Raimundo* (Subscrevo a declaração de Voto Conjunta) – *Joana Fernandes Costa* (subscrevo declaração de voto conjunta) – *Gonçalo de Almeida Ribeiro* (subscrevo declaração de voto conjunta) – *Lino Rodrigues Ribeiro* (Vencido de acordo com declaração junta) – *João Pedro Caupers* (Subscrevo a declaração de voto conjunta).

Atesto o voto de conformidade da Senhora Conselheira *Mariana Canotilho* (que subscreve declaração de voto conjunta) e do Senhor Conselheiro *António Ascensão Ramos*, que participaram na sessão por videoconferência.
*Afonso Patrão*

**DECLARAÇÃO DE VOTO CONJUNTA**

Subscrevemos integralmente a decisão. No entanto, e tal como sustentou a requerente, consideramos que as normas dos artigos 4.º e 6.º da Lei n.º 32/2008, 17 de julho, materializam também uma restrição desproporcionada do direito à inviolabilidade das comunicações, consagrado nos n.ºs 1 e 4 do artigo 34.º da Constituição, ao determinarem a conservação generalizada dos dados de tráfego gerados pelas comunicações entre pessoas (ou sua tentativa).

A garantia de inviolabilidade das comunicações, que vincula as entidades privadas (cfr. Acórdão n.º 464/2019), dirige-se à proteção de uma esfera de privacidade e de sigilo no específico domínio das comunicações interpessoais. A Constituição consagra uma garantia constitucional autónoma face àquela que já decorreria do n.º 1 do artigo 26.º da Constituição; uma *defesa constitucional independente quanto à proteção das comunicações*, com um regime de inviolabilidade mais intenso e cujas exceções são constitucionalmente determinadas. E que abrange não apenas o *conteúdo* da comunicação como os dados de tráfego gerados a seu propósito (Acórdão n.º 403/2015).

Nessa medida, ainda que se considerasse que a agressão ao direito à inviolabilidade das comunicações pudesse ser incluída no âmbito da «*matéria de processo criminal*», tendo especialmente em conta que se procede a uma ingerência nas comunicações entre pessoas que não estão, sequer remotamente, ligadas a qualquer processo criminal, consideramos que deveria ter sido mobilizado

como parâmetro do juízo positivo de inconstitucionalidade o direito consagrado nos n.ºs 1 e 4 do artigo 34.º da Constituição.

*Afonso Patrão – José João Abrantes - Assunção Raimundo -*

Atestando também a subscrição da Declaração pela Senhora Conselheira *Mariana Canotilho*.
*Afonso Patrão*

**DECLARAÇÃO DE VOTO**

**[apresentada conjuntamente pelos Conselheiros José António Teles Pereira, Maria Benedita Urbano, Pedro Machete, Joana Fernandes Costa, Gonçalo de Almeida Ribeiro e João Pedro Caupers]**

**1.** Concordando com a declaração de inconstitucionalidade com força obrigatória geral das normas indicadas no pedido – os artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de julho –, entendemos que nos parâmetros constitucionais desse juízo teria de constar – adicionalmente aos artigos 35.º, n.ºs 1 e 4, 26.º, nº 1, e 20.º, n.º 1, em conjugação com o artigo 18.º, n.º 2, da CRP – o artigo 8.º, n.º 4 da CRP, referido ao seu segmento inicial. A inclusão deste parâmetro, dando conteúdo à necessária projeção do Direito da União Europeia (DUE) na apreciação da questão colocada, assinala que a aplicação deste – *nos termos por ele próprio definidos* – é neste caso determinante do percurso conducente à decisão. Aliás, na fundamentação do pedido, foi esse o caminho que a Requerente, a título principal, indicou (pontos 44 a 46 do requerimento[1]), sendo de natureza assumidamente *subsidiária* a referência subsequente a um controlo "[…] *à luz de parâmetros exclusivamente decorrentes do texto da Constituição da República*" (ponto 47 do requerimento).

Por outro lado, a definição dos termos em que o DUE condiciona o juízo de inconstitucionalidade, corresponde a um outro ponto de afastamento dos subscritores da presente declaração da fundamentação do Acórdão. Referimo-nos concretamente ao recurso, no processo de construção da decisão, *ao princípio da interpretação conforme ao Direito da União*.

São estas divergências que explicitaremos nos subsequentes pontos da presente declaração.

**1.1.** Desde logo o Acórdão parte de um equívoco, qual seja, o de que os tribunais ordinários e o Tribunal Constitucional são chamados a apreciar e decidir questões distintas: os tribunais ordinários a apreciar uma questão de desaplicação do direito nacional que contraria regras de DUE; o Tribunal Constitucional uma questão de validade – e não de mera desaplicação – de normas nacionais que, de igual modo, contrariam regras de DUE.

Na realidade, o problema é o mesmo – qual seja, o da necessidade de dar solução a situações de contrariedade de regras de DUE por parte de normas de Direito nacional. A forma de o decidir é que é distinta, devendo ter-se em consideração as diferentes competências atribuídas pela Constituição aos tribunais ordinários e ao Tribunal Constitucional.

Partindo de uma dicotomia desaplicação/invalidação das normas, chega-se, no Acórdão, à seguinte conclusão. No caso dos tribunais ordinários, os mesmos deverão desaplicar as normas internas com base no princípio do primado das regras de DUE – tal como são por eles desaplicadas as normas julgadas inconstitucionais em sede de controlo concreto. No caso do Tribunal Constitucional, o problema da contrariedade surge no âmbito de um controlo abstrato de constitucionalidade, *sendo de assinalar que a referida dicotomia deixa por explicar todo o vasto domínio da fiscalização concreta – em que se aprecia a validade constitucional de uma norma, mas o efeito do juízo positivo de inconstitucionalidade é a sua desaplicação no caso concreto.* Ora, no controlo de tipo abstrato, a contrariedade de uma norma com a Constituição gera a invalidade da norma, e a mesma invalidade deve ser mobilizada para os casos de contrariedade da norma interna com o DUE. Sucede que isto cria alguns escolhos em termos do controlo a efetuar, designadamente, por se entender que as normas de Direito Europeu não podem constituir ou servir de parâmetro de inconstitucionalidade, o qual será sempre e unicamente a própria Constituição ("*O juízo de inconstitucionalidade – e, assim, de invalidade da norma nacional – depende da desconformidade das normas fiscalizadas com o seu parâmetro hierarquicamente superior – maxime, a Constituição*"). Ao invés, porém, de defender a invalidade das normas internas por força da violação da primeira parte do n.º 4 do artigo 8.º da CRP, mais concretamente, das obrigações às quais Portugal ficou adstrito por conta da sua adesão às, então, Comunidades Europeias, na fundamentação do Acórdão optou-se por sustentar a invalidade das normas internas recorrendo ao *princípio da interpretação conforme* (com o DUE). Especificando, aí se afirma que as normas internas são inválidas por violação de direitos fundamentais consagrados na Constituição da República, designadamente por serem os mesmos restringidos de forma desproporcionada pelas normas impugnadas, direitos e princípio da proporcionalidade interpretados em conformidade com o DUE.

Este tipo de raciocínio seguido no Acórdão – os tribunais ordinários desaplicam a norma interna convocando o princípio do primado do Direito Europeu e o Tribunal Constitucional invalida a norma interna recorrendo ao princípio da interpretação conforme – suscita-nos as maiores dúvidas. Dúvidas essas que têm que ver essencialmente, como adiante melhor se explicitará, com a utilização da figura da interpretação conforme com um sentido que não corresponde à lógica que lhe é própria. Na verdade, a aplicação da interpretação conforme consubstancia uma forma de suprir a falta de um efeito direto de certas normas de Direito Europeu através da produção de um efeito útil.

Num outro plano, pode afirmar-se que a interpretação conforme com o Direito Europeu constitui um poder-dever do juiz ordinário. Sinteticamente, a interpretação conforme é uma prática conciliatória que impõe ao juiz nacional a resolução, *in casu*, de uma contradição entre normas internas e normas de Direito Europeu pela via hermenêutica. O que encontra justificação na primazia do Direito Europeu, nos seguintes termos: se não for possível tornar operativa a interpretação conforme de uma norma interna – porque nenhum dos seus sentidos possíveis está

conforme com o DUE –, essa norma deve ser desaplicada ou invalidada. Com o recurso à interpretação conforme, na medida em que se mostre operativa, não se chega a conhecer o problema da desconformidade das normas internas com o DUE. Admitindo-se a utilização da interpretação conforme pelo Tribunal Constitucional, a mesma, tendo em consideração a sua lógica própria, servirá necessariamente para salvar uma norma interna da sua inconstitucionalidade e não, como se faz no presente acórdão, para a fundar.

**1.2.** Discordamos, assim, da construção através da qual o Tribunal caracteriza a incidência do DUE, como condicionante do juízo de inconstitucionalidade, lançando mão do *princípio da interpretação conforme ao Direito da União Europeia*. Com efeito, diversamente da lógica que presidiu à redação do Acórdão, entendemos resultar da conjugação dos artigos 7.º, n.º 6 e 8.º, n.º 4 da CRP, no quadro do DUE (por força *do princípio da cooperação leal*, na sua vertente negativa, decorrente do artigo 4.º, n.º 3, 3.º parágrafo, do TUE) e da jurisprudência do Tribunal Constitucional sobre a interação das duas ordens jurídicas (designadamente do Acórdão n.º 422/2020), que este Tribunal deveria ter assumido (integrando como condicionante), no *iter* conducente ao juízo de inconstitucionalidade, o que qualificamos como o *standard europeu* de controlo de proporcionalidade (referido às situações nacionais, designadamente as decorrentes da Diretiva 2006/24/CE[2], indutoras de uma *situação de conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização relativos às comunicações eletrónicas*). Tal *standard* foi fixado pelo Tribunal de Justiça da União Europeia (TJ), em 8 de abril de 2014, no Acórdão *Digital Rights* (processos C-293/12 e C-594/12)[3], que declarou inválida a Diretiva 2006/24/CE – tenha-se presente que essa invalidação, suprimindo a fonte de DUE transposta pela Lei n.º 32/2008, fez desaparecer as disposições determinantes, no seio do DUE, do exato conteúdo das normas nacionais que o Tribunal considerou inconstitucionais. É esta a solução que resulta da primeira parte do n.º 4 do artigo 8.º da CRP ("[*a*]*s disposições dos Tratados que regem a União Europeia e as normas emanadas das suas instituições, no exercício das respetivas competências, são aplicáveis na ordem interna, nos termos definidos pelo Direito da União* […]"), no sentido em que tem de valer para normas de Direito nacional tão estreitamente conexionadas com normas de DUE – porque diretamente determinadas por estas, como *obrigação de resultado* (artigo 288.º, terceiro parágrafo, do TFUE) – o controlo, funcionalmente equivalente ao nacional, efetuado pelo TJ relativamente a essas normas de DUE, com base em valores paramétricos materialmente equivalentes aos que estão em causa na Constituição da República.

Entendemos que esta asserção é a que descreve adequadamente a teleologia do trecho inicial do referido n.º 4 do artigo 8.º, que aqui se aplica, e sublinhamos que a mesma está implícita no Acórdão n.º 422/2020. A circunstância de na presente situação estar em causa o exercício do controlo da constitucionalidade do Direito nacional, e não do DUE (como sucedia no Acórdão n.º 422/2020), não torna imprestável, neste contexto, a fundamentação constante desse aresto. Este, com efeito, interpretou e definiu o n.º 4 do artigo 8.º da CRP, nos dois espaços de alcance da jurisdição constitucional que nele coexistem, sendo que aqui releva, decididamente, o sentido que o Tribunal Constitucional fixou ao segmento inicial da norma, que nos permite deduzir, integrando os termos específicos do Direito da União, o caminho para a adequada abordagem do pedido, com base no princípio da cooperação leal – aliás, coisa diversa não resulta da fundamentação do presente Acórdão, ao recorrer, como pressuposto decisório, a um instituto próprio do DUE.

**2.** A questão do parâmetro (a ausência no dispositivo da referência ao artigo 8.º, n.º 4, da CRP) reflete, pois, uma discordância de fundo quanto ao percurso argumentativo seguido nos itens 8.2. a 9.2. do Acórdão, onde a "*relevância do direito europeu para o pedido formulado*" é reconduzida a uma muito particular leitura do *princípio da interpretação conforme ao Direito da União Europeia*, arvorando-o, como antes dissemos, à categoria de chave de interpretação dos parâmetros constitucionais nacionais – numa leitura particularmente radical da projeção paramétrica do DUE na ordem constitucional nacional – conferindo ao princípio da interpretação conforme uma aptidão geral, ampla ao ponto de gerar juízos de invalidade total de normas – como aqui sucedeu – e não, como seria apropriado ao sentido de uma interpretação conforme, juízos de validação de determinadas dimensões interpretativas por referência a valores paramétricos pretendidos projetar nessas normas.

De facto, contrariamente ao que se depreende de diversos passos da fundamentação do Acórdão, a aplicação neste caso do princípio da interpretação conforme ao DUE, como justificativo dessa invalidade (total) das normas nacionais, desvirtua a própria ideia de *interpretação conforme* – de qualquer operação de interpretação conforme –, que se dirige à conservação de uma norma "problemática", posicionando-se como meio de evitar um juízo de invalidade desta. É paradoxal, pois, que o Tribunal, na fundamentação adotada, recorra a esse "mecanismo" destinado ao aproveitamento de algo (uma norma em determinada interpretação) para, na realidade, nada aproveitar. Veja-se que toda e qualquer dimensão interpretativa, passível de ser configurada quanto às normas objeto do pedido, é inviabilizada pela supressão pura e simples destas, através da declaração de inconstitucionalidade com força obrigatória geral, à qual não foi acrescentada – admitindo, apenas *pro argumento*, que o pudesse ser – qualquer condicionante interpretativa.

Assistimos, pois, a um uso desviado do princípio da interpretação conforme ao DUE na sua finalidade precípua: a "[…] *procura de um sentido que resgate a norma interna do destino da desaplicação* […]", através da incorporação nesta do valor que o DUE expresse, por via de uma construção interpretativa que a norma – desde logo a sua letra –, seja apta a suportar. É que, esbarrando a interpretação conforme "[…] *no limite da contradição literal ou da oposição entre regimes jurídicos*", cessa o seu fundamento[4]. Ademais, o recurso à interpretação conforme, que está teleologicamente direcionada à garantia de uma plena efetividade do DUE, justifica-se – mas só se justifica –, no quadro da tipologia dos *atos jurídicos da União*, em situações de ausência de *efeito direto*, decorrente da particular natureza da concreta fonte de DUE.

Todas estas asserções estão consolidadas na jurisprudência do TJ. Com efeito, para referir o exemplo mais recente que encontrámos, contendo uma caracterização geral do princípio da interpretação conforme, transcrevemos as seguintes passagens do Acórdão *ZX*, de 21 de outubro de 2021 (processo C-282/20):

"[…]

*39. Tendo em conta as interrogações suscitadas pelo tribunal de reenvio relativas à questão de saber se o direito da União impõe ou a interpretação conforme do direito nacional ou que fique inaplicada a disposição* [deste] […], *importa recordar que, a fim de garantir a efetividade de todas as disposições do direito da União, o princípio do primado deste direito impõe, nomeadamente, aos órgãos jurisdicionais*

*nacionais que, tanto quanto possível, interpretem o seu direito interno em conformidade com o direito da União (v., neste sentido, Acórdão de 24 de junho de 2019, Popławski, C-573/17, EU:C:2019:530, n.º 57).*

*40. Só quando é impossível proceder a uma interpretação da regulamentação nacional conforme com as exigências do direito da União é que o juiz nacional encarregado de aplicar as disposições do direito da União tem a obrigação de assegurar o seu pleno efeito deixando inaplicada se necessário, pela sua própria autoridade, toda e qualquer disposição contrária da legislação nacional, mesmo posterior, sem ter de requerer ou esperar pela sua eliminação prévia pela via legislativa ou por qualquer outro procedimento constitucional (v., neste sentido, Acórdão de 24 de junho de 2019, Popławski, C-573/17, EU:C:2019:530, n.º 58 e jurisprudência referida).*

*41. Assim, em caso de impossibilidade de interpretação conforme, qualquer juiz nacional, chamado a pronunciar-se no quadro da sua competência, tem, como órgão de um Estado-Membro, a obrigação de deixar inaplicada qualquer disposição nacional contrária a uma disposição do direito da União que tenha efeito direto no litígio que tem de decidir (v., neste sentido, Acórdão de 24 de junho de 2019, Popławski, C-573/17, EU:C:2019:530, n.º 61 e jurisprudência referida). A este respeito, o Tribunal de Justiça já declarou que o artigo 6.º, n.º 3, da Diretiva 2012/13* [a disposição de DUE em causa no processo] *deve ser considerado como tendo esse efeito direto (v., neste sentido, Acórdão de 14 de maio de 2020, Staatsanwaltschaft Offenburg, C-615/18, EU:C:2020:376, n.º 72).*

[…]" (sublinhado acrescentado).

Este último aspeto – a ausência de *efeito direto* da disposição de DUE (circunstância que é particularizada no ponto 41 do Acórdão *ZX*) – carece, para uma correta compreensão do sentido e do âmbito de aplicação do princípio da interpretação conforme ao DUE, de algum enquadramento adicional.

**2.1.** Importa ter presente, com efeito, que a construção do princípio pela jurisprudência do TJ – tomando como pontos de referência iniciais os Acórdãos *Colson Kamann*, de 10 de abril de 1984 (processo 14/83) e *Marleasing*, de 13 de novembro de 1990 (processo C-106/89)[5] e considerando as decisões posteriores sobre o princípio da interpretação conforme – assentou fundamentalmente na consideração de fontes de DUE desprovidas de *efeito direto*, ou portadoras de alguma ambiguidade quanto a essa característica. Ou seja, o TJ só considerou aptas à convocação do referido princípio, dentro da tipologia de fontes de Direito da União: (i) Diretivas não transpostas ou deficientemente transpostas; (ii) disposições de uma Diretiva não contendo uma obrigação incondicional e suficientemente precisa (suscetível de induzir um *efeito direto vertical*); (iii) Decisões-Quadro[6]. Daí que, a alternativa à interpretação conforme, quando esta não é (interpretativamente) possível, consistente na desaplicação da norma nacional em contradição com o DUE, dependa invariavelmente da circunstância de este ter efeito direto[7].

**3.** A situação apresentada ao Tribunal pela Requerente (o destino das normas da Lei n.º 32/2008, face à invalidação pelo TJ da Diretiva que essas normas transpuseram) conduz-nos a um outro plano de incidência do DUE, distinto do da atuação do princípio da interpretação conforme, ao qual a questão do efeito direto é estranha. Coloca-nos, como já antes dissemos, no quadro de atuação do *princípio da cooperação leal*.

Com efeito, qualquer das normas indicadas pela Requerente (artigos 4.º, 6.º e 9.º da Lei 32/2008) era redundante relativamente a normas da Diretiva 2006/24/CE invalidada, ou preenchia espaços de

regulação por esta abertos[8], tratando-se aqui, enquanto incidência relevante supervenientemente induzida pela dinâmica própria do DUE, de projetar o sentido de uma decisão do TJ de invalidação da "causa" (de DUE) que determinou as normas nacionais.

Ora, a obrigação de transposição de uma Diretiva – e a vinculação dos Estados-membros quanto ao resultado a alcançar (como estabelece o artigo 288.º, terceiro parágrafo, do TFUE: "[*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*") – dá expressão à *vertente positiva* do princípio da cooperação leal (artigo 4.º, n.º 3, 2.º parágrafo, parte final, do TUE), segundo o qual *os Estados-membros tomam todas as medidas adequadas para garantir a execução das obrigações decorrentes* (neste caso) *dos atos das instituições da União*.

Do mesmo modo, no caso de invalidade da Diretiva que fixa a obrigação de resultado, ou fim, aos Estados-Membros, cabe igualmente a estes, por força do princípio da cooperação leal – nas suas vertentes positiva e negativa (esta prevista no artigo, 4.º, n.º 3, 3.º parágrafo, do TUE: "[*o*]*s Estados-membros facilitam à União o cumprimento da sua missão e abstêm-se de qualquer medida suscetível de pôr em perigo a realização dos objetivos da União*") – não só não aplicar as normas adotadas em transposição da Diretiva, e que concretizam a sua obrigação de resultado, como de as eliminar do ordenamento jurídico nacional, assim pondo fim à *contradição* (aqui supervenientemente induzida pelo Acórdão *Digital Rights*) do Direito nacional com o Direito da União[9] – e/ou de as modificar (no quadro do *princípio da subsidiariedade* e no respeito por outras vinculações que possam advir do DUE).

É neste sentido, como manifestação atuante do *princípio da cooperação leal*, que, por força do artigo 8.º, n.º 4, primeira parte[10], da CRP, a projeção do controlo de proporcionalidade já efetuado pelo TJ no Acórdão *Digital Rights* aqui se impõe, enquanto manifestação do DUE (correspondente aos *termos por ele definidos*) e, consequentemente, como *dado prévio* que deve ser integrado na apreciação de constitucionalidade protagonizada pelo Tribunal Constitucional, não realizando este um controlo redundante daquele – que sempre envolverá a possibilidade, mesmo que eventual, de chegar a resultados diferentes dos correspondentes ao *standard europeu* fixado pelo TJ, que aqui deve ser projetado.

**4.** Os subscritores do presente voto concordam com o resultado que o dispositivo expressa (exceção feita à omissão do parâmetro do artigo 8.º, n.º 4, da CRP), não se revendo, todavia – e corresponde a uma divergência significativa –, na parte da fundamentação do Acórdão que, na decisiva tarefa de procurar esclarecer a relação entre normas de direito interno agora, depois do Acórdão *Digital Rights*, suscetíveis de serem reconduzidas ao (ou lidas no quadro do) exercício da faculdade condicionada, prevista no artigo 15.º, n.º 1, da Diretiva 2002/58/CE, e a interpretação que dele faz o TJ à luz dos direitos consagrados nos artigos 7.º, 8.º e 11.º da CDFUE, não apenas desconsidera o sentido que o artigo 8.º, n.º 4, da CRP, atribui a este controlo, como convoca, em sua substituição, o princípio da interpretação conforme ao Direito da União Europeia. Nessa medida, e porque daquele controlo, *funcionalmente equivalente* àquele que seria autonomamente realizável pelo Tribunal Constitucional, decorre já que o nível de proteção dos direitos ao respeito pela vida privada, à proteção dos dados pessoais e à liberdade de expressão assegurado pela CDFUE é

incompatível com regimes de direito interno como aquele que resulta das normas sob fiscalização, afastam-se do controlo de natureza sucedânea que a maioria considerou imperativo.

*José António Teles Pereira - Maria Benedita Urbano - Pedro Machete – Joana Fernandes Costa – Gonçalo de Almeida Ribeiro – João Pedro Caupers*

**DECLARAÇÃO DE VOTO**

**1.** No presente acórdão de que este voto faz parte integrante foi entendido padecerem as normas dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, de 17 de julho, de inconstitucionalidade, por violação dos n.ºs 1 e 4 do artigo 35.º, n.º 1 do artigo 26.º, e n.º 1 do artigo 20.º, em conjugação com o n.º 2 do artigo 18.º da CRP.

Para tanto, aí se expendeu, em síntese, o seguinte raciocínio.

- no que respeita à obrigação dos fornecedores de serviços de comunicações eletrónicas conservarem os *dados de base* que não pressupõem a análise de quaisquer comunicações (incluindo os endereços de protocolo IP que identificam a fonte da comunicação), «o direito da União Europeia não põe em causa a ponderação de proporcionalidade feita pelo Tribunal Constitucional no Acórdão n.º 420/2017, sendo esta *conforme* ao parâmetro europeu, cujo sentido foi clarificado pela jurisprudência do Tribunal de Justiça»;

- já quanto aos *dados de tráfego* e *dados de localização*, ainda que não gerados em virtude de uma comunicação pessoal, à luz dos parâmetros europeus aqui convocáveis (Acórdão do TJUE, *la quadrature du net*) «trata-se de uma solução legislativa desequilibrada, por atingir sujeitos relativamente aos quais não há qualquer suspeita de atividade criminosa. Ao conservar todos os dados de localização e de tráfego de todos os assinantes, abrangem-se as comunicações eletrónicas de quase toda a população, sem qualquer diferenciação, exceção ou ponderação face ao objetivo perseguido»;

- o regime de acesso aos dados armazenados constante do artigo 9.º da Lei n.º 32/2008, ao não prever a notificação ao visado de que os seus dados foram acedidos, restringe de modo desproporcionado o direito à autodeterminação informativa e o direito a uma tutela jurisdicional efetiva, uma vez que não se criam «as condições efetivas para não só *saber* da difusão dos seus dados como de *exercer um controlo* sobre a licitude e regularidade daquele acesso», tal como o TJUE decidiu no Acórdão *Tele 2.*

**2**. Não podemos concordar com o entendimento de que tais normas sacrificam ou prejudicam de modo excessivo, intolerável ou desrazoável um dos bens ou valores em presença. Relativamente à existência de um *período de conservação* dos dados, previsto no artigo 6.º da Lei n.º 32/2008, o acórdão utiliza como *único* instrumento de ponderação valorativa o *grau de intensidade* da agressão à intimidade da vida privada e à autodeterminação informativa do respetivo titular: os dados de base, «*tendo em conta a mais baixa intensidade da agressão*», podem ser conservados de modo generalizado; já os dados de tráfego e de localização, porque materializam uma «*agressão*

*particularmente intensa*» desses direitos, não podem ser objeto de conservação generalizada, não podendo abranger «todos os dados de todas as pessoas».

Ora, a existência de um período de conservação de dados – no caso, o período de um ano – põe em conflito dois bens, valores ou interesses afirmados por normas ou princípios constitucionais: a *liberdade e segurança* (n.º 1 do artigo 27.º da CRP) e a *privacidade* e *autodeterminação* dos dados pessoais (artigos 26.º e 35.º da CRP). A ameaça de crimes violentos (v.g. terrorismo, sequestro e rapto) justifica que o Estado imponha um período de conservação de dados, em nome da segurança; já a vida privada e a autodeterminação informativa justificam medidas contra a devassa e intrusão na privacidade do titular dos dados. Não me parece que os bens ou valores em presença tenham um peso tão diferente ou distinto que levem ao sacrifício a 100% do valor da segurança, como acaba por resultar da declaração de inconstitucionalidade a que chegou a maioria que fez vencimento. Pelo contrário, na "concordância prática" entre os bens e valores em jogo - direito à autodeterminação informativa e o direito à segurança – consideramos que a Lei n.º 32/2008 encontrou um equilíbrio que otimiza e satisfaz razoavelmente ambos os direitos.

Com efeito, a conservação de dados está rodeada de *condicionamentos restritivos* que dão substância à garantia da privacidade: a conservação tem por finalidade exclusiva a investigação, deteção e repressão de crimes graves (artigo 3.º, n.º 1); a conservação é limitada a um ano (artigo 6.º); só abrange chamadas estabelecidas e falhadas (artigo 5.º); os ficheiros onde são conservados os dados devem estar separados de quaisquer outros ficheiros destinados a outros fins (artigo 3.º, n.º 3); os dados permanecem bloqueados, só sendo desbloqueados para transmissão às entidades competentes (artigo 7.º, n.º 2); a transmissão de dados só pode ser autorizada por um juiz de instrução, verificados certos pressupostos (artigo 9.º, n.º 1); os dados são destruídos logo que deixem de ser estritamente necessários para os fins a que se destinam (artigo 11.º, n.º 1); as rigorosas condições de proteção e segurança dos dados estão sujeitas ao controlo da Comissão Nacional de Proteção de Dados (artigo 7.º, n.º 5); e o não bloqueio dos dados ou o desbloqueio ilícito constituem crime punível com pena de prisão até dois anos ou multa até 240 dias (artigo 13.º, n.º 1).

Todavia, o que resulta do presente acórdão é que só é possível impor um período de conservação de dados de tráfego relativamente a pessoas em relação às quais existam indícios de que o seu comportamento possa ter algum *nexo* com os crimes graves enunciados na alínea g) do n.º 1 do artigo 2.º da Lei n.º 32/2008. A ser assim, os fornecedores de serviços de telecomunicações apenas podem "*conservar*" os dados quando a autoridade judiciária competente os solicitar no decurso de uma investigação criminal. Ora, esta situação de "*preservação*" de dados (*quick freeze*), que já se encontra prevista no artigo 12.º da Lei do cibercrime (Lei n.º 109/2009, de 15 de setembro), não se mostra eficaz para garantir a recolha de prova em processo penal. Verifique-se, por exemplo, uma situação de rapto, um dos crimes incluídos naquela norma: se os dados relativos às comunicações das vítimas forem apagados, findas que sejam tais comunicações, poderá ser muito difícil identificar os agentes dos crimes; o mesmo se diga relativamente a toda a criminalidade que é praticada com recurso a meios informáticos e de telecomunicações eletrónicas, como, por exemplo, o crime de aliciamento de menores. De modo que a disponibilidade de dados históricos para a investigação criminal só é possível se eles forem temporariamente retidos pelos operadores de

telecomunicações. Ou seja, a conservação de dados é *estritamente necessária* para as finalidades da investigação, porque só assim é possível obter dados historicamente determinados.

Tendo em conta as circunstâncias em que os dados são retidos, não creio *excessiva* a restrição ao direito à autodeterminação informativa, previsto no artigo 35.º da CRP. As normas deste preceito constitucional autorizam *expressamente* o legislador a definir as condições em que os dados pessoais podem ser automatizados (n.º 2), a autorizar o tratamento de dados referentes à vida privada (n. º 3) e a especificar as situações excecionais em que terceiros podem ter acesso aos dados (n.º 4). Ora, a definição legislativa dos termos e condições em que este direito deve ser afirmado não pode deixar de considerar os avanços tecnológicos das últimas décadas, que potenciam o uso de mecanismos de intrusão na esfera de vida privada dos utilizadores, com o consequente risco de perda da privacidade, assim como a possibilidade de esses espaços digitais serem utilizados para o cometimento de crimes. Por isso, em nome do direito à liberdade e à segurança, podem e devem ser impostas restrições ao direito à autodeterminação informativa. Assim acontece com a conservação de dados de comunicações, cujo regime está dotado dos meios adequados, indispensáveis e equilibrados ao cumprimento pelo Estado do dever de proteção dos cidadãos contra a criminalidade violenta, sem sacrifício excessivo da proteção da privacidade do titular dos dados. O reforço dos meios ao alcance das autoridades judiciárias para garantir uma mais fácil obtenção de prova, através da imposição de regras de conservação de dados pessoais, constitui um valor que justifica alguma compressão da proibição do tratamento informático de dados referentes à vida privada. De resto, a lei habilita os operadores a conservarem pelo prazo de seis meses grande parte desses dados para efeitos de faturação (n.º 3 do artigo 6.º da Lei 41/2004, de 18 de agosto, na redação dada pela Lei n.º 46/2012, de 29 de agosto e artigos 9.º, n.º 2 e 10.º. n.º 1, da Lei n.º 23/96 de 26 de julho), sem que isso ponha em causa a privacidade dos utilizadores. A maioria que fez vencimento atendeu *unicamente* à intensidade da agressão que a conservação dos metadados causa na esfera privada do respetivo titular, desconsiderando, porém, o interesse público da segurança, quando temos por certo que a norma questionada reclama e reflete um equilibro desses diferentes bens, valores e interesses.

**3.** A apreciação que o acórdão faz sobre a proporcionalidade das normas questionadas é influenciada pelo juízo de proporcionalidade efetuado pelo TJUE nos Acórdãos *Digital Rights Ireland*, *Tele 2 e La quadrature du net*. Simplesmente, apesar de se estar no âmbito de aplicação de direito europeu, tal juízo não pode aqui ser seguido por três ordens de razão: (i) foi realizado num *contexto normativo* bastante diferente da Lei n.º 32/2008; (ii) aplicou o princípio da proporcionalidade baseado numa *proposta metódica* que os artigos 18.º, n.º 2 e 35.º da CRP não consentem; (iii) A *competência* para aferir se o direito europeu está em conformidade com os "princípios fundamentais do Estado de direito Democrático" pertence ao Tribunal Constitucional.

Em primeiro lugar, a Diretiva 2006/24/CE, que o Acórdão *Digital Rights Ireland* invalidou, por exceder os limites impostos pelo respeito do princípio da proporcionalidade à luz dos artigos 7.º e 8.º da CDFUE, foi transposta para a ordem jurídica interna pela Lei n.º 32/2008. Todavia, o legislador nacional optou por criar um quadro normativo que vai *muito para além* da Diretiva, prevendo um regime processual específico nesta matéria, nomeadamente quanto à segurança e

acesso aos dados armazenados. De modo que as principais objeções que o TJUE colocou à Diretiva e que foram determinantes no juízo sobre a violação do princípio da proporcionalidade, como a inexistência de critérios objetivos da duração da conservação de dados, a criação de mecanismos de segurança e proteção eficaz dos dados e o estabelecimento de garantias de acesso das autoridades a essas informações, não podem ser apontadas à Lei n.º 32/2008. Como já se referiu, contrariamente ao que ocorre na Diretiva, a Lei n.º 32/2008 contém normas que garantem a segurança dos dados conservados e critérios disciplinadores do acesso aos dados armazenados. Portanto, sem o reenvio prejudicial, não se pode concluir com segurança que o juiz de proporcionalidade efetuada pelo TJUE naqueles acórdãos pode ser transposto para a ordem interna ou influenciar a aplicação do mesmo princípio às normas da Lei n.º 32/2008.

Em segundo lugar, e na sequência do que se acaba de dizer, perante o que se dispõe nos n.ºs 1 e 4 do artigo 35.º da CRP não é possível aplicar o princípio da proporcionalidade separando o *regime da conservação* dos dados pelos operadores de telecomunicações do *regime de acesso* aos mesmos. A parte final dos n.ºs 1 e 4 do artigo 35.º autoriza a informatização de dados sem o consentimento do titular, remetendo para a lei a definição dessas condições. Na primitiva redação a ressalva incluía apenas o «disposto na lei sobre segredo de Estado e segredo de justiça»; mas na revisão de 1997 adotou-se uma fórmula mais ampla ("nos termos da lei"), para possibilitar outras restrições ao direito de acesso, designadamente no caso de medidas necessárias em matéria de segurança do Estado, defesa, segurança pública, prevenção, investigação, detenção e repressão de infrações penais, restrições que já estavam previstas no artigo 13.º da Diretiva 95/46/CE do Parlamento Europeu e do Conselho. A Lei n.º 32/2008 é um desses diplomas que contém normas restritivas do acesso, pois no n.º 4 do artigo 3, º prevê que «o titular dos dados não pode opor-se à respetiva conservação e transmissão». Ora, como se refere acórdão, sem que depois retire daí as devidas consequências em matéria de dados de tráfego (contrariamente ao que se fez com os dados de base), «*um maior rigor do legislador no acesso e na transmissão dos dados conservados pode, em abstrato, autorizar uma maior amplitude no domínio da sua conservação pelos operadores, contanto se garanta a sua segurança*». É evidente que, para aplicar o primeiro pressuposto do princípio da proporcionalidade - a existência de um conflito entre a segurança e a privacidade – não pode deixar de se considerar as condições de segurança e de acesso aos dados armazenados. Com efeito, a intensidade da restrição que a conservação representa depende em grande medida das garantias inerentes à transmissão e acesso a esses dados. Se apenas as autoridades judiciárias tiverem acesso aos dados encriptados, com base em pressupostos previamente definidos, é óbvio que as oportunidades de devassa e difusão dos dados pessoais são escassas. Por outro lado, se assim não fosse, não poderia haver tratamento automático de informações pessoais em situações em que estão em causa valores supremos, como sejam a segurança do Estado e a necessidade de levar a cabo atos de prevenção, investigação e repressão criminal, já que tal tratamento tem por finalidade a transmissão de dados às autoridades policiais e judiciárias (nacionais ou estrangeiras) para efeito de prevenção e investigação criminal.

Em terceiro lugar, no âmbito das relações entre os Estados-membros e a União Europeia, no que se refere à validade de normas, quem tem a *competência das competências* é o Tribunal Constitucional. O TJUE, porque subordinado aos Tratados, não pode determinar a amplitude das suas prerrogativas de controlo. Isto resulta claramente do n.º 4 do artigo 8.º da CRP que impõe dois

limites ao primado do Direito da União: (i) trata-se de um primado de normas de Direito da UE emanadas no exercício de competências que são atribuídas; (ii) trata-se de um primado sobre todas as normas que não tenham valor normativo constitucional. Sobre a relevância deste último limite, estando em causa o *princípio da igualdade*, o Tribunal Constitucional já se prenunciou por duas vezes: no *Acórdão n.º 141/2015,* que tinha por objeto uma norma de direito interno, o Tribunal analisou o Direito da União Europeia e a interpretação que dele foi feita pelo TJUE, concluído que não havia qualquer dúvida que se tolerava a diferença de tratamento constante da norma sindicada quanto à atribuição de prestações de regimes não contributivos de uma prestação social; *no Acórdão n.º 422/2020*, estando em causa uma norma de Direito da União Europeia já interpretada pelo TJUE, o Tribunal conclui que o requerente não demonstrou que o artigo 13.º da CRP garantia um nível de proteção superior ao da CDFUE na atribuição de auxílios de estado.

No caso dos autos, está em causa a aplicação do *princípio da proporcionalidade*, que indiscutivelmente é um princípio jurídico fundamental abrangido por aquele limite ao primado. Ainda que haja identidade material do princípio da proporcionalidade *enquanto tal* (artigo 52.º, n.º 1 da CDFUE e artigo 18.º, n.º 2 da CRP), os pressupostos da sua *aplicação* foram diferentes. No segmente da necessidade - ingerência nos direitos fundamentais para além do estritamente necessário -, o TJUE considerou nos três acórdãos referidos que a conservação de dados só é admissível quando obedeça a três critérios objetivos: «*um período temporal*»; «*uma zona geográfica determinada*»; e «*um círculo de pessoas determinado*». Ora, uma medida legislativa de conservação preventiva de dados, geograficamente condicionada, dirigida a um círculo de pessoas determinadas, sem qualquer facto típico cometido, não é tolerada pela norma do n.º 3 do artigo 35.º da CRP, que apenas admite que o legislador autorize tratamento informático de dados relativos à vida privada «*com garantias de não discriminação*». O entendimento do TJUE, para além de metodicamente incorreto, na medida em que não atende a um dos bens ou interesses em conflito – a segurança – e considera isoladamente a norma que delimita o âmbito subjetivo da conservação dos dados, viola o princípio da igualdade e a proibição de discriminação. Não é por mero acaso que o Tribunal Constitucional Alemão – onde não existe normas constitucionais tão densas como os artigos 8.º, n.º 4, e 35.º da CRP – considerou por duas vezes que a conservação *generalizada* de metadados (de todos os dados de todos os utilizadores) não é, por si só, desconforme à Constituição, desde que haja um regime adequado de segurança da conservação e de transmissão de dados (Acórdão do 1. Senat de 2 de março de 2010 – 1 BvR 256/08; 1 BvR 263/08; 1 BvR 586/08, e de 19 de maio de 2020, - 1 BvR 2835/17). Na medida em que o n.º 4 do artigo 8.º da CRP impõe limites jurídicos à receção do Direito da União Europeia, impondo o "respeito pelos princípios fundamentais do Estado de direito democrático", o Tribunal Constitucional não pode aceitar uma interpretação do direito europeu que está em desconformidade com a norma do n.º 3 do artigo 35.º da CRP.

**4**. Quanto à *territorialidade* dos dados e à falta de *notificação*, o problema nem sequer se deveria colocar perante a Lei n.º 32/2008.

O n.º 4 do artigo 7.ª desta Lei, relativo à proteção e segurança dos dados, remete para as normas previstas na Lei de Proteção de Dados - Lei n.º 67/98, de 26 de outubro - (artigos 4.º, 18.º e 19l) e na Lei n.º 41/2004, de 18 de agosto, onde se resolve a questão da territorialidade e da transferência na

e para fora União Europeia. Atualmente a questão está regulada no Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (artigos 44.º a 50.º). De resto, quando se sujeita a conservação dos dados ao controlo da CNPD, implicitamente se está a admitir que a sede dos dados tem que ser o território português.

De igual modo, o artigo 9.º da Lei n.º 32/2008 não é a sede para regular se e quando o titular dos dados deve ser notificado pelas autoridades judiciárias do acesso e transmissão de dados. De resto, se se conclui que os dados não podem ser conservados, como se faz no acórdão, o problema da notificação fica prejudicado, porque não havendo dados armazenados não há acesso e consequentemente não haverá notificação. Ou seja, o problema da notificação só se coloca se se admitir a conservação dos dados e a respetiva transmissão. Porém, o n.º 5 do artigo 10.º da Lei de Proteção de Dados preceitua que, para além de outros casos, a «obrigação de informação pode ser *dispensada* mediante disposição legal ou deliberação da CNPD, por motivos de segurança do Estado e prevenção ou investigação criminal». É evidente que assim tem que ser: se o processo estiver em segredo de justiça, pode não haver conveniência em notificar o suspeito de que os seus dados foram recolhidos. Portanto, a questão da notificação dos meios de prova recolhidos é matéria que só o direito processual penal tem que resolver no âmbito do estatuto do arguido (artigo 61.º do CPP).

*Lino José Batista Rodrigues Ribeiro*

---

[1] "[…]

***44.º**. Pelo que ainda que, no plano jurídico-constitucional, a declaração pelo TJUE da invalidade da Diretiva 2006/24/CE não tenha como efeito automático a invalidade da Lei n.º 32/2008, a deliberação do Tribunal Constitucional quanto à conformidade das normas constantes desse ato legislativo com a Constituição da República Portuguesa deve adotar uma fundamentação que, tanto quanto possível, seja consistente com a do TJUE nos acórdãos Digital Rights Ireland e Tele2.*

***45.º**. Em virtude da direta vinculação à Carta da Lei n.º 32/2008, tal «dever de consistência na fundamentação» retira-se do princípio da cooperação leal a que a República Portuguesa - e, portanto, todos os órgãos do Estado, inclusive de índole jurisdicional - se encontra vinculada (artigo 4.º, n.º 3, do Tratado da União Europeia).*

***46.º**. Em nosso entender, tanto bastaria para que o Tribunal Constitucional declarasse com força obrigatória geral, a inconstitucionalidade dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, por violação do princípio da proporcionalidade na restrição dos direitos à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1) e por violação do direito a uma tutela jurisdicional efetiva (artigo 20.º, n.º 1).*

[…]".

[2] … do Parlamento Europeu e do Conselho, de 15 de março, *relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE*.

[3] E esse mesmo *standard* tem sido invariavelmente reafirmado pelo TJ, nos pronunciamentos subsequentes ao Acórdão *Digital Rights* em que uma conservação generalizada desses dados, não parametrizada por "*filtros*" (temáticos, geográficos, situacionais) previamente estabelecidos, confrontou o Tribunal – Acórdãos, *Tele2 Watson* (de 21/12/2016; procs. C-203/15 e C-698/15), *Privacy International* (06/10/2020; proc. C-623/17), *La Quadrature du Net* (de 06/10/2020; procs. C-511/18 e C-512/18); *H. K. Prokuratur* (de 02/03/2021; proc. C-746/18), e, como exemplo mais recente, no Acórdão *Commissioner of the Garda Síochána* (de 05/04/2022; proc. C-140/20):

"[…]

*O artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que se opõe a medidas legislativas que preveem, a título preventivo, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização. Em contrapartida, o referido artigo 15.º, n.º 1, lido à luz dos artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, não se opõe a medidas legislativas que prevejam, para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública,*

*– uma conservação seletiva dos dados de tráfego e dos dados de localização que seja delimitada, com base em elementos objetivos e não discriminatórios, em função das categorias de pessoas em causa ou através de um critério geográfico, por um período temporalmente limitado ao estritamente necessário, mas que pode ser renovado;*

*– uma conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário;*

*– uma conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos, e*

*– uma imposição aos prestadores de serviços de comunicações eletrónicas, através de uma decisão da autoridade competente sujeita a fiscalização jurisdicional efetiva, do dever de procederem, por um determinado período, à conservação rápida dos dados de tráfego e dos dados de localização de que esses prestadores de serviços dispõem, desde que essas medidas assegurem, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e que as pessoas em causa disponham de garantias efetivas contra os riscos de abuso.*

[…]".

[4] Citando e parafraseando, Maria Luísa Duarte, *Direito da União Europeia. Lições Desenvolvidas*, Lisboa, 2021, p. 350.

[5] É relevante sublinhar, quanto aos limites da interpretação conforme, o inciso – "*na medida do possível"* – introduzido pelo Tribunal de Justiça, na caracterização do princípio da interpretação conforme ao Direito da União, no ponto 8 do Acórdão *Marleasing*: "[…] *ao aplicar o direito nacional, quer se trate de disposições anteriores ou posteriores à diretiva, o órgão jurisdicional nacional chamado a*

*interpretá-lo é obrigado a fazê-lo, na medida do possível, à luz do texto e da finalidade da diretiva, para atingir o resultado por ela prosseguido e cumprir desta forma o artigo 189.º, terceiro parágrafo, do Tratado* [atualmente, artigo 288.º, terceiro parágrafo do TFUE]".

[6] Importa ter presente a natureza especial das Decisões-Quadro, caso do Mandado de Detenção Europeu – que estava em causa no Acórdão *Poplawski* (nota 7, infra) –, enquanto instrumentos legislativos peculiares, anteriores ao Tratado de Lisboa, e que este suprimiu (cfr. o atual elenco dos atos jurídicos da União, no artigo 288.º do TFUE). Correspondiam as Decisões-Quadro a fontes específicas do III Pilar, *Cooperação política e judiciária em matéria penal* (sistema que terminou com o Tratado de Lisboa), então previstas no artigo 34.º do Tratado da União ("pré-Lisboa", versão de 2006, pós-Nice):

*Artigo 34.º*

---

*-----2- O Conselho toma medidas e promove a cooperação, sob a forma e segundo os processos adequados instituídos pelo presente título, no sentido de contribuir para a realização dos objetivos da União. Para o efeito, o Conselho pode, deliberando por unanimidade, por iniciativa de qualquer Estado-Membro ou da Comissão:*

---

*b) Adotar decisões-quadro para efeitos de aproximação das disposições legislativas e regulamentares dos Estados-Membros. As decisões-quadro vinculam os Estados-Membros quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios. As decisões-quadro não produzem efeito direto;*

---

[sublinhado acrescentado].

O destino das Decisões-Quadro adotadas anteriormente ao Tratado de Lisboa é matéria tratada no Protocolo Relativo às Disposições Transitórias (anexo ao Tratado de Lisboa):

*Artigo 9.º*

*Os efeitos jurídicos dos atos das instituições, órgãos e organismos da União adotados com base no Tratado da União Europeia com base no Tratado da União Europeia antes da entrada em vigor do Tratado de Lisboa são preservados enquanto esses atos não forem revogados, anulados ou alterados em aplicação dos Tratados.*

[7] Esta questão é tratada no Acórdão *Poplawski*, de 24 de junho de 2019 (C-573/17), amplamente citado no Acórdão *ZX*, estando em causa, precisamente, uma fonte desprovida de efeito direto, uma Decisão-Quadro (mandado de detenção europeu):

"[…]

***59***.[*I*]*mporta* […] *ter em conta outras características essenciais do direito da União, mais especificamente o reconhecimento de um efeito direto a uma parte apenas das disposições desse direito.*

***60*** *O princípio do primado do direito da União não pode, portanto, ter como consequência pôr em causa a distinção essencial entre as disposições do direito da União que dispõem de efeito direto e as que não têm esse*

*efeito, nem, portanto, instituir um regime único de aplicação de todas as disposições do direito da União pelos órgãos jurisdicionais nacionais.*

***61*** *A este respeito, há que sublinhar que qualquer juiz nacional, chamado a pronunciar-se no âmbito da sua competência, tem, enquanto órgão de um Estado-Membro, a obrigação de não aplicar qualquer disposição nacional contrária a uma disposição de direito da União que tenha efeito direto no litígio que é chamado a decidir (v., neste sentido, Acórdãos de 8 de setembro de 2010, Winner Wetten, C-409/06, EU:C:2010:503, n.º 55 e jurisprudência referida; de 24 de janeiro de 2012, Dominguez, C-282/10, EU:C:2012:33, n.º 41; e de 6 de novembro de 2018, Bauer e Willmeroth, C-569/16 e C-570/16, EU:C:2018:871, n.º 75).*

***62*** *Em contrapartida, uma disposição do direito da União que não tenha efeito direto não pode ser invocada, enquanto tal, no âmbito de um litígio abrangido pelo direito da União, a fim de afastar a aplicação de uma disposição de direito nacional que lhe seja contrária.*

***63*** *Assim, o juiz nacional não é obrigado, com fundamento unicamente no direito da União, a deixar de aplicar uma disposição do direito nacional incompatível com uma disposição da Carta dos Direitos Fundamentais da União Europeia que, como o seu artigo 27.º* [refere-se este ao Direito à informação e à consulta dos trabalhadores na empresa]*, não tem efeito direto (v., neste sentido, Acórdão de 15 de janeiro de 2014, Association de médiation sociale, C-176/12, EU:C:2014:2, n.os 46 a 48).*

***64*** *De igual modo, a invocação de uma disposição de uma diretiva que não seja suficientemente clara, precisa e incondicional para lhe ser reconhecido efeito direto não pode ter como consequência, com fundamento unicamente no direito da União, que a aplicação de uma disposição nacional seja afastada por um órgão jurisdicional de um Estado-Membro (v., neste sentido, Acórdãos de 24 de janeiro de 2012, Dominguez, C-282/10, EU:C:2012:33, n.º 41; de 6 de março de 2014, Napoli, C-595/12, EU:C:2014:128, n.º 50; de 25 de junho de 2015, Indėlių ir investicijų draudimas e Nemaniūnas, C-671/13, EU:C:2015:418, n.º 60; e de 16 de julho de 2015, Larentia Minerva e Marenave Schiffahrt, C-108/14 e C-109/14, EU:C:2015:496, n.os 51 e 52).*

[…]" (sublinhados acrescentados).

[8] Os artigos 4.º, 6.º e 9.º da Lei n.º 32/2008, referiam-se às categorias de dados a conservar, no quadro criado pela Diretiva. Em concreto, o artigo 4.º transpunha, nos seus termos exatos, o artigo 5.º da Diretiva; o artigo 6.º da Lei n.º 32/2008 referia-se ao período de conservação desses dados pela operadora, fixando o período de um ano, "*a contar da data da conclusão da comunicação*", transpondo no seu termo médio o período variável que estava fixado no artigo 6.º da Diretiva (que previa um mínimo de 6 meses e um máximo de 2 anos); o artigo 9.º da Lei n.º 32/2008, referia-se à transmissão desses dados, pretendendo materializar, no quadro geral traçado pelo artigo 4.º da Diretiva, as condições de acesso a esses dados pelas autoridades nacionais competentes.

[9] "[*M*]*esmo que na prática, as autoridades de um Estado-membro não apliquem aos nacionais dos outros Estados-membros disposições nacionais contrárias ao* [DUE]*, esta circunstância não é suscetível de fazer desaparecer a violação do* [DUE] *consubstanciada por tais disposições*", uma vez que "[…] *a incompatibilidade de uma legislação nacional com as disposições* [de DUE]*, mesmo diretamente aplicáveis, não pode ser definitivamente eliminada senão através de normas internas de carácter coercivo com o mesmo valor jurídico que as que devem ser modificadas*" [parágrafos 16 e 17 do Acórdão *Comissão das Comunidades Europeias c. República italiana*, de 9 de março de 2000 (proc. C358/98)].

[10] Estamos fora do âmbito de aplicação do contralimite que subjaz ao trecho final do referido n.º 4.