A Sua Excelência
A Ministra da Justiça
Praça do Comércio
1149-019 Lisboa

– por protocolo –

Lisboa, 22 de janeiro de 2019

Sua referência	Sua comunicação	Nossa referência
		Q/7746/2017 (UT 6)

Assunto: Lei n.º 32/2008, de 17 de julho, 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

Recomendação n.º 1/B/2019

(alínea b) do n.º 1 do artigo 20.º, da Lei n.º 9/91, de 9 de abril)

Nos termos e para os efeitos do disposto na alínea b) do n.º 1 do artigo 20.º do Estatuto do Provedor de Justiça (Lei n.º 9/91, de 9 de abril) recomendo a Vossa Excelência que promova a alteração à Lei n.º 32/2008, de 17 de julho, a fim de que o regime nela inscrito se venha a conformar com as exigências decorrentes da Carta dos Direitos Fundamentais da União Europeia, tal como foram tais exigências interpretadas pela jurisprudência pertinente do Tribunal de Justiça.

É a seguinte, a motivação da minha Recomendação

I

A proteção dos dados pessoais e o Direito da União

1. Há muito que o Direito da União Europeia se vem ocupando da resolução dos problemas atinentes ao tratamento de dados pessoais e da sua necessária e equilibrada compatibilização com o direito fundamental à reserva da vida privada. Foi assim que, com o intuito de assegurar que, no contexto do estabelecimento e do funcionamento do mercado interno, «os dados pessoais [pudessem] circular livremente de um Estado-membro para outro, mas igualmente que [fossem] protegidos os direitos fundamentais das pessoas», a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, definiu o regime geral de proteção das pessoas singulares quanto ao tratamento e livre circulação dos dados; como foi assim que, ciente de que as «tradicionais estruturas de mercado» estariam a ser derrubadas pela Internet, e que esta última, apesar de abrir «novas possibilidades aos utilizadores», suscitava igualmente «novos riscos quanto aos seus dados pessoais e a sua privacidade» a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, veio por seu turno definir o regime aplicável ao tratamento de dados e à protecção da privacidade no setor específico das comunicações electrónicas.

2. Tanto num como noutro caso, os regimes definidos pelo Direito da União assentaram em três princípios estruturantes: o da proteção da confidencialidade dos dados e das comunicações; o da proteção do anonimato dos seus concretos titulares

e agentes; e o da proibição da conservação, por parte de agentes económicos e (ou) de operadores de comunicações electrónicas, de acervos de dados pessoais. Sendo estes os princípios estruturantes dos regimes – e servindo cada um deles o propósito de tutela dos direitos fundamentais em causa – as diretivas que os estabeleceram procuraram em geral compatibilizá-los com as exigências comunitárias que lhes fossem, *prima facie,* contrárias. Entre estas últimas contavam-se, quer as decorrentes da necessidade de garantir a fluidez do tráfego jurídico (v.g. faturação de assinantes e pagamento de interligações), quer as decorrentes da necessidade de garantir a livre circulação, no território da União, de dados, equipamentos e serviços.

3. Na Diretiva 2002/58/CE este esforço de compatibilização entre certas exigências comunitárias e os princípios da confidencialidade, do anonimato e da não-conservação de dados torna-se especialmente visível no artigos 1.º [«Âmbito e objectivos»]; no artigo 5.º [«Confidencialidade das comunicações]; no artigo 6.º, n.º 1 [eliminação e anonimização dos dados de tráfego por parte uma rede pública de comunicações ou de um serviço de comunicações electrónicas], e nos artigos 8.º e 9.º, sobre, respectivamente, «[a]presentação e restrição da identificação da linha chamadora» e «[d]ados de localização para além dos dados de tráfego».

4.Todavia, a par desta sistémica compatibilização entre os princípios estruturantes do regime e exigências comuns que lhe fossem contrárias, a Diretiva 2002/58/CE (na sequência, aliás, do que fora já previsto na Diretiva 95/46/CE) admitiu ainda a possibilidade de *derrogação* daqueles mesmos princípios em circunstâncias bem identificadas. A admissão consta do n.º 1 do seu artigo 15.º, que diz: «[o]s Estados-Membros podem adoptar 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 directiva 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 detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas».

5. A possibilidade de derrogação do princípio relativo à *proibição de conservação de dados* merece, no preceito que vimos analisando, especial menção. De acordo com segunda parte do n.º 1 do artigo 15.º da diretiva «(…) os Estados-Membros podem designadamente adoptar medidas legislativas prevendo que os dados sejam conservados durante um período limitado, pelas razões anunciadas no presente número)».

Assim, se de acordo com o regime-regra (artigos 5.º, 6.º e 9.º da Diretiva 2002/58/CE), as obrigações impendentes sobre os fornecedores de redes e serviços se traduziam no dever de eliminar ou tornar anónimos todos os dados de tráfego e todos os dados de localização gerados pela utilização de serviços de comunicações electrónicas (assim que tais dados deixassem de ser necessários para efeitos de transmissão da comunicação)[1], nos termos do regime excecional previsto no n.º 1 do artigo 15.º admite-se a possibilidade da tese contrária: sobre os fornecedores de redes e de serviços poderá vir a impender a *obrigação de conservação de dados,* sempre que tal se mostre necessário para a realização dos fins enumerados no preceito. Às legislações dos Estados-Membros cabe definir os termos em que, em cada território nacional, se virá a cumprir esta última obrigação.

6. Na sequência desta previsão excecional, vários Estados-Membros aprovaram, logo após 2002, as respetivas leis definidoras dos termos em que os

[1] Com as excepções previstas para, nomeadamente, garantir a faturação e o pagamento das interligações.

fornecedores de redes e de serviços deveriam cumprir a *obrigação de conservação de dados,* com vista à prevenção, investigação e repressão de infrações penais. Todavia, em 2006, o Parlamento Europeu e o Conselho, considerando que« [a]s disparidades legislativas e técnicas existentes entre as disposições nacionais [já aprovadas] constituem obstáculos ao mercado interno das comunicações electrónicas» , uma vez que «os fornecedores de serviços são obrigados a satisfazer exigências diferentes quanto aos tipos de dados de tráfego e de dados de localização a conservar, bem como às condições e aos períodos de conservação dos dados»[2], adotaram a Diretiva 2006/24/CE, de 15 de março, «relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicação», alterando-se assim a Directiva 2002/58/CE».

7. Apesar de invocar, para justificar a sua adoção, o propósito de harmonização de leis nacionais já existentes, a diretiva de 2006 veio fazer muito mais do que apenas «harmonizar». Uma vez que vários Estados-Membros (entre eles, como se verá já de seguida, Portugal) ainda não tinham feito uso da possibilidade, que fora aberta em 2002, de prever regimes nacionais que regulassem a *obrigação de conservação de dados,* a Diretiva 2006/24/CE veio, para além de harmonizar o já existente, *instituir* a disciplina geral a que, doravante, deveriam obedecer os direitos nacionais na fixação dos termos e da amplitude que viria a assumir a referida obrigação [de conservação de dados]. Tratou-se, portanto, de uma diretiva dotada de uma dupla função[3], a um tempo harmonizadora e constitutiva: harmonizadora em relação aos Estados-Membros que já haviam "cumprido" a possibilidade que lhes fora dada pela diretiva de 2002; constitutiva em relação a todos os demais, que ainda

[2] Considerando 6 da diretiva a seguir mencionada

[3] A expressão «dualidade funcional» é a usada pelo Advogado-Geral Pedro Cruz Villalón nas conclusões apresentadas ao Tribunal de Justiça a 12 de dezembro de 2013 no processo C- 293/12 (*Digital Rights Ireland*), processo esse que dará origem ao acórdão em que o Tribunal – como se verá já de seguida - declara a invalidade da diretiva de 2006 (ponto 37 das conclusões).

o não haviam feito, mas que se viam doravante confrontados com a *obrigação* de o fazer. Nunca será de mais, creio, sublinhar esta dupla função ou "dupla dimensão", que teve por efeito transformar em *obrigação* algo que antes não passava de mera *possibilidade*. Como se verá adiante, o escrutínio estrito que o Tribunal de Justiça da União virá a aplicar, anos mais tarde, ao regime fixado na diretiva será em larga medida por ela [por essa transformação] explicado: como o acto de Direito da União impunha doravante aos Estados-Membros *a obrigação da conservação de dados,* e como tal obrigação, pela sua própria natureza, se traduzia numa ingerência acentuada em direitos fundamentais tutelados pela Carta, o conteúdo de tal acto não podia deixar de estar sujeito ao mais intenso controlo do Tribunal. Mas a este ponto, como já disse, adiante voltarei; por agora, um outro há que merece ser sublinhado.

8. O regime fixado pela Diretiva de 2006, e que mais tarde virá a ser invalidado pelo Tribunal de Justiça, preocupava-se em dar resposta a três questões essenciais. A primeira era a relativa ao *âmbito da obrigação da conservação de dados,* impendente, não sobre as autoridades públicas, mas sobre os operadores de serviços e redes de comunicação; a segunda era a relativa *ao regime de acesso aos dados conservados,* acesso esse que, em princípio – e dada a finalidade prosseguida pela conservação –, deveria ser restringido às autoridades de cada Estado-Membro; e a terceira era a relativa *ao regime de proteção e segurança dos dados conservados*, na esteira de preocupações desde o início reveladas, neste domínio, pelo Direito da União (Capítulo III da Diretiva 95/46/CE e artigo 13.º da Diretiva 2006/24/CE).

9. Assim, e em primeiro lugar, quanto ao *âmbito da obrigação de conservação de dados,* a diretiva deixava antes do mais claro que conservados seriam apenas os dados de tráfego e de localização «relativos quer a pessoas singulares quer a pessoas colectivas», bem como os necessários «para identificar o assinante ou o utilizador

registado», com exclusão dos que fossem referentes ao próprio conteúdo das comunicações electrónicas (artigos 1.º e 5.º da Diretiva 2006/24/CE)[4]. Para além disso, fazia impender sobre os Estados-membros a obrigação de tomar medidas para garantir tal conservação, «na medida em que [tais dados fossem] gerados ou tratados no contexto da oferta de serviços de comunicações em causa por fornecedores de serviços de comunicações electrónicas publicamente disponíveis quanto estes fornecedores [estivessem] sob a sua jurisdição.» (artigo 3.º) com um único limite: o de que a conservação não fosse feita nem durante um período de tempo inferior a seis meses, nem por mais de dois anos (artigo 6.º).

Em segundo lugar, e quanto ao *regime de acesso aos dados conservados,* determinava-se que os Estados-Membros tomassem medidas – a definir de acordo com o princípio da proporcionalidade, e sob reserva das disposições pertinentes do Direito da União e da CEDH, estas últimas tal como interpretadas pelo Tribunal Europeu dos Direitos do Homem – para assegurar que tais dados fossem *apenas* transmitidos «às autoridades nacionais competentes para casos específicos e de acordo com a legislação nacional» (artigo 4.º).

Finalmente, em terceiro lugar, quanto ao *regime de proteção e segurança dos dados conservados,* determinava a diretiva que cada Estado-Membro designasse uma ou mais autoridades públicas independentes para controlar a aplicação, no seu território, por parte das entidades obrigadas a conservar os dados, das regras relativas ao seu modo de armazenamento e tratamento (artigos 7.º e 9.º), destinadas naturalmente a prevenir o uso ilícito da informação obtida. Por seu turno, e para garantir a adequada repressão da ilicitude, determinava-se ainda que fossem tomadas as medidas necessárias para a aplicação plena, no domínio de tratamento de dados, de «recursos judiciais, responsabilidade e sanções.» (artigo 13.º).

[4]Ou seja, dados que permitam identificar tanto a fonte quanto o destino da comunicação, sua data, hora e duração, bem como o tipo de comunicação e o tipo de material utilizado.

10. Esta diretiva, com este conteúdo que acabou de ser resumido, foi transposta para a ordem jurídica interna pela Lei n.º 32/2008, de 17 de julho.

Ao definir o regime aplicável ao território nacional, a lei seguiu em geral a estrutura normativa já adotada pela diretiva. Obedeceu ao quadro geral que nela fora fixado quanto ao *âmbito da obrigação de conservação de dados,* quer proibindo expressamente «[a] conservação de dados que revelem o conteúdo das comunicações» (artigo 1.º, n.º 2), quer identificando exaustivamente as categorias dos dados a conservar (artigo 4.º); além disso, precisou o limite temporal de conservação que fora definido pelo Direito da União, fixando-o em um ano a partir da data da comunicação (artigo 6.º). Quanto ao *acesso aos dados conservados,* decidiu que ele só poderia ser justificado para a «investigação, detecção e repressão de crimes graves por parte das autoridades competentes» (artigo 3.º, n.º 1), enumerando o que considerava ser «crime grave» (artigo 2.º, n.º 1, *alínea* g]) e definindo o procedimento que deveria ser seguido para que, no âmbito de perseguição de tais crimes, e por despacho fundamentado do juiz de instrução, pudesse ser dada autorização à «autoridade competente» [Ministério Público ou autoridade policial] para que esta acedesse à informação que fora retida. Finalmente, quanto à *protecção e segurança dos dados conservados,* para além de ter especificado as regras que os fornecedores de serviços ou redes públicas de comunicações deveriam seguir no modo de armazenamento (artigo 7.º, n.os 1 a 4), identificou a Comissão Nacional de Proteção de Dados como sendo a entidade competente para o controlo da aplicação de tais regras (artigo 7.º, n.º 5), definiu os comportamentos ilícitos, a elas contrárias, que constituiriam contra-ordenações e distinguiu-os dos que constituiriam crimes (artigos 12.º e 13.º), e, finalmente, conferiu ainda à mesma Comissão Nacional [de Proteção de Dados] a competência para a instrução dos processos contra-ordenacionais e para a aplicação das correspondentes coimas.

II

A Jurisprudência do Tribunal de Justiça da União e a invalidação da Diretiva 2006/24/CE

11. A Diretiva 2006/24/CE, de 15 de março, veio no entanto a ser declarada inválida pelo Tribunal de Justiça da União Europeia (doravante TJUE) no Acórdão *Digital Rights Ireland Ltd,* proferido pela Grande Secção nos processos C-293/12 e C-594/12 a 8 de abril de 2014.

Os fundamentos da declaração de invalidade, constantes já do *Digital Rights*, viriam mais tarde a ser esclarecidos e completados no Acórdão *Tele 2,* proferido também pela Grande Secção do TJUE, mas desta vez a 21 de dezembro de 2016, nos processos C-203/15 3 C- 698/15.[5]

Nos dois acórdãos, o tribunal partiu do princípio segundo o qual a mera previsão de uma *obrigação de conservação de dados,* impendente sobre as operadoras de telecomunicações, constituía por si só uma medida que não podia deixar ser questionada face a valores decorrentes da Carta dos Direitos Fundamentais da União Europeia. Em causa estariam, particularmente, os direitos à proteção da vida privada (artigo 7.º da Carta), à proteção dos dados pessoais (artigo 8.º) e à liberdade de expressão (artigo 11.º). [§25 do *Digital Rights* e § 92 do *Tele 2*].

Também nos dois acórdãos a assunção deste princípio decorreu de um pressuposto muito claro: tanto num caso como noutro – tanto no do *Digital Rights,* em que o processo tinha como objeto toda a Diretiva de 2006, quanto no do *Tele 2,*

[5] Tendo por objeto, este último Acórdão, a *interpretação* do n.º 1 do artigo 15.º da Diretiva 2002/58/CE.

em que o processo tinha como objeto, apenas, a interpretação do disposto no n.º 1 do artigo 15.º da Diretiva de 2002 – estavam em causa actos da União, sujeitos naturalmente aos direitos previstos pela Carta; como a eles estariam sujeitos os actos dos direitos internos dos Estados-Membros que viessem a dar cumprimento às referidas diretivas, uma vez que seriam sempre, estes últimos, «actos [praticados pelos Estados-Membros] em aplicação do Direito da União». Nenhumas dúvidas restariam, pois, quanto à legitimidade de inclusão de todas as normas constantes destes actos no âmbito de aplicação da Carta, conforme o disposto pelo seu artigo 51.º [sobre este último ponto, e com particular desenvolvimento, vejam-se os § 63 a 81 do Acórdão *Tele 2*].

Depois, sempre em ambos os acórdãos, o TJUE deixou claro que considerava a *obrigação de conservação de dados* como uma ingerência *particularmente grave* nos direitos fundamentais em causa. O facto de tais dados, que deveriam ser conservados, serem «apenas» os dados de tráfego ou de localização não diminuía segundo o TJUE a intensidade da ingerência; pelo contrário, mantinha-a ou acentuava-a, na exata medida em que «[c]onsiderados no seu todo, estes dados são susceptíveis de permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as actividades exercidas, as relações sociais dessas pessoas e os meios sociais que frequentam, [pelo que] estes dados fornecem os meios para determinar (…) o perfil das pessoas em causa, informação tão sensível, à luz do respeito da privacidade, como o conteúdo das próprias comunicações.» [§ 99 do *Tele 2*. Veja-se ainda o §27 do *Digital Rights*].

12. Porém, e assentes estes pontos, o TJUE não deixou de salientar que esta ingerência grave em direitos fundamentais (que a *obrigação de conservação de dados* só

por si constituía) fora prevista para responder a um legítimo objetivo de interesse geral. Recordando que o artigo 6.º da Carta enunciava tanto o direito das pessoas à liberdade quanto o seu direito à segurança; que o acesso das autoridades públicas nacionais aos dados conservados forneceria um contributo não despiciendo «para a luta contra a criminalidade grave» e contra o «terrorismo internacional»; e que o combate a este último se apresentava também como «um objectivo de interesse geral da União» [§41 e 42 do *Digital Rights*], o Tribunal concluiu que a medida – a *obrigação de conservação de dados* – se traduzia, não na aniquilação do conteúdo essencial de direitos e liberdades fundamentais, mas numa *restrição* daquele mesmo conteúdo, no sentido que ao termo "restrição" era dado pelo artigo 52.º da Carta. E como este último preceito consentia as restrições desde que estas fossem «previstas por lei» e ordenadas com «observância do princípio da proporcionalidade», o TJUE passou a averiguar se as normas sob juízo satisfariam, ou não, estas duas exigências.

A averiguação foi feita, no *Digital Rights,* a partir do seu § 45; e no *Tele 2,* a partir do § 94.

13. O percurso argumentativo seguido, a partir daqui, pelo Tribunal, teve naturalmente desfechos diferentes num caso e noutro. No *Digital Rights,* culminou com a declaração de invalidade da Diretiva 2006/24/CE. No *Tele 2,* culminou com a interpretação do n.º 1 do artigo 15.º da Diretiva 2002/58/CE. Assim, enquanto a primeira decisão teve por efeito a «destruição» de um certo ato [a directiva declarada inválida], a segunda teve por efeito a identificação dos critérios que deveriam ser seguidos por quaisquer leis nacionais que quisessem neste domínio, conformar-se com o Direito da União, fosse ele originário ou derivado.

Todavia, esta diversidade de efeitos (que decorre da diversidade, num caso e noutro, do objecto do processo) não impede que se continue a ler os dois arestos de forma integrada e conjunta. É que foi sobretudo aqui, no momento culminante de realização do juízo de proporcionalidade, que se tornou bem patente a

complementaridade existente entre as duas decisões: o *Digital Rights* enunciou a este propósito fundamentos e critérios que serão depois mantidos, esclarecidos e desenvolvidos pelo Acórdão *Tele 2,* numa continuidade de pensamento jurisprudencial que não pode deixar de ser considerada.

14. Subjacente a esta continuidade está um certo entendimento, que em ambos os casos o Tribunal mantém, sobre o significado a atribuir à primeira exigência constante do n.º 1 do artigo 52.º da Carta, a saber, a exigência segundo a qual *devem ser previstas por lei* todas as *restrições* aos direitos fundamentais nela [na Carta] consagrados.

Nas duas decisões o Tribunal «lerá» sempre este requisito à luz de critérios *materiais* e não apenas formais. Quer isto dizer que, de acordo com a jurisprudência do TJUE, não basta à lei restritiva ser, formalmente, «acto legislativo»; mais se lhe exige que o seja materialmente, por conter uma disciplina normativa *suficientemente precisa e específica,* de forma a que todos – privados e autoridades públicas – possam saber de antemão quais os direitos que são restringidos e qual a amplitude da restrição, adequando assim os seus comportamentos e funções às exigências legais (§ 54 do *Digital Rights* e § 105 do *Tele 2*).[6]

Da adoção deste entendimento substancial ou material do conceito de «lei restritiva» decorrerão consequências importantes para o juízo de proporcionalidade que é feito pelo TJUE em ambos os arestos. Tanto no caso do *Digital Rights* quanto no caso do *Tele 2,* dirá o Tribunal que, sendo embora em si mesma adequada ao fim legítimo que se propunha realizar – o combate à criminalidade grave – a medida da *obrigação de conservação dados* não era, no entanto, necessária (nem proporcional em

[6] Veja-se também o ponto 139 das Conclusões do Advogado Geral Henrik Saugmandsguaard, apresentadas a 19 de julho de 2016 nos processos que darão origem ao Acórdão *Tele 2.* Aí se salienta que esta interpretação material do conceito de «lei restritiva» é também a seguida por jurisprudência, abundantemente identificada, do Tribunal Europeu dos Direitos do Homem.

sentido estrito), por existirem à disposição do legislador outros meios, aptos à realização do mesmo fim, menos lesivos dos direitos fundamentais tutelados pela Carta. É esta a posição de princípio do TJUE, expressa nos §§ 45 e seguintes do *Digital Rights* e nos §§ 94 e seguintes do *Tele 2*. Todavia, como o juízo sobre a desproporcionalidade da medida, com a sua estrutura de demonstração da sua desnecessidade e da sua «desproporção em sentido estrito», se associa estreitamente à noção material de reserva de lei a que acima se fez referência, todos, ou quase todos, os argumentos que o Tribunal apresenta para justificar ou precisar as suas conclusões sobre a [ausência de] proporcionalidade acabarão por ser argumentos de teor negativo. Acabarão por incidir, não tanto sobre o que a «lei restritiva» disse ou dispôs, mas sobre aquilo que ela, em especificação deficiente, deixou de dizer, de regular ou de dispor.

15. Uma tal argumentação negativa aplicá-la-á o Tribunal a propósito dos três principais problemas colocados pela regulação em causa, problemas esses já atrás identificados: por um lado, *o âmbito da obrigação da conservação de dados;* por outro, *o regime de acesso aos dados conservados;* e, por fim, *a segurança e a protecção dos dados conservados.* Além disso, e como «lei restritiva», na aceção atrás referida, seriam (de acordo com o Tribunal) todos os actos normativos que se lhes referissem – fossem eles actos da União, fossem eles atos dos Estados-Membros em aplicação do Direito da União – a dita argumentação negativa, decorrente da ideia material da reserva de lei, acabou por fundar, não apenas a declaração de invalidade da Diretiva 2006/24/CE levada a cabo pelo *Digital Rights,* mas ainda a interpretação do n.º 1 do artigo 15.º da Diretiva 2002/58/CE fixadas no *Tele 2,* com todas as consequências daí [dessa interpretação] decorrentes para os direitos internos que viessem a «aplicar» a norma interpretada pelo Tribunal.

16. Assim, e quanto ao *âmbito da obrigação de conservação de dados,* o Tribunal considerou desproporcionada toda a regulamentação que previsse «uma conservação generalizada e indiferenciada de todos os dados de tráfego e dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica» (§ 112 do *Tele* 2) por entender 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» (idem, § 106; vejam-se ainda os §§ 58 e 59 do *Digital Rights*).

Depois, e quanto ao *regime de acesso aos dados conservados,* disse o Tribunal que tal acesso só seria justificado se servisse apenas a prevenção e repressão da criminalidade grave, nos termos a definir por cada direito interno; que, por isso, a informação deveria ser – ainda nos termos a estabelecer por cada legislador nacional – reservada às autoridades competentes para levar cabo tal repressão; e que se estas últimas deveriam poder aceder aos dados nos termos de um procedimento que integrasse um controlo prévio, a efetuar por um órgão jurisdicional ou por uma autoridade administrativa independente (§ 117 a 121 do *Tele 2*; § 61 a 62 do *Digital Rights*)[7].

Finalmente, e quanto à *segurança e protecção dos dados conservados,* o Tribunal, tendo em conta o risco de acesso ilícito aos mesmos, bem como a sua «quantidade e sensibilidade», deixou claro que aos direitos internos caberia definir os termos,

[7] Como é evidente, os §§ 117 a 121 do *Tele 2* identificaram as exigências a seguir por parte dos direitos internos que se quisessem conformes com o Direito da União (originário e derivado). Finalidade diferente serviram os argumentos dos §§ 61 e 62 do *Digital Rights,* onde a falta de clareza e especificação das regras (relativas ao acesso) foram uns dos argumentos fundantes do juízo de invalidade da diretiva de 2006.

exigentes, nos quais os serviços de comunicações electrónicas seriam obrigados a assegurar a plena integridade e confidencialidade dos dados, e a adotar medidas técnicas e de organização adequadas para «garantir um nível particularmente elevado de protecção e segurança» (§ 122 do *Tele 2)*. Entre tais medidas o Tribunal salientou duas: (i) os dados deveriam ser conservados em território da União; (ii) os direitos internos deveriam atribuir a uma entidade independente a competência para controlar o cumprimento, por parte dos serviços de comunicação electrónica, dos seus deveres de garantia da «integridade» e «confidencialidade» dos dados conservados §§ 112 e 113 do *Tele 2*)[8].

III

As consequências para o direito interno

17. A Lei n.º 32/2008, de 17 de julho, transpôs para a ordem jurídica interna a Diretiva 2006/24/CE. O facto de tal diretiva ter sido invalidade pelo Tribunal de Justiça da União não impede, porém, que se considere que o regime português relativo à «conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações», que aquela lei visa instituir, é ainda um regime definido pelos órgãos legislativos da República *em aplicação do Direito da União.* Com efeito, e

[8] E § 67 e 68 do *Digital Rights,* onde, uma vez mais, a ausência de previsão destas salvaguardas foi fundamento para a declaração o de invalidade da Diretiva de 2006.

neste domínio, a lei portuguesa continua a ser adoptada nos termos da possibilidade aberta pelo n.º 1 do artigo 15.º da Diretiva 2002/58/CE do Parlamento e do Conselho, de 12 de julho de 2002.

18. Assim sendo, sobre o legislador nacional impende o dever de reavaliar se o regime inscrito neste seu acto se mostra ou não conforme com as exigências decorrentes da Carta dos Direitos Fundamentais da União, de acordo com a interpretação que a tais exigências foi dada pela jurisprudência, que vimos analisando, do Tribunal de Justiça.

19. Ora, a este propósito, se parece claro que a Lei n.º 32/2008 se conforma com tais exigências em tudo o que diz respeito ao *regime de acesso aos dados conservados* – por exigir que tal acesso sirva o propósito estrito da prevenção e repressão da criminalidade grave; por definir em que consiste tal criminalidade; por reservar o acesso às autoridades competentes; por prever para tanto um procedimento que integra necessidade de prévia autorização jurisdicional – também parece claro que tal lei se não conforma com as exigências decorrentes do Direito da União, tal como foram elas interpretadas pelo TJUE, em tudo o que diz respeito ao *âmbito da obrigação da conservação de dados.*

20. Com efeito, e neste último domínio, o legislador português acolhe a solução que, expressamente, o Tribunal de Justiça censurou: prevê a 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 eletrónica, sem limitar tal obrigação em função dos critérios indicados pelo TJUE nos termos do § 106 e seguintes do Acórdão *Tele 2*.

21. A este facto, um outro acresce, relativo à *segurança e protecção dos dados conservados*. Por um lado, a lei portuguesa não obriga a que os dados sejam conservados em território da União, em contradição com o que decorre da interpretação feita pelo TJUE quanto ao sentido do n.º 1 do artigo 15.º da diretiva de 2002; por outro, o estado actual de aplicação prática da lei é tal que fundados receios existem de que, neste domínio – no domínio da segurança e protecção de dados – se não estejam a cumprir as exigências decorrentes da Carta, tal como elas foram interpretadas pela jurisprudência pertinente do TJUE.

22. Recorde-se que tais exigências se traduziam: (i) no dever de assegurar, ao nível nacional, que os serviços de comunicações eletrónicas, adoptassem medidas técnicas e de organização adequadas para «garantir um nível particularmente elevado de protecção e segurança»; (ii) no dever de identificar, ainda ao nível nacional, a entidade independente capaz de controlar e fiscalizar, neste domínio, a atuação dos operadores das comunicações electrónicas.

23. Ora, como já se disse (cfr. *supra,* ponto 10), a Lei n.º 32/2008 identificou a Comissão nacional de Protecção de Dados [CNPD] como sendo a autoridade pública competente para o controlo da aplicação das regras relativas à segurança e proteção de dados (artigo 7.º, n.º 3), conferindo-lhe ainda a competência para a instrução dos processos de contra-ordenação e para a aplicação das correspondentes coimas (artigo 14.º da Lei n.º 32/2008).

24. Todavia, através da Deliberação nº 1008/2017, de 18 de julho, a CNPD resolveu «desaplicar aquela lei [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». O dado é relevante, na exata medida em que é legítimo pensar-se que, por causa dele, podem agora os operadores de serviços de telecomunicações não dispor de qualquer desincentivo para incumprir as obrigações que sobre eles impendem, as quais – de acordo com o Direito da União – deveriam corresponder às exigências de garantia de um «nível particularmente elevado de protecção e segurança».

25. Perante todos estre dados, penso, Senhora Ministra da Justiça, que urge promover a reforma da Lei n.º 32/2008, de 17 de julho, de modo a que o regime nela fixado se conforme com o Direito, originário e derivado, da União. Na verdade, a garantia de uma tal conformidade é um dever constitucionalmente assumido pela República; e, embora cabendo o cumprimento de tal dever ao legislador parlamentar, não ignoro que a iniciativa de lei, pela incidência que tem em várias áreas da política de investigação criminal, melhor caberá ao Executivo de que Vossa Excelência faz parte.

26. Do mesmo modo não ignoro que é também dever do legislador – *recte,* que é primacialmente dever do legislador – cumprir as exigências decorrentes da Constituição; e que, nos domínios de que me venho ocupando, existe uma natural

convergência axiológica entre as disposições da Carta dos Direitos Fundamentais da União e as normas jusfundamentais da Constituição da República. O direito à reserva da vida privada; o direito à proteção de dados pessoais; a liberdade de expressão – enfim, todos os valores pelos quais o TJUE orientou a jurisprudência que venho de analisar e expor – são valores igualmente, ou até superiormente, tutelados pela ordem constitucional portuguesa.

27. Todavia, o Tribunal Constitucional, decidindo em processo de fiscalização concreta (Acórdão n.º 420/2017), não julgou inconstitucional «a norma que estabelece o dever de os fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações conservarem pelo período de um ano a contar da data da conclusão da comunicação os dados relativos ao nome e ao endereço do assinante ou do utilizador registado, a quem o endereço do protocolo IP estava atribuído no momento da comunicação».

28. Uma vez que o Tribunal, em juízo que teve como parâmetro exclusivo as normas da Constituição da República, entendeu que, *neste caso,* por estar em causa um «dado de rede», não havia nem violação do disposto no n.º 4 do artigo 34.º da CRP, nem restrição desproporcionada da reserva de vida privada, nada parece impedir que, em outro caso, estando em causa um outro dado, o Tribunal conclua pela inconstitucionalidade das normas constantes da Lei n.º 32/2008.

29. Creio no entanto que, perante um regime jurídico como aquele que tal lei dispõe, que visa, como o afirmou o Tribunal de Justiça da União, a prossecução de um legítimo objetivo de interesse geral, melhor será que o legislador previna a sua

invalidação por intermédio da competência estritamente cassatória do Tribunal Constitucional., adequando-o desde já às exigências decorrentes dos direitos fundamentais.

Eis as razões pelas quais, Senhora Ministra da Justiça, a Vossa Excelência dirijo esta recomendação.

Apresento-lhe, Senhora Ministra, os meus melhores cumprimentos.

A Provedora de Justiça

(*Maria Lúcia Amaral*)