Duarte Rodrigues Nunes
Professor Associado na Universidade Europeia
Professor Associado Convidado na Universidade Lusíada de Angola
Doutor em Direito
Jurisconsulto
Conferencista

Observações ao Projeto de Lei n.º 70/XV/1.ª (PSD) e à Proposta de Lei n.º 11/XV/1.ª (GOV) quanto à conservação e ao acesso aos metadados para fins de investigação criminal

1. O Acórdão do Tribunal Constitucional n.º 268/2022: fundamentos da declaração de inconstitucionalidade:

A) Conservação dos dados de base:

- Falta de previsão da obrigatoriedade do armazenamento dos dados num Estado-Membro da União Europeia.

B) Conservação dos dados de tráfego e de localização:

- Falta de previsão da obrigatoriedade do armazenamento dos dados num Estado-Membro da União Europeia;
- Conservação de todos os dados de localização e de tráfego de todos os assinantes, abrangendo as comunicações eletrónicas da quase totalidade da população, incluindo pessoas relativamente às quais não há qualquer suspeita de atividade criminosa, e sem qualquer diferenciação, exceção ou ponderação face ao objetivo visado.

C) Transmissão dos dados conservados:

- Falta de previsão da obrigatoriedade da notificação das pessoas cujos dados relativos às suas comunicações foram transmitidos às autoridades públicas a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros.

2. O estado atual da jurisprudência do Tribunal de Justiça da União Europeia após o Acórdão *Digital Rights Ireland Ltd e Kärntner Landesregierung*, de 8 de abrik de 2014

Acórdão *Tele2 Sverige AB* (21/12/2016):

- A CDFUE proíbe a 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;
- A CDFUE impõe que os dados sejam conservados no território da União Europeia;
- A CDFUE apenas permite o acesso aos dados conservados para efeitos de luta contra a criminalidade grave e desde que esse acesso esteja sujeito a controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente.

Acórdão *Privacy International* (06/10/2020):

- A CDFUE proíbe a imposição aos prestadores de serviços de comunicações eletrónicas, para efeitos da salvaguarda da segurança nacional, da transmissão generalizada e indiferenciada de dados de tráfego e de dados de localização aos serviços de segurança e de informações

Acórdão *La Quadrature du Net* (06/10/2020):

- A CDFUE proíbe a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização a título preventivo, mas permite:
    - A conservação generalizada e indiferenciada de dados de tráfego e de dados de localização para salvaguarda da segurança nacional, quando o Estado-Membro em causa enfrente uma ameaça grave e que seja real e atual ou previsível, desde que a decisão que prevê tal imposição possa ser objeto de fiscalização efetiva (por um órgão jurisdicional ou por uma entidade administrativa independente), cuja decisão produza efeitos

vinculativos, e essa conservação apenas ocorra durante um período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça;

- A conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, desde 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;
- A conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública.

Acórdão *Prokuratuur* (02/03/2021):

- A CDFUE proíbe o acesso de autoridades públicas a dados de tráfego ou de localização para fins de prevenção, investigação, deteção e perseguição de infrações penais, sem que esse acesso esteja circunscrito a processos que visem a luta contra a criminalidade grave ou a prevenção de ameaças graves à segurança pública, independentemente da duração do período em relação ao qual o acesso aos referidos dados é solicitado e da quantidade ou da natureza dos dados disponíveis sobre tal período;
- A atribuição da competência ao MP para autorizar o acesso aos dados de tráfego e aos dados de localização para fins de investigação criminal viola a CDFUE, dado que a missão do MP é dirigir a instrução do processo penal e exercer a ação penal.

Acórdão *G. D. e Commissioner of An Garda Síochána* (05/04/2022):

- A CDFUE proíbe a conservação generalizada e indiferenciada de dados de

tráfego e de dados de localização a título preventivo para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, mas permite:

- A conservação seletiva de dados de tráfego e de dados de localização, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional, 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;
- A conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional, por um período temporalmente limitado ao estritamente necessário;
- A conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional,

desde que esteja assegurado, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e as pessoas visadas disponham de garantias efetivas contra os riscos de abuso.

Acórdão *SpaceNet* (20/09/2022):

- A CDFUE proíbe a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização a título preventivo para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, mas permite:

- A conservação generalizada e indiferenciada de dados de tráfego e de dados de localização para salvaguarda da segurança nacional, quando o Estado-Membro em causa enfrente uma ameaça grave e que seja real e

atual ou previsível, desde que a decisão que prevê tal imposição possa ser objeto de fiscalização efetiva (por um órgão jurisdicional ou por uma entidade administrativa independente), cuja decisão produza efeitos vinculativos, e essa conservação apenas ocorra durante um período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça;

- A conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, desde 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;
- A conservação generalizada e indiferenciada dos endereços IP atribuídos à fonte de uma ligação, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional, por um período temporalmente limitado ao estritamente necessário;
- A conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública,

desde que esteja assegurado, mediante regras claras e precisas, que a conservação dos dados em causa está sujeita ao respeito das respetivas condições materiais e processuais e as pessoas visadas disponham de garantias efetivas contra os riscos de abuso.

Em suma:

Quanto à conservação:

- A CDFUE proíbe a conservação generalizada e indiferenciada de dados de tráfego e de dados de localização a título preventivo para efeitos da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública;
- A CDFUE permite:

  - A conservação generalizada e indiferenciada de dados de tráfego e de dados de localização para salvaguarda da segurança nacional, quando o Estado-Membro em causa enfrente uma ameaça grave, real e atual ou previsível, desde que essa conservação apenas ocorra durante um período temporalmente limitado ao estritamente necessário, mas renovável em caso de persistência dessa ameaça, contanto que a decisão que determina a conservação seja efetivamente fiscalizada por um órgão jurisdicional ou por uma entidade administrativa independente, cuja decisão produza efeitos vinculativos;

  - A conservação seletiva dos dados de tráfego e dos dados de localização, para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade grave e da prevenção de ameaças graves contra a segurança pública, desde 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;

  - A conservação generalizada e indiferenciada, *mas por um período temporalmente limitado ao estritamente necessário*, dos endereços IP atribuídos à fonte de uma ligação, para efeitos de luta contra a criminalidade grave e de salvaguarda da segurança nacional;

  - A conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos (dados de base), para efeitos da salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública; e

- A CDFUE impõe que os dados sejam conservados no território da União Europeia.

Quanto ao acesso:

- A CDFUE apenas permite o acesso aos dados conservados para efeitos de luta contra a criminalidade grave e desde que esse acesso esteja sujeito a controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente (que não inclui o MP, pois é o titular da ação penal).

3. A jurisprudência do Tribunal Europeu dos Direitos Humanos

   Acórdão Big Brother Watch e Outros c. Reino Unido (GC) (25/05/2021):

   - A interceção massiva (e, como tal, generalizada e indiferenciada) de dados de conteúdo de comunicações (sob a forma de dados informáticos) e de dados de tráfego (*bulk interception*), por si só, não viola o art. 8.º da CEDH, contanto que sejam observadas determinadas garantias mínimas;
   - A interceção massiva de dados de conteúdo de comunicações (sob a forma de dados informáticos) e de dados de tráfego passa por 4 fases:
     1. Interceção e conservação dos dados informáticos relativos ao conteúdo de comunicações eletrónicas (dados de conteúdo) e dos dados relativos a comunicações (dados de tráfego);
     2. Tratamento e seleção, de forma automatizada e com e utilização de critérios de seleção, dos dados de conteúdo e de tráfego previamente conservados;
     3. Exame, por analistas, dos dados de conteúdo e de tráfego previamente selecionados; e
     4. Ulterior conservação dos dados considerados relevantes após o respetivo exame e utilização desses dados, incluindo no que tange à sua partilha com outras entidades (nacionais ou estrangeiras).

- No caso da vigilância generalizada e indiferenciada (e que, por isso, não tem alvos determinados e delimitados), como é o caso da interceção massiva de dados de conteúdo e de dados de tráfego, as salvaguardas são ainda mais fundamentais do que no caso da vigilância dirigida a pessoas determinadas (e, como tal, seletiva e não generalizada e indiferenciada);
- Na medida em que a interceção massiva de dados de conteúdo e de dados de tráfego, pela sua própria natureza, é, por um lado, preventiva e prévia à existência de qualquer *notitia criminis* ou ao conhecimento da existência de uma ameaça concreta à segurança nacional e, por outro lado, generalizada e indiferenciada (e não seletiva), não é possível aplicar-lhe duas das seis salvaguardas mínimas exigidas pelo TEDH no seu *case law* relativo às medidas de vigilância seletivas (*v.g.*, as escutas telefónicas): delimitação, pelo legislador, de um catálogo de crimes e de alvos e exigência da ocorrência de uma suspeita fundada da prática de um crime do catálogo;
- No entanto, ainda assim terão de ser existir salvaguardas mínimas no Direito interno dos Estados para que a interceção massiva de dados de conteúdo e de dados de tráfego observe as exigências do art. 8.º da CEDH, mais concretamente:
    - O Direito interno deverá prever, de forma clara, as circunstâncias em que as autoridades poderão lançar mão da interceção massiva de dados de conteúdo e de dados de tráfego, a duração da execução da medida, o procedimento relativo ao exame, utilização e conservação dos dados recolhidos, as precauções a observar relativamente à transmissão dos dados a outras entidades e em que circunstâncias os dados deverão ser apagados ou destruídos;
    - Em face do carácter necessariamente secreto da interceção massiva de dados de conteúdo e de dados de tráfego (sob pena de inutilidade), a supervisão e o controlo efetivos (por uma entidade independente do poder executivo, que não é forçoso que seja um Juiz) da implementação da medida em todas as fases suprarreferidas (e não apenas em matéria de

autorização do recurso à medida e da sua renovação) é absolutamente essencial para evitar abusos, incluindo no que tange à necessidade e à proporcionalidade do recurso à interceção em massa no caso concreto;

- O Direito interno deverá prever mecanismos que permitam às pessoas que suspeitem de que os seus dados foram alvo de interceção em massa contestar, de forma efetiva e não meramente aparente, a legalidade da medida e/ou a conformidade do regime da interceção em massa à CEDH, sem dependência de uma qualquer notificação de que os seus dados foram alvo da medida; para tal, a entidade competente para apreciar a impugnação deverá ser independente do poder executivo (mas não tendo de ser necessariamente um Tribunal) e o procedimento terá de ser equitativo, que deverá incluir a possibilidade de contraditório (na medida do possível) e a fundamentação da decisão, que deverá ser juridicamente vinculativa para o poder executivo, ao ponto de poder determinar a cessação de uma interceção ilegal e a destruição dos dados obtidos ou conservados de forma ilegal.

O TEDH tem considerado que a proteção dos direitos fundamentais inclui o dever de as autoridades levarem a cabo uma investigação efetiva e eficaz (no sentido de serem utilizados meios de investigação que se mostrem necessários para investigar no caso concreto) em ordem a investigar os crimes que atinjam algum dos direitos fundamentais garantidos pela CEDH, desde logo no caso de homicídios, tendo em conta o disposto no artigo 2.º da CEDH (cfr. Acórdãos McCann e Outros c. Reino Unido, Mahmut Kaya c. Turquia, Hugh Jordan c. Reino Unido, Paul e Audrey Edwards c. Reino Unido, Nachova e Outros c. Bulgária, Kaya e Outros c. Turquia, Ramsahai e Outros c. Países Baixos, Angelova e Iliev c. Bulgária, Opuz c. Turquia, Kolevi c. Bulgária, Al-Skeini e Outros c. Reino Unido, Vasîlka c. Moldávia, Jaloud c. Países Baixos, Mustafa Tunç e Fecire Tunç c. Turquia e Armani da Silva c. Reino Unido, todos acessíveis em *https://hudoc.echr.coe.int/*).

No que concerne à obtenção de metadados numa investigação criminal, o TEDH considerou que a não obtenção de metadados que se mostre necessária para uma determinada investigação criminal de crimes cometidos através da Internet ou com utilização da Internet (*v. g.*, divulgação de vídeos anteriormente obtidos através de uma câmara oculta colocada no domicílio da vítima, permitindo a obtenção dos metadados identificar o autor da publicação e, eventualmente, o autor das gravações ilícitas) é incompatível com o artigo 8.º da CEDH (que também inclui um dever positivo de as autoridades levarem a cabo uma investigação efetiva e eficaz relativamente a crimes que lesem os direitos fundamentais tutelados por esse preceito da CEDH) se essa não obtenção puser em causa a eficácia dessa mesma investigação [cfr. Acórdãos K.U. c. Finlândia, Khadija Ismayilova c. Azerbaijão e Volodina c. Rússia (N.º 2)].

Aliás, no Acórdão K.U. c. Finlândia é particularmente evidente a censura do TEDH à excessiva importância que foi atribuída pelas autoridades finlandesas à confidencialidade dos dados de tráfego dos internautas face à necessidade de identificar o indivíduo que publicou um anúncio na Internet, desse modo tornando um menor em alvo de abordagens de pedófilos, sendo que a lei finlandesa em vigor, que visava proteger a liberdade de expressão e o direito à expressão anónima e protegia os autores de mensagens anónimas na Internet, impedia as autoridades de, numa tal situação, imporem ao fornecedor de serviços o fornecimento de metadados que permitissem a identificação do agente da infração, o que votara ao insucesso a investigação que fora aberta.

4. O legislador português entre a espada e a parede

Transpondo a jurisprudência do TEDH para a realidade portuguesa:

a) A conservação generalizada e indiferenciada de dados de tráfego e de dados de localização só é admissível se existir uma ameaça grave, real e atual ou previsível à segurança nacional (o que é mais restritivo do que a luta contra a criminalidade grave) e apenas enquanto essa ameaça persistir;
b) A conservação generalizada e indiferenciada dos endereços de IP só é admissível por um período temporalmente limitado, ainda que renovável, e

para salvaguarda da segurança nacional ou luta contra a criminalidade grave (o que inclui a prevenção e a repressão);

c) É admissível a conservação seletiva de dados de tráfego e dos dados de localização, para a salvaguarda da segurança nacional, luta contra a criminalidade grave e prevenção de ameaças graves contra a segurança pública, desde 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;
d) É admissível a conservação generalizada e indiferenciada de dados relativos à identidade civil dos utilizadores de meios de comunicações eletrónicos, para salvaguarda da segurança nacional, da luta contra a criminalidade e da salvaguarda da segurança pública;
e) Os dados têm de ser conservados no território da União Europeia;
f) É admissível a utilização dos dados conservados para efeitos de luta contra a criminalidade grave e desde que esse acesso esteja sujeito a controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente, não bastando a autorização do MP.

Contudo, se, por um lado, a CDFUE, de acordo com a interpretação dos arts. 7.º, 8.º e 52.º tal como levada a cabo pelo TJUE, são estes os limites (muito apertados), por outro lado, a CEDH, tal como interpretada pelo TEDH, além de, inclusivamente no caso de interceções em massa (inclusive de dados informáticos relativos a dados de conteúdo de comunicações) – que inclui o tratamento em massa dos dados conservados com base em critérios de pesquisa e não apenas o acesso a metadados relativos ao arguido, suspeito, intermediário ou vítima mediante o respetivo consentimento – não impor restrições tão intensas como o TJUE, ainda impõe que sejam utilizados meios de investigação que se mostrem necessários para investigar no caso concreto em ordem a investigar, com eficácia e efetividade, os crimes que atinjam algum dos direitos fundamentais garantidos pela CEDH, tendo condenado a Finlândia pelo facto de a Lei finlandesa não prever a

conservação de metadados, o que impedia a obtenção de metadados que permitissem identificar o agente de crimes informáticos contra um menor.

Relativamente às relações entre a CDFUE (tal como interpretada pelo TJUE) e a CEDH (tal como interpretada pelo TEDH), há que ter em conta as seguintes normas:

a) Artigo 53.º da CDFUE: «*Nenhuma disposição da presente Carta deve ser interpretada no sentido de restringir ou lesar os direitos do Homem e as liberdades fundamentais reconhecidos, nos respetivos âmbitos de aplicação, pelo direito da União, o direito internacional e as Convenções internacionais em que são Partes a União ou todos os Estados-Membros, nomeadamente a Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, bem como pelas Constituições dos Estados-Membros*»;

b) Artigo 6.º, n.ºs 2 e 3, do TUE:

«(...) 2. A União adere à Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. Essa adesão não altera as competências da União, tal como definidas nos Tratados.

3. Do direito da União fazem parte, 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».

c) Ainda que, formalmente, a UE não tenha aderido à CEDH e, pelo menos, as versões inglesa e espanhola refiram que a UE "aderirá" e que os direitos fundamentais garantidos pela CEDH "farão parte" do Direito da União Europeia enquanto princípios gerais de direito, pelo menos nas versões portuguesa, italiana, alemã e francesa (e cada versão oficial numa das línguas oficiais da UE valem por si mesmas), refere-se que a UE "adere" e que os direitos fundamentais garantidos pela CEDH "fazem parte" do Direito da União Europeia enquanto princípios gerais de direito.

d) Por isso, do ponto de vista material, tendo em conta, não apenas o art. 6.º, n.ºs 2 e 3, do TUE, mas sobretudo o art. 53.º da CDFUE, a UE aderiu mesmo

à CEDH ou, pelo menos, está vinculada à CEDH e os direitos fundamentais garantidos pela CEDH tal como interpretados pelo TEDH integram o Direito da União Europeia;

e) Deste modo, a CEDH, tal como interpretada pelo TEDH, prevalece sobre a CDFUE e a jurisprudência do TJUE, que cedem igualmente perante a CRP nos casos em que esta conceda uma melhor proteção dos direitos fundamentais, havendo que relembrar que a prevenção e a repressão de crimes graves é justificada e até imposta enquanto forma de proteção dos bens jurídico-penais e, consequentemente, de direitos fundamentais.

5. Apreciação crítica do Projeto de Lei n.º 70/XV/1.ª (PSD) e da Proposta de Lei n.º 11/XV/1.ª (GOV)

5.1. Artigos 2.º e 15.º da Lei n.º 32/2008

Concordo com a atualização dos arts. 2.º, n.º 2, e 15.º tendo em conta a ulterior entrada em vigor do RGPD e a revogação da Lei n.º 67/98, de 26 de outubro, pela Lei n.º 58/2019, de 8 de agosto.

5.2. Artigo 4.º da Lei n.º 32/2008

Concordo com a exigência de que a conservação dos dados tenha lugar em Portugal ou no território de outro Estado-Membro da União Europeia, pois desse modo são cumpridas, sem qualquer margem para dúvidas, as exigências do TC e do TJUE sem qualquer prejuízo para a investigação da criminalidade grave.

Ao ser mantido, quanto ao mais, o disposto no art. 4.º da Lei n.º 32/2008, não está a ser observada nem a jurisprudência do TC nem a jurisprudência do TJUE, visto que se trata de uma conservação generalizada e indiferenciada.

No entanto, por um lado, a conservação – para ulterior utilização, se necessário – de metadados é essencial para responder à criminalidade grave (o que torna constitucionalmente ilegítima a impossibilidade dessa conservação) e, por outro, as

exigências colocadas pelo TJUE e pelo TC são impossíveis de cumprir, são de difícil (ou mesmo impossível) determinação e, mais do que isso, abrem as portas à discriminação.

São impossíveis de cumprir porque conservação de metadados é uma medida de prevenção criminal que se integra na chamada investigação proativa e ocorre, por natureza, num momento prévio à obtenção da notícia do crime: e, por isso, é *impossível* definir um qualquer critério delimitador dos metadados a conservar e, ainda que fosse possível, tal critério sempre violaria os princípios da proibição da discriminação e da presunção de inocência.

São de difícil (ou mesmo impossível) determinação, pois, ainda que o TJUE esclareça que a preservação da segurança nacional corresponde ao interesse primordial de proteger as funções essenciais do Estado e os interesses fundamentais da sociedade, através da prevenção e da repressão de atividades suscetíveis de desestabilizar gravemente as estruturas constitucionais, políticas, económicas ou sociais fundamentais de um país, em especial de ameaçar diretamente a sociedade, a população ou o Estado enquanto tal e dá o exemplo do terrorismo, fica por saber, por exemplo, se tal também inclui a criminalidade organizada, *maxime* as máfias e, na afirmativa, se inclui todos os casos de criminalidade organizada mafiosa ou apenas aqueles casos em que as máfias ameacem diretamente o Estado, os seus agentes e os cidadãos de uma forma generalizada (gerando um ambiente generalizado de medo), excluindo as situações em que isso não sucede ou tenha deixado de suceder.

E também são de difícil (ou mesmo impossível) determinação pelo facto de não vermos como é que, com base em elementos objetivos e não discriminatórios (e quais são ou poderão ser esses elementos), em função das categorias de pessoas em causa ou através de um critério geográfico, será possível definir um qualquer critério delimitador dos metadados a conservar e, sobretudo, fazê-lo sem violar a presunção de inocência e a proibição de discriminação.

E abrem as portas à discriminação na medida em que a limitação da conservação de dados em função das categorias de pessoas (v.g., indivíduos com antecedentes criminais ou com antecedentes criminais de uma determinada tipologia, indivíduos oriundos de países ou de regiões conotadas com determinadas atividades criminosas ou

que desempenham uma determinada atividade profissional ou económica conotada com certas atividades criminosas) ou de um critério geográfico (v.g., os habitantes de uma determinada região, de uma determinada localidade, de parte de uma localidade ou de um bairro) encerra um enorme risco de discriminação dos visados face aos não visados, inclusivamente no que tange à presunção de inocência e não apenas no que concerne ao tratamento informático de dados relativos à vida privada *ex se*.

O entendimento do TJUE parece mesmo ignorar o facto de a criminalidade organizada, o terrorismo, o cibercrime e criminalidade económico-financeira serem formas de criminalidade tendencialmente e em muitos casos (porventura na maioria dos casos) transnacional, podendo a atividade criminosa desenvolver-se no território de dois ou mais Estados, podendo ser um ou alguns deles Estados-Membros da UE e os demais Estados não-membros da UE, mas aos quais o ou os Estados-Membros da UE deva prestar cooperação no âmbito, desde logo, de instrumentos de Direito internacional extracomunitários, como instrumentos de prevenção e repressão da criminalidade adotados no âmbito da ONU ou do Conselho da Europa.

Além disso, o TJUE também parece olvidar que a atividade criminosa pode ser levada a cabo ou as suas consequências danosas podem verificar-se no Estado A, mas os criminosos utilizarem o Estado B como base de operações ou como ponto de recuo depois do cometimento dos crimes ou praticarem no Estado B os atos preparatórios ou de execução dos crimes cujas consequências se verificam no Estado A. Do mesmo modo, as ações de prevenção criminal relativamente a crimes que virão ou poderão vir a ser cometidos no Estado A podem ter de ser ou podem ter de ser também levadas a cabo no Estado B.

Por fim, a impossibilidade de conservação dos metadados é inconstitucional, porquanto dessa impossibilidade resulta ou pode resultar uma proteção insuficiente dos direitos fundamentais que se concretizam nos bens jurídico-penais tutelados pelos crimes constantes do catálogo do artigo 2.º, n.º 1, alínea g), da Lei n.º 32/2008 ao dificultar de sobremaneira a resposta à criminalidade grave (*maxime* a criminalidade organizada, o terrorismo, a criminalidade económico-financeira, a criminalidade violenta, a criminalidade sexual e o cibercrime), pois impedirá – caso não seja possível encontrar no

Direito vigente uma via alternativa – a conservação preventiva dos metadados e o acesso aos mesmos ou a valoração das provas já obtidas no âmbito dos processos em curso, podendo abrir a porta a insustentáveis situações de impunidade com a absolvição de criminosos.

E, ainda que existam caminhos alternativos no Direito vigente para a conservação dos metadados, é preferível, pois permite evitar quaisquer dúvidas, sobretudo quando a jurisprudência tem entendido que esses caminhos alternativos não são admissíveis em face do Acórdão do TC n.º 268/2022.

5.3. Artigo 6.º da Lei n.º 32/2008

Relativamente ao n.º 1 do art. 6.º, na medida em que se entende maioritariamente que o IP é um dado de base, talvez se justificasse inverter as als. b) e c).

Passando ao n.º 2 do art. 6.º, existe uma incongruência face aos arts. 6.º, n.º 3, e 7.º da Lei n.º 41/2004, de 18 de agosto, e 9.º, n.º 2 e 10.º. n.º 1, da Lei n.º 23/96 de 26 de julho, pois se os operadores de comunicações eletrónicas podem conservar os metadados por seis meses para cobrança dos serviços prestados, por maioria de razão, no caso da resposta à criminalidade grave, o prazo de conservação terá de ser, pelo menos, o mesmo.

Não faz sentido presumir o consentimento no sentido da prorrogação do prazo de conservação para 6 meses até porque, no nosso Direito, o consentimento presumido suscita-se em situações de perigo na demora e de impossibilidade de obter o consentimento expresso em tempo útil, sendo que não se verifica aqui qualquer situação dessa natureza.

Além disso, para que o consentimento possa ser presumido, é necessário que seja razoável supor que, em face das circunstâncias do caso concreto, o visado teria prestado consentimento se tivesse sido consultado e não me parece que seja possível formular uma tal suposição no que concerne à extensão do prazo de conservação de metadados.

Quanto aos n.ºs 3 e 6, não me parece que exista qualquer justificação para a atribuição da competência a um coletivo de Juízes do STJ: se um Tribunal de Comarca pode condenar em penas de 25 anos de prisão e um Juiz de 1.ª Instância pode determinar a prisão preventiva ou autorizar o recurso a meios de obtenção de prova muito mais

restritivos de direitos do que a conservação de metadados (que nem sequer restringe direitos fundamentais), não vejo qualquer razão para que tenham de intervir um coletivo de Juízes do STJ.

A lei nem sequer refere qual o número de Juízes, mas deduzo que sejam 3 (os dois presidentes das 2 secções criminais e um outro Juiz-Conselheiro das secções criminais nomeado pelo STJ).

De todo o modo, parecendo que a prorrogação prevista no n.º 3 dependerá da ocorrência de circunstâncias excecionais (como parece resultar do n.º 4), ao ponto de justificarem a intervenção do PGR, nesse caso, fará sentido que a prorrogação seja decidida pelo STJ, embora me pareça excessiva a intervenção de um coletivo, sobretudo quando a mera conservação não restringe quaisquer direitos fundamentais.

O n.º 5 do art. 6.º não me merece qualquer observação para além se justificar essa clarificação na lei.

5.4. Artigo 7.º da Lei n.º 32/2008

As alterações introduzidas parecem-me adequadas, existindo uma salutar preocupação em incrementar as garantias de inviolabilidade dos dados conservados.

5.5. Artigo 9.º da Lei n.º 32/2008

Sempre defendi que, apesar do art. 11.º, n.º 2, da Lei n.º 109/2009, o art. 9.º da Lei n.º 32/2008 foi revogado pelos arts. 12.º e ss. da Lei n.º 109/2009:

a) a regulamentação da obtenção de dados informáticos prevista na Lei n.º 109/2009 é muito mais detalhada do que a contida no art. 9.º da Lei n.º 32/2008;
b) O art. 9.º da Lei n.º 32/2008 é a concretização, na nossa ordem jurídica, do art. 4.º da Diretiva 2006/24/CE (que foi declarada nula pelo TJUE, além de a Diretiva deixar ao legislador de cada um dos Estados-Membros a escolha das condições de acesso a dados conservados), ao passo que os arts. 12.º a 16.º e 18.º da Lei n.º 109/2009 constituem a consagração, na nossa ordem

jurídica, dos arts. 16.º a 21.º da CCiber, que impõem obrigações de legislar muito mais especificadas do que o art. 4.º da Diretiva 2006/24/CE;

c) não vejo razão para, em matéria de dados de base e de localização, coexistirem dois regimes diversos de obtenção, consoante a mesma ocorra em tempo real (a que se aplicará o regime do art. 14.º da Lei n.º 109/2009, que, desde logo, não contém qualquer elenco de crimes ou de alvos nem exige autorização judicial prévia na fase de inquérito) ou incida sobre dados conservados (a que se aplicaria o art. 9.º da Lei n.º 32/2008), porquanto o facto de os dados terem sido conservados não aumenta a lesividade da sua transmissão;

d) e, pelas mesmas razões, mesmo no caso dos dados de tráfego, também não vemos razão para a coexistência de dois regimes diversos, consoante a obtenção ocorra em tempo real (a que se aplicará o regime do art. 18.º da Lei n.º 109/2009, cujo catálogo de crimes é muito mais vasto do que o do art. 2.º, n.º 1, al. g), da Lei n.º 109/2009) ou incida sobre dados conservados (a que se aplicará o art. 9.º da Lei n.º 32/2008).

Por isso, seria preferível introduzir melhoramentos na Lei n.º 109/2009 (por exemplo, introduzir o que consta dos n.ºs 7 a 9 do art. 9.º da Lei n.º 32/2008 nos arts. 14 e 18 da Lei n.º 109/2009 e clarificar a subsunção da obtenção dos dados de tráfego ao art. 18.º, n.º 2) em vez de estar a reformular o art. 9.º da Lei n.º 32/2008.

De todo o modo, a manter-se a reformulação do art. 9.º da Lei n.º 32/2008:

a) concordo com o aditamento daquilo que consta dos n.ºs 7 a 9 (a fim de observar a jurisprudência do TJUE e do TC), embora devesse aditar-se a possibilidade de protelar a comunicação também nos casos em que a mesma possa prejudicar outras investigações em curso;

b) no que tange ao n.º 2, tendo em conta o critério previsto nos arts. 268.º, n.º 2, e 269.º, n.º 2, do CPP, deveria prever-se a possibilidade de, em casos de perigo na demora, o pedido de acesso ser apresentado ao Juiz diretamente pela APC ou mesmo a possibilidade de a autorização ser concedida pelo MP, embora

com sujeição a ulterior ratificação *expressa* do Juiz (o que, a meu ver, não contradiz a jurisprudência do TJUE).

5.6. Artigos 16.º e 17.º da Lei n.º 32/2008

As alterações introduzidas parecem-me adequadas.