Coletânea da Jurisprudência

CONCLUSÕES DO ADVOGADO-GERAL
MANUEL CAMPOS SÁNCHEZ-BORDONA
apresentadas em 30 de março de 2023 [1]

Processo C-162/22

A. G.
sendo intervenientes:
Lietuvos Respublikos generalinė prokuratūra

[pedido de decisão prejudicial apresentado pelo Lietuvos vyriausiasis administracinis teismas (Supremo Tribunal Administrativo da Lituânia)]

«Reenvio prejudicial — Telecomunicações — Tratamento de dados pessoais — Diretiva 2002/58/CE — Âmbito de aplicação — Artigo 15.º, n.º 1 — Acesso aos dados conservados pelos prestadores de serviços de comunicações eletrónicas e recolhidos no âmbito de procedimentos de inquérito — Utilização posterior dos dados no inquérito relativo a uma infração disciplinar»

1. Em síntese, este reenvio prejudicial suscita a questão de saber se determinados dados pessoais obtidos durante um inquérito penal podem ser utilizados, posteriormente, num processo de natureza administrativa instaurado contra um funcionário público.

2. A resposta a esta questão dá ao Tribunal de Justiça uma nova oportunidade para se pronunciar sobre os âmbitos de aplicação, respetivamente, da Diretiva 2002/58/CE [2], por um lado, e da Diretiva (UE) 2016/680 [3] e do Regulamento (UE) 2016/679 [4], por outro.

3. No que se refere à Diretiva 2002/58, o Tribunal de Justiça tem uma jurisprudência firme sobre os casos e as condições em que os Estados-Membros podem restringir o âmbito dos direitos e obrigações que prevê [5].

1 Língua original: espanhol.

2 Diretiva 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) (JO 2002, L 201, p. 37).

3 Diretiva do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO 2016, L 119, p. 89).

4 Regulamento do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO 2016, L 119, p. 1); a seguir «RGPD».

5 Sem intenção de exaustividade, entre os exemplos principais dessa jurisprudência refiram-se os Acórdãos de 8 de abril de 2014, Digital Rights Ireland e o. (C-293/12 e C-594/12, EU:C:2014:238), de 21 de dezembro de 2016, Tele2 Sverige e Watson e o. (C-203/15 e C-698/15, EU:C:2016:970), de 6 de outubro de 2020, La Quadrature du Net e o. (C-511/18, C-512/18 e C-520/18, EU:C:2020:791; a seguir «Acórdão La Quadrature du Net»), de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas) (C-746/18, EU:C:2021:152), e de 5 de abril de 2022, Commissioner of An Garda Síochána e o. (C-140/20, EU:C:2022:258; a seguir «Acórdão Commissioner of An Garda Síochána»).

I. Quadro jurídico

A. Direito da União

1. Diretiva 2002/58

4. O artigo 1.º («Âmbito e objetivos») dispõe:

«1. A presente diretiva prevê a harmonização das disposições dos Estados-Membros necessárias para garantir um nível equivalente de proteção dos direitos e liberdades fundamentais, nomeadamente o direito à privacidade e à confidencialidade, no que respeita ao tratamento de dados pessoais no setor das comunicações eletrónicas, e para garantir a livre circulação desses dados e de equipamentos e serviços de comunicações eletrónicas na Comunidade.

2. Para os efeitos do n.º 1, as disposições da presente diretiva especificam e complementam a Diretiva 95/46/CE [6]. Além disso, estas disposições asseguram a proteção dos legítimos interesses dos assinantes que são pessoas coletivas.

3. A presente diretiva não é aplicável às atividades fora do âmbito do [TFUE], tais como as abrangidas pelos títulos V e VI do Tratado da União Europeia [TUE], e em caso algum é aplicável às atividades relacionadas com a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando as atividades se relacionem com matérias de segurança do Estado) e as atividades do Estado em matéria de direito penal.»

5. O artigo 5.º («Confidencialidade das comunicações»), n.º 1, estabelece:

«Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa, exceto quando legalmente autorizados a fazê-lo, de acordo com o disposto no n.º 1 do artigo 15.º O presente número não impede o armazenamento técnico que é necessário para o envio de uma comunicação, sem prejuízo do princípio da confidencialidade.»

6. O artigo 15.º («Aplicação de determinadas disposições da Diretiva 95/46/CE») prevê:

«1. 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

[6] Diretiva do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO 1995, L 281, p. 31).

sejam conservados durante um período limitado, pelas razões enunciadas no presente número. Todas as medidas referidas no presente número deverão ser conformes com os princípios gerais do direito comunitário, incluindo os mencionados nos n.os 1 e 2 do artigo 6.º do [TUE].

[…]

2. O disposto no capítulo III da Diretiva 95/46/CE relativo a recursos judiciais, responsabilidade e sanções é aplicável no que respeita às disposições nacionais adotadas nos termos da presente diretiva e aos direitos individuais decorrentes da presente diretiva.

[…]»

2. RGPD

7. O artigo 2.º («Âmbito de aplicação material») estabelece:

«1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

2. O presente regulamento não se aplica ao tratamento de dados pessoais:

a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União;

[…]

d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

[…]»

8. O artigo 5.º («Princípios relativos ao tratamento de dados pessoais») dispõe:

«1. Os dados pessoais são:

[…]

b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 (“limitação das finalidades”);

[…]»

9. O artigo 6.º («Licitude do tratamento») dispõe:

«1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

[…]

e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;

[…]

3. O fundamento jurídico para o tratamento referido no n.º 1, alíneas c) e e), é definido:

a) Pelo direito da União; ou

b) Pelo direito do Estado-Membro ao qual o responsável pelo tratamento está sujeito.

[…]

4. Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.º, n.º 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta:

a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;

b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;

c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.º, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.º;

d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;

[…]»

3. Diretiva 2016/680

10. O artigo 1.º («Objeto e objetivos»), n.º 1, dispõe:

«1. A presente diretiva estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública.»

11. O artigo 2.º («Âmbito de aplicação»), n.º 1, estabelece:

«A presente diretiva aplica-se ao tratamento de dados pessoais pelas autoridades competentes para os efeitos estabelecidos no artigo 1.º, n.º 1.»

12. O artigo 4.º («Princípios relativos ao tratamento de dados pessoais») refere:

«1. Os Estados-Membros preveem que os dados pessoais sejam:

[…]

b) Recolhidos para finalidades determinadas, explícitas e legítimas, e não tratados de uma forma incompatível com essas finalidades;

[…]

2. É permitido o tratamento pelo mesmo ou por outro responsável pelo tratamento para as finalidades previstas no artigo 1.º, n.º 1, diferentes da finalidade para a qual os dados pessoais foram recolhidos, desde que:

a) O responsável pelo tratamento esteja autorizado a tratar esses dados pessoais com essa finalidade, nos termos do direito da União ou dos Estados-Membros; e

b) O tratamento seja necessário e proporcionado para essa outra finalidade, nos termos do direito da União ou dos Estados-Membros.

[…]»

13. O artigo 9.º («Condições específicas do tratamento»), n.º 1, dispõe:

«Os dados pessoais recolhidos pelas autoridades competentes para os fins do artigo 1.º, n.º 1, não podem ser tratados para fins diferentes dos previstos no artigo 1.º, n.º 1, a não ser que esse tratamento seja autorizado pelo direito da União ou de um Estado-Membro. Caso os dados pessoais sejam tratados para esses outros fins, é aplicável o [RGPD], salvo se o tratamento for efetuado no âmbito de uma atividade não sujeita à aplicação do direito da União.»

B. Direito nacional

1. Lietuvos Respublikos elektroninių ryšių įstatymas [7]

14. O artigo 65.º, n.º 2, impõe aos prestadores de serviços de comunicações eletrónicas a obrigação de conservarem os dados enumerados no anexo 1 da mesma lei e, se necessário, de os disponibilizarem às autoridades competentes, para que possam ser utilizados na luta contra a criminalidade grave [8].

[7] Lei da República da Lituânia relativa às comunicações eletrónicas, na redação da Lei IX-2135, de 15 de abril de 2004, conforme alterada pela Lei XIII-2172, de 6 de junho de 2019; a seguir «LCE».

[8] Os dados enumerados no referido anexo («Categorias de dados objeto de proteção») são os necessários para identificar a origem e o destino de uma comunicação, a sua data, hora e duração, o tipo de comunicação e a localização do material de comunicação (incluindo o de comunicação móvel) dos utilizadores.

15. Nos termos do artigo 77.º, n.º 1, os prestadores de serviços de comunicações eletrónicas devem disponibilizar às autoridades competentes as informações cuja posse legal detenham e que sejam necessárias, designadamente para a prevenção, deteção e repressão de infrações penais.

16. De acordo com o artigo 77.º, n.º 4, perante uma decisão judicial fundamentada ou outra base jurídica prevista por lei, os prestadores de serviços de comunicações eletrónicas devem viabilizar tecnicamente, em especial aos órgãos responsáveis pelo inquérito e pelo exercício da ação penal, de acordo com as modalidades previstas pela legislação processual penal, o controlo do conteúdo das comunicações difundidas pelas redes de comunicações eletrónicas.

2. Lietuvos Respublikos kriminalinės žvalgybos įstatymas [9]

17. Nos termos do artigo 6.º, n.º 3, ponto 1), se estiverem reunidas as condições previstas pela própria LIC e com a prévia autorização do Ministério Público ou de um órgão judicial, os órgãos responsáveis pela investigação penal [10] podem recolher informações junto dos prestadores de serviços de comunicações eletrónicas.

18. Em conformidade com o artigo 8.º, n.ºs 1 e 3, os organismos de investigação em matéria de direito penal atuam assim que dispõem de informações relativas à preparação ou à prática de uma infração penal muito grave, grave ou relativamente grave, instaurando-se imediatamente uma ação penal caso o inquérito revele a existência de uma infração penal.

19. De acordo com o artigo 19.º, n.º 1, ponto 5, as informações procedentes de diligências de inquérito podem ser utilizadas nos casos definidos nos n.ºs 3 e 4 da mesma disposição e noutros casos previstos por lei.

20. Nos termos do artigo 19.º, n.º 3, as informações relativas a um facto que revista as características de uma infração relacionada com a corrupção podem deixar de ter caráter confidencial, mediante autorização do Ministério Público, e ser utilizadas no âmbito de um inquérito relativo a infrações disciplinares ou de serviço.

3. Lietuvos Respublikos baudžiamojo proceso kodeksas [11]

21. Nos termos do artigo 154.º («Controlo, gravação e conservação da informação transmitida através de redes de comunicações eletrónicas»), n.º 1, por decisão do juiz de instrução adotada a requerimento do Ministério Público, o responsável pelo inquérito pode escutar, gravar e conservar as conversas difundidas pelas redes de comunicações eletrónicas caso existam razões para considerar que podem ser obtidos dados relativos a uma infração muito grave ou grave em fase de preparação, de execução ou já executada, ou sobre uma infração relativamente grave ou sem gravidade.

[9] Lei da República da Lituânia relativa às informações criminais, na redação da Lei XI-2234, de 2 de outubro de 2012, conforme alterada pela Lei XIII-1837, de 20 de dezembro de 2018; a seguir «LIC».

[10] Utilizarei o termo «informação», e não «inteligência», para designar os serviços responsáveis pelas investigações correspondentes.

[11] Código de Processo Penal da República da Lituânia, de 14 de março de 2002, na sua versão aplicável ao processo principal; a seguir «CEC».

22. Nos termos do artigo 177.º («Proibição de divulgação dos dados do inquérito»), n.º 1, os dados da instrução são confidenciais e, até à apreciação judicial do processo, só podem ser divulgados mediante autorização do Ministério Público e na medida em que tal se justifique [12].

II. Matéria de facto, litígio e questão prejudicial

23. A Lietuvos Respublikos generalinė prokuratūra (Ministério Público da República da Lituânia; a seguir «Ministério Público») abriu um inquérito interno relativo à conduta de A. G., à data Procurador num Apygardos prokuratūra (Delegação do Ministério Público junto de um Tribunal Regional), por existirem indícios de conduta ilícita no exercício das suas funções.

24. A Comissão do Ministério Público concluiu que A. G. tinha adotado uma conduta ilícita no exercício de funções, e propôs que lhe fosse aplicada a sanção disciplinar de demissão.

25. Essa conduta teria sido demonstrada com base na informação, obtida durante o processo administrativo, decorrente das diligências dos serviços de informação criminal, das explicações de outros funcionários e do recorrente, e dos despachos de encerramento de dois inquéritos.

26. Em particular, teriam existido comunicações telefónicas entre A. G. e o advogado de um arguido, no âmbito de um inquérito conduzido por A. G. relativamente a processos em que esse advogado agira na qualidade de representante do arguido [13].

27. A vigilância e o registo das informações transmitidas através das redes de comunicações eletrónicas tinham sido autorizados por despachos judiciais.

28. O Procurador-Geral aplicou a sanção de destituição de funções a A. G., que dela interpôs recurso no Vilniaus apygardos administracinis teismas (Tribunal Administrativo Regional de Vilna, Lituânia), requerendo a sua anulação.

29. Ao recurso foi negado provimento por Decisão de 16 de julho de 2021, considerando o tribunal de primeira instância que a atuação dos serviços de informação criminal fora lícita, tal como a utilização dos dados obtidos por estes serviços no procedimento disciplinar.

30. A. G. interpôs recurso da decisão de primeira instância para o Lietuvos vyriausiasis administracinis teismas (Supremo Tribunal Administrativo da Lituânia), que submete ao Tribunal de Justiça a seguinte questão prejudicial:

«Deve o artigo 15.º, n.º 1, da Diretiva 2002/58 […], lido em conjugação com os artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia [Carta], ser interpretado no sentido de que proíbe as autoridades públicas competentes de usarem, no âmbito de investigações por conduta ilícita relacionada com corrupção no exercício de funções, os dados conservados pelos prestadores de serviços de comunicações eletrónicas que podem fornecer informações sobre os dados de um utilizador de um meio de comunicação eletrónica e sobre as

[12] Segundo as Ikiteisminio trio duomenų teikimo ir panaudojimo ne baudžiamojo persekiojimo tikslais ir ikiteisminio tyrimo duomenų apsaugos rekomendajos (Recomendações para o fornecimento e utilização de dados do inquérito para fins não judiciais e para a proteção de dados do inquérito) aprovadas pela Decisão n.º 1-279 do procurador-geral de 17 de agosto de 2017, conforme alterada pela Decisão n.º 1-211 de 25 de junho de 2018, em especial a cláusula 23, quando recebe um pedido de aceso aos dados da instrução, o Procurador decide se os mesmos devem ser disponibilizados. Em caso afirmativo, deve precisar em que medida o podem ser.

[13] Conforme exposto na audiência, ainda se encontram pendentes de apreciação processos penais contra A. G. e contra o advogado por esses factos.

comunicações por este efetuadas, independentemente de ter sido concedido acesso a esses dados, no caso concreto, para fins de luta contra a criminalidade grave e de prevenção de ameaças graves à segurança pública?»

III. Tramitação do processo no Tribunal de Justiça

31. O pedido de decisão prejudicial foi registado no Tribunal de Justiça em 3 de março de 2022.

32. Apresentaram observações escritas A. G., os Governos checo, estónio, húngaro, irlandês, italiano e lituano, bem como a Comissão Europeia.

33. Na audiência pública, realizada em 2 de fevereiro de 2023, compareceram A. G., os Governos francês, húngaro, irlandês e lituano, bem como a Comissão.

IV. Análise

A. Admissibilidade. Delimitação da resposta à questão prejudicial

34. O órgão jurisdicional de reenvio é um tribunal administrativo, competente para a fiscalização jurisdicional de decisões também elas administrativas. Tem esta natureza a decisão adotada pelo Procurador-Geral, que aplicou uma sanção de destituição de funções a um funcionário de uma delegação do Ministério Público junto de um tribunal regional, por factos constitutivos de infração disciplinar.

35. Assim, o litígio *a quo* não tem por objeto decisões das autoridades judiciais com competência penal. Mesmo que essas decisões coexistam com o procedimento administrativo (disciplinar) que levou à destituição de funções [14], há que salientar que a controvérsia apenas se suscita no que diz respeito a esta última.

36. Dito isto, observa-se na decisão de reenvio uma certa imprecisão quanto aos factos do litígio, que prefiguram o contexto em que se insere a questão prejudicial.

37. Como salientaram o Governo checo e a Comissão, não é possível determinar inequivocamente, com base no despacho de reenvio, se as autoridades competentes: a) se dirigiram aos prestadores de serviços de comunicações eletrónicas para obter os dados controvertidos; ou b) elas próprias obtiveram diretamente esses dados.

38. A questão de modo nenhum é despicienda. Dela depende a determinação da legislação da União pertinente para responder à questão prejudicial. Consoante os factos se tenham verificado de uma ou de outra forma, é aplicável:

— A Diretiva 2002/58, se os dados obtidos resultam de uma obrigação de tratamento imposta aos prestadores de serviços de comunicações eletrónicas; ou

— A Diretiva 2016/680, se os dados foram diretamente obtidos pela autoridade pública, sem impor obrigações a esses prestadores.

[14] V. nota de pé de página 13 destas conclusões.

39. Nesta segunda hipótese, a proteção dos dados pessoais seria regulada pelo direito nacional, sem prejuízo da aplicação da Diretiva 2016/680 [15]. Consequentemente, a questão prejudicial, por se centrar na Diretiva 2002/58, teria adotado uma abordagem inadequada.

40. O Governo húngaro, convencido de que os dados pessoais teriam sido obtidos mediante operações de interceção telefónica executadas pelos serviços de informação criminal, questiona a admissibilidade do reenvio prejudicial, uma vez que a Diretiva 2002/58 seria, como foi dito, inaplicável.

41. No entanto, para a Comissão,

— Seria aplicável a Diretiva 2016/680, na medida em que se trate de utilizar, para um inquérito posterior, dados pessoais recolhidos e conservados diretamente pelas autoridades no âmbito de um inquérito criminal anterior;

— Aplicar-se-ia a Diretiva 2002/58 se, como declarou o tribunal de reenvio [16], pelo menos alguns dos dados tiveram de ser recolhidos e conservados por força de uma legislação nacional adotada em aplicação do seu artigo 15.º, n.º 1. A Diretiva 2002/58 seria, assim, relevante para a decisão do litígio.

42. Concordo com esta abordagem da Comissão que, além do mais, é a única que permite superar as (justificadas) dúvidas suscitadas pela decisão de reenvio quanto à sua admissibilidade.

43. Assim entendida a questão prejudicial, a pertinência da Diretiva 2002/58 para lhe responder:

— Decorre da presunção inerente a qualquer reenvio prejudicial, no que se refere à necessidade da sua submissão, cuja responsabilidade cabe ao juiz que o submete [17].

— Pode aceitar-se na medida em que seja apenas desta Diretiva 2002/58, que o órgão jurisdicional de reenvio considera determinante para decidir o litígio, que se pede a interpretação do Tribunal de Justiça [18].

44. Com efeito, segundo o tribunal de reenvio, no processo submetido à sua apreciação são relevantes:

«i) a utilização dos *dados conservados pelos prestadores de serviços de comunicações eletrónicas* para fins diferentes dos de luta contra a criminalidade grave e de prevenção de ameaças graves à segurança pública;

[15] Acórdão La Quadrature du Net, n.º 103: «quando os Estados-Membros aplicam diretamente medidas que derrogam a confidencialidade das comunicações eletrónicas, sem imporem obrigações de tratamento aos prestadores de serviços de tais comunicações, a proteção dos dados das pessoas em causa não está abrangida pela Diretiva 2002/58, mas apenas pelo direito nacional, sem prejuízo da aplicação da [Diretiva 2016/680]».

[16] N.º 37 do despacho de reenvio.

[17] Por todos, Acórdãos de 4 de dezembro de 2018, Minister for Justice and Equality e Commissioner of An Garda Síochána (C-378/17, EU:C:2018:979, n.º 26) e de 22 de dezembro de 2022, Airbnb Ireland e Airbnb Payments UK (C-83/21, EU:C:2022:1018, n.º 82).

[18] A inequívoca referência à Diretiva 2002/58 no dispositivo da decisão de reenvio e o silêncio relativamente à Diretiva 2016/680 na sua fundamentação jurídica militam no mesmo sentido. Diferente é o facto de o Tribunal de Justiça, sem exceder os limites da questão, poder facultar ao órgão jurisdicional de reenvio indicações úteis para a prolação da sua decisão, eventualmente recorrendo a outras normas do direito da União. Neste sentido, Acórdão de 18 de setembro de 2019, VIPA (C-222/18, EU:C:2019:751, n.º 50, e jurisprudência referida).

ii) *utilização do acesso aos dados conservados* para fins de luta contra a criminalidade grave e de prevenção de ameaças graves à segurança pública na investigação de infrações relacionadas com corrupção no exercício de funções» [19].

45. Assim, tudo parece indicar que, além da eventual existência de dados pessoais cujo tratamento não podia ser incluído no âmbito de aplicação da Diretiva 2002/58 (e sim no da Diretiva 2016/680), o inquérito que conduziu à aplicação da sanção fez uso de dados pessoais recolhidos junto dos prestadores de serviços de comunicações eletrónicas.

46. A resposta do Tribunal de Justiça deve circunscrever-se ao pedido do órgão jurisdicional de reenvio nos termos em que este o submete. Por conseguinte, deve esclarecer se os dados pessoais obtidos e tratados ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58 no âmbito de um inquérito penal podem ser utilizados, posteriormente, num procedimento (administrativo) de natureza disciplinar dirigido contra um funcionário público.

47. Assim delimitados os termos do reenvio prejudicial, o inverso de tudo o anteriormente exposto é que o mesmo não abrange as seguintes questões:

— Em primeiro lugar, as relativas à legalidade da *obtenção inicial* dos dados pessoais ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58. A questão do tribunal de reenvio circunscreve-se à *utilização posterior* destes dados no procedimento disciplinar, sem pôr em causa a licitude da sua obtenção inicial [20].

— Em segundo lugar, as relativas à utilização dos dados obtidos e tratados diretamente pelas autoridades públicas no âmbito de inquéritos penais anteriores. Quanto a este ponto, cuja disciplina se enquadra no âmbito do direito nacional e da Diretiva 2016/680, o órgão jurisdicional de reenvio também não manifesta dúvidas.

48. Em suma, as considerações que se seguem quanto ao mérito têm de excluir a interpretação da Diretiva 2016/680 [21]. Serão circunscritas, no que se refere à Diretiva 2002/58, à utilização de dados pessoais obtidos ao abrigo desta mediante tratamentos cuja licitude inicial se pressupõe, uma vez que não é posta em causa no litígio *a quo*.

B. Quanto ao mérito

1. Resenha da jurisprudência do Tribunal de Justiça quanto à aplicação da Diretiva 2002/58

49. Do artigo 15.º, n.º 1, primeiro período, da Diretiva 2002/58 infere-se que os Estados-Membros podem adotar uma medida derrogatória do princípio da confidencialidade, consagrado no artigo 5.º, n.º 1, da mesma diretiva, quando seja «necessária, adequada e proporcionada numa sociedade democrática» e «rigorosamente» proporcionada ao objetivo a alcançar [22].

[19] N.º 35 do despacho de reenvio. O sublinhado é meu.

[20] Não é necessário, assim, que o Tribunal de Justiça se pronuncie sobre a licitude dessas operações prévias. Se o fizesse, teria de reiterar que o *acesso* aos dados em poder dos prestadores de serviços de comunicações eletrónicas só pode ser concedido se foram *conservados* em conformidade com o artigo 15.º, n.º 1, da Diretiva 2002/58. V., neste sentido, Acórdão La Quadrature du Net, n.º 167. Esta disposição, interpretada em conjugação com os artigos 7.º, 8.º, 11.º e 52.º, n.º 1, da Carta, opõe-se a medidas legislativas que preveem, para essas finalidades, a título preventivo, uma conservação generalizada e indiferenciada dos dados de tráfego e dos dados de localização (Acórdão La Quadrature du Net, n.º 168).

[21] No entanto, referir-me-ei a ela, a título subsidiário, na parte final das presentes conclusões.

[22] Acórdão La Quadrature du Net, n.º 129.

50. Em particular, a possibilidade de os Estados-Membros justificarem uma limitação aos direitos e às obrigações previstos nos artigos 5.º, 6.º e 9.º da Diretiva 2002/58 deve ser apreciada através 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 [23].

51. «Para cumprir o requisito de proporcionalidade, uma regulamentação deve prever normas claras e precisas que regulem o âmbito e a aplicação da medida em causa e impor requisitos mínimos, de modo que as pessoas cujos dados foram conservados disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso. Esta regulamentação deve ser vinculativa no direito interno e, em particular, indicar em que circunstâncias e em que condições uma medida que prevê o tratamento de tais dados pode ser adotada […]» [24].

52. No que respeita aos motivos de interesse geral suscetíveis de justificar uma medida adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, em conformidade com o princípio da proporcionalidade, existe uma hierarquia de objetivos em função da respetiva importância: a importância do objetivo prosseguido por essa medida deve estar relacionada com a gravidade da ingerência [25].

53. Nessa hierarquia de objetivos, a salvaguarda da segurança nacional, lida à luz do artigo 4.º TUE, n.º 2, está acima dos outros objetivos referidos no artigo 15.º, n.º 1, da Diretiva 2002/58, isto é a defesa, a segurança pública ou a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas. O objetivo de lutar contra a criminalidade em geral, incluindo a grave, e de salvaguardar a segurança pública insere-se nesta segunda categoria [26].

54. Desta categorização de objetivos deduz-se que:

— O objetivo de defender a segurança nacional, o primeiro na ordem hierárquica referida pelo Tribunal de Justiça, permite ingerências tão graves como as representadas por medidas legislativas que permitam impor aos prestadores de serviços de comunicações eletrónicas que procedam a uma conservação generalizada e indiferenciada de dados de tráfego e de dados de localização [27].

— O objetivo imediatamente a seguir em termos de importância, isto é, a luta contra a criminalidade grave, pode justificar ingerências como, por exemplo, uma conservação selecionada dos dados de tráfego e dos dados de localização ou dos endereços IP atribuídos à fonte de uma ligação, por um período temporalmente limitado ao estritamente necessário [28].

[23] Acórdão La Quadrature du Net, n.º 131 e jurisprudência referida.

[24] Acórdão Commissioner of An Garda Síochána, n.º 54.

[25] Acórdão Commissioner of An Garda Síochána, n.º 56.

[26] Acórdão La Quadrature du Net, n.ºs 135 e 136, onde se explica que a segurança nacional constitui uma responsabilidade exclusiva do Estado que corresponde ao interesse primordial de proteger as funções essenciais do Estado e os interesses fundamentais da sociedade contra atividades suscetíveis de desestabilizar gravemente as estruturas constitucionais, políticas, económicas ou sociais fundamentais de um país, e, em especial, de ameaçar diretamente a sociedade, a população ou o Estado enquanto tal, como, nomeadamente, as atividades terroristas. Ameaças que se distinguem, pela sua natureza e particular gravidade, do risco geral de ocorrência de tensões ou perturbações, ainda que graves, à segurança pública. Daí resulta que o objetivo de salvaguarda da segurança nacional é suscetível de justificar medidas que incluam ingerências nos direitos fundamentais mais graves do que aquelas que esses outros objetivos poderiam justificar.

[27] Acórdão Commissioner of An Garda Síochána, n.º 58.

[28] Acórdão La Quadrature du Net, n.º 168.

2. Aplicação desta jurisprudência ao presente reenvio prejudicial

55. Segundo o tribunal de reenvio, os dados controvertidos teriam sido obtidos mediante ingerências graves nos direitos garantidos pelos artigos 7.º, 8.º e 11.º da Carta [29].

56. Não se trata aqui, repito, de apreciar a licitude inicial da obtenção destes dados, ou seja, de apreciar se a ingerência foi suficientemente justificada em razão da gravidade da infração penal contra a qual se pretendia agir.

57. O tribunal de reenvio pronunciou-se sobre ambos os pontos (gravidade da ingerência e gravidade da infração) em termos que não são contestados no processo *a quo* e não são, portanto, relevantes para o reenvio prejudicial.

58. O que importa agora, nas palavras do órgão judicial *a quo*, é determinar se esses dados: a) podem ser igualmente utilizados em inquéritos posteriores que tenham por objeto a luta contra a criminalidade em geral (pressupondo que este conceito abrange a conduta objeto da sanção disciplinar controvertida); ou b) só podem ser utilizados nos inquéritos destinados a lutar contra a criminalidade grave.

59. Os Governos checo e irlandês verificaram se a conduta que está em causa perante o tribunal de reenvio deve, ou não, ser qualificada de «infração grave», e concluíram em sentido afirmativo.

60. No entanto, na minha opinião, este é um ponto sobre o qual o Tribunal de Justiça não tem de se pronunciar, uma vez que a qualificação da conduta é da competência do órgão jurisdicional de reenvio.

61. O tribunal *a quo* afirma que, se a utilização dos dados obtidos mediante uma ingerência grave nos direitos fundamentais só pudesse ser justificada pela luta contra a criminalidade grave e pela prevenção de ameaças graves à segurança pública, estes dados não poderiam ser utilizados nos inquéritos de infrações disciplinares relacionadas com a corrupção [30], ou seja, em inquéritos como o controvertido neste processo.

62. Com base nesta apreciação, o que interessa é esclarecer se as infrações disciplinares para cuja repressão se pretende utilizar determinados dados pessoais têm de ser qualitativamente equivalentes, quanto à sua gravidade, às infrações que justificaram a obtenção desses dados [31].

[29] É o que decorre do n.º 46 do despacho de reenvio: neste são referidos dados que podem facultar informação sobre as comunicações efetuadas por um utilizador de um meio de comunicação eletrónica ou sobre a localização dos equipamentos terminais que utiliza e que permitem tirar conclusões precisas sobre a vida privada das pessoas em causa.

[30] Despacho de reenvio, n.º 46, *in fine*.

[31] No Acórdão do Tribunal Europeu dos Direitos do Homem (TEDH) de 18 de janeiro de 2022, Adomaitis c. Lituânia (CE:ECHR:2022:0118JUD001483318; a seguir, «Acórdão TEDH Adomaitis»), referente à interceção de comunicações eletrónicas num caso de abuso de poder continuado por parte do diretor de um estabelecimento prisional, são facultadas pistas para avaliar essa equivalência.

63. Na audiência, o Governo lituano reconheceu que a destituição de funções fora aplicada por uma infração deontológica do Procurador punido. Verificar se essa infração (fuga de informação relativa a um inquérito) pode ser equiparada a uma infração penal grave ou implicar um risco grave para a salvaguarda da segurança pública depende de um conjunto de fatores que só o tribunal de reenvio está em condições de verificar [32].

64. Na audiência foram feitas numerosas referências à luta contra a corrupção enquanto fenómeno subjacente a condutas como a que está em causa. O debate sobre este ponto requer muitos matizes, para garantir o rigor exigível em todas as manifestações do poder punitivo do Estado. Há que determinar, por exemplo, se o termo «corrupção» é utilizado num sentido genérico ou se alude a um tipo específico de comportamento no qual, em abstrato, talvez seja excessivo incluir a mera violação do dever de sigilo se não for acompanhada de uma vantagem correlativa para o funcionário [33].

65. De qualquer modo, caso o tribunal de reenvio considere que a infração deontológica aqui punida é de menor gravidade do que a infração penal cujo inquérito justificou a medida adotada ao abrigo do artigo 15.º da Diretiva 2002/58, a resposta à sua questão prejudicial infere-se destas declarações do Tribunal de Justiça:

— «O acesso a dados de tráfego e a dados de localização conservados pelos prestadores em aplicação de uma medida adotada ao abrigo do artigo 15.º, n.º 1, da Diretiva 2002/58, que deve ser efetuado no pleno respeito das condições resultantes da jurisprudência que interpretou a Diretiva 2002/58, apenas pode, em princípio, ser justificado pelo objetivo de interesse geral pelo qual essa conservação foi imposta a esses prestadores. Só assim não será se a importância do objetivo prosseguido pelo acesso ultrapassar a do objetivo que justificou a conservação» [34].

— «Em particular, […] um acesso a tais dados para efeitos de repressão e de sanção de uma infração penal ordinária não pode, em caso algum, ser concedido quando a sua conservação foi justificada pelo objetivo de luta contra a criminalidade grave ou, *a fortiori*, de salvaguarda da segurança nacional» [35].

66. Assim, é aplicável a este respeito uma espécie de princípio da equivalência entre os objetivos de interesse geral que justificam a *obtenção* de dados pessoais, por um lado, e os que legitimam a sua *utilização* posterior, por outro. A única exceção a este princípio é, como se acaba de expor, que a importância do objetivo prosseguido pelo acesso ultrapasse a do objetivo que justificou a conservação.

[32] Em princípio, não são equiparáveis condutas puníveis cuja repressão se verifica através de um processo penal, por um lado, e meras infrações deontológicas, cuja sanção é aplicada mediante um procedimento disciplinar, por outro. O processo penal e o procedimento disciplinar distinguem-se, quanto ao seu objeto, pela natureza e gravidade da conduta em causa. A disparidade de procedimentos é, para este efeito, indicativa da diferente gravidade dos seus respetivos objetos.

[33] Na Convenção estabelecida com base no n.º 2, alínea c), do artigo K.3, do Tratado da União Europeia, relativa à luta contra a corrupção em que estejam implicados funcionários das Comunidades Europeias ou dos Estados-Membros da União Europeia (JO 1997, C 195, p. 2) são previstos casos de corrupção passiva («o facto de um funcionário, intencionalmente, de forma direta ou por interposta pessoa, solicitar ou receber vantagens de qualquer natureza, para si próprio ou para terceiros, ou aceitar promessas dessas vantagens, para que pratique ou se abstenha de praticar, em violação dos deveres do seu cargo, atos que caibam nas suas funções ou no exercício das mesmas») e ativa («o facto de uma pessoa prometer ou dar intencionalmente, de forma direta ou por interposta pessoa, uma vantagem de qualquer natureza a um funcionário, para este ou para terceiros, para que pratique ou se abstenha de praticar, em violação dos deveres do seu cargo, atos que caibam nas suas funções ou no exercício das mesmas»), que devem ser tipificados como infrações penais.

[34] Acórdão Commissioner of An Garda Síochána, n.º 98.

[35] Acórdão La Quadrature du Net, n.º 166.

67. Interpretá-lo de outra forma desvirtuaria o sistema de garantias da Diretiva 2002/58: os direitos que salvaguarda poderiam ser objeto de ingerências graves fora dos casos previstos no seu artigo 15.º e das condições determinadas na jurisprudência do Tribunal de Justiça.

68. Em especial, o sacrifício da inviolabilidade do direito à confidencialidade das comunicações só é legitimamente admissível em função do concreto objetivo de interesse geral visado. Por esse motivo, a legitimidade do acesso aos dados conservados deve ser verificada casuisticamente, ponderando a respetiva gravidade, por um lado, e a importância do objetivo de interesse geral que essa ingerência prossegue, por outro.

69. O que não se pode aceitar como interpretação da Diretiva 2002/58 é que, disponibilizado o acesso no âmbito de um primeiro caso que validamente o justifique, se abra caminho a um acesso posterior (na realidade, uma reutilização dos dados obtidos) com base num objetivo hierarquicamente inferior ao daquele primitivo caso.

70. Para este efeito, as exigências requeridas para o acesso inicial (incluindo as pedidas pelo Tribunal de Justiça para a sua autorização) [36] são transponíveis para a utilização posterior dos mesmos dados por outras autoridades.

C. A título subsidiário: incidência da Diretiva 2016/680

71. Até aqui expus o que considero mais adequado para responder ao pedido de decisão prejudicial nos seus próprios termos, ou seja, facultando ao tribunal de reenvio a interpretação da Diretiva 2002/58, tal como é pedida.

72. Na hipótese de os dados controvertidos neste processo não terem sido obtidos ao abrigo do artigo 15.º, n.º [1], da Diretiva 2002/58, mas diretamente pelos serviços de informação criminal do Estado-Membro, num processo penal, o cenário seria diferente.

73. Nesta hipótese, estariam em jogo as normas do direito nacional, sem prejuízo da aplicação da Diretiva 2016/680 no que se refere ao tratamento de dados pessoais obtidos num inquérito penal. Considero facto assente que a atuação dos serviços de informação criminal em casos como este se integra no âmbito da Diretiva 2016/680, o que se confirmou na audiência.

74. Como expus nas conclusões no processo Inspektor v Inspektorata kam Visshia sadeben savet (Fins do tratamento de dados pessoais — Inquérito penal) [37], «o RGPD e a Diretiva 2016/680 integram um sistema coerente em que:

— Cabe ao RGPD fixar as *normas gerais* para a proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais.

— A Diretiva 2016/680 institui *normas específicas* para o tratamento desses dados no domínio da cooperação judiciária em matéria penal e da cooperação policial» [38].

[36] Acórdão Commissioner of An Garda Síochána, n.º 106, com referência do Acórdão Prokuratuur, n.º 51.

[37] C-180/21 (EU:C:2022:406); a seguir «Conclusões Inspektor v Inspektorata».

[38] Conclusões Inspektor v Inspektorata, ponto 35.

75. Recordava então [39] que:

— «A proteção conferida pelo regime constituído por estas duas disposições assenta nos princípios da licitude, da lealdade, da transparência e, no que aqui interessa, no princípio da estrita limitação da recolha de dados e do seu tratamento para as finalidades previstas na lei».

— «Em especial, o artigo 5.º, n.º 1, alínea b), do RGPD dispõe que os dados são "recolhidos para finalidades determinadas, explícitas e legítimas *e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades*". Exprime-se igualmente nesses termos, enquanto *lex specialis*, o artigo 4.º, n.º 1, alínea b), da Diretiva 2016/680».

— «Assim, os dados pessoais não podem ser recolhidos ou tratados de forma geral, mas apenas em função de finalidades determinadas nas condições de licitude fixadas pelo legislador da União» [40].

— «O princípio da ligação estrita entre a recolha e o tratamento de dados, por um lado, e as finalidades que as duas operações devem servir, por outro, não tem caráter absoluto, uma vez que tanto o RGPD como a Diretiva 2016/680 permitem uma certa flexibilidade […]»

76. Ora, tal como o Tribunal de Justiça interpretou o artigo 4.º, n.º 2, da Diretiva 2016/680 [41], dificilmente se pode admitir que os dados pessoais recolhidos durante o processo penal sejam utilizados *com a mesma finalidade* no contexto de um posterior procedimento disciplinar contra um funcionário público.

77. Devo recordar, porém, que, nos termos do artigo 4.º, n.º 2, da Diretiva 2016/680, «é permitido o tratamento pelo mesmo ou por outro responsável pelo tratamento para as finalidades previstas no artigo 1.º, n.º 1, diferentes da finalidade para a qual os dados pessoais foram recolhidos, desde que:

— O responsável pelo tratamento esteja autorizado a tratar esses dados pessoais com essa finalidade, nos termos do direito da União ou dos Estados-Membros; e

— O tratamento seja necessário e proporcionado para essa outra finalidade, nos termos do direito da União ou dos Estados-Membros».

78. Com base nesta premissa, o tribunal de reenvio deve considerar se a finalidade (*diferente*) do tratamento posterior se encontra entre as previstas no artigo 1.º, n.º 1, da Diretiva 2016/680 ou se não é abrangida por estes:

— No primeiro caso (reafetação *ad intra*) há que demonstrar que estão preenchidos os dois requisitos previstos no artigo 4.º, n.º 2, da Diretiva 2016/680.

— No segundo caso (reafetação *ad extra*) é chamado à colação o artigo 9.º, n.º 1, da Diretiva 2016/680.

[39] Conclusões Inspektor v Inspektorata, pontos 36 a 39.

[40] O requisito da «licitude» é exigido pelo artigo 5.º, n.º 1, alínea a), do RGPD [artigo 4.º, n.º 1, alínea a), da Diretiva 2016/680], explicitando-se no artigo 6.º do mesmo regulamento quais são as suas condições. No que aqui interessa e ao abrigo da alínea e) desta última disposição, o tratamento deve ser necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável (pelo próprio tratamento).

[41] Acórdão de 8 de dezembro de 2022, Inspektor v Inspektorata kam Visshia sadeben savet (Finalidades do tratamento de dados pessoais — Instrução penal), C-180/21 (EU:C:2022:967); a seguir «Acórdão Inspektor v Inspektorata».

1. Utilização dos dados ao abrigo do artigo 4.º, n.º 2, da Diretiva 2016/680

79. No que se refere ao *primeiro* dos dois requisitos exigidos por esta disposição, só tem de ser cumprido se o direito do Estado-Membro constar de uma lei [42] que defina quando é que o responsável é autorizado a tratar os dados pessoais. Além disso, essa lei deve conter regras vinculativas, claras e precisas [43].

80. No entanto, este é um ponto que, naturalmente, cabe ao tribunal de reenvio verificar, após a análise do artigo 177.º do CEC, do artigo 19.º, n.º 3, da LIC e das Recomendações do Ministério Público [44]. Com estes elementos há que avaliar até que ponto o direito nacional permite que as informações obtidas no âmbito de um processo penal possam ser utilizadas, sob determinadas condições, no contexto do inquérito relativo a infrações disciplinares. Para essa verificação, podem ser-lhe úteis as considerações do Acórdão do TEDH, Adomaitis [45].

81. Quanto ao *segundo* requisito, o tribunal de reenvio deve apreciar se, no tratamento de dados objeto deste processo, se verificou a necessidade da ingerência e o seu caráter proporcionado [46].

82. Mais uma vez, as declarações do Acórdão Adomaitis podem contribuir para essa apreciação:

— Quanto à necessidade, há que ponderar até que ponto a insuficiência probatória de outros dados disponibilizados durante o procedimento disciplinar torna efetivamente necessária, para o êxito do inquérito em curso, a utilização dos dados controvertidos [47].

— Quanto à proporcionalidade, há que avaliar a gravidade da infração que deu origem ao procedimento disciplinar, tendo em consideração que, como alegou o Governo lituano e decorre do Acórdão TEDH Adomaitis [48], a utilização de dados pessoais é reservada aos casos de infrações para os quais é prevista a sanção disciplinar mais grave, isto é, a destituição.

2. Utilização dos dados ao abrigo do artigo 9.º da Diretiva 2016/680

83. Nos termos do artigo 9.º, n.º 1, da Diretiva 2016/680, os dados pessoais recolhidos pelas autoridades competentes para os fins do seu artigo 1.º, n.º 1, podem ser tratados para fins *diferentes dos previstos no artigo 1.º, n.º 1*, quando esse tratamento seja autorizado pelo direito da União ou de um Estado-Membro. Neste caso, é aplicável o RGPD, salvo se o tratamento for efetuado no âmbito de uma atividade não sujeita à aplicação do direito da União [49].

[42] Concordo com a Comissão no sentido de que, sendo a utilização posterior de dados pessoais obtidos durante um inquérito penal uma ingerência nos direitos fundamentais garantidos pelos artigos 7.º e 8.º da Carta, é indispensável, por força do artigo 52.º, n.º 1, da Carta, que seja prevista por lei.

[43] Ponto 51 das presentes conclusões.

[44] Nota de pé de página 12 das presentes conclusões.

[45] Acórdão em cujo n.º 83 se considera suficiente a garantia de legalidade da ingerência resultante das disposições legislativas nacionais e da jurisprudência constitucional lituana.

[46] Como refere a Comissão, este processo não é muito diferente do analisado no Acórdão do TEDH de 16 de junho de 2016, Versini-Campinchi e Crasnianski c. França (CE:ECHR:2016:0616JUD004917611). De acordo com o seu n.º 57, corresponde a uma finalidade legítima, ao abrigo do artigo 8.º da CEDH, a utilização, no âmbito de um procedimento disciplinar por violação de sigilo profissional, das comunicações intercetadas num processo penal. A estreita interligação material entre os objetos respetivos dos processos penal e disciplinar conduz à legitimidade comum das finalidades de ambos.

[47] Acórdão TEDH Adomaitis, n.º 85.

[48] Acórdão TEDH Adomaitis, n.º 87.

[49] Esta derrogação foi objeto de interpretação estrita no Acórdão de 22 de junho de 2021, Latvijas Republikas Saeima (Pontos de penalização) (C-439/19, EU:C:2021:504, n.º 66).

84. Na hipótese de o tribunal de reenvio considerar inaplicável o artigo 4.º, n.º 2, da Diretiva 2016/680, há que recorrer ao RGPD. Em conformidade com este regulamento terá de esclarecer se, além da previsão legal, se verifica pelo menos uma das condições de licitude do tratamento de dados pessoais taxativamente fixadas no seu artigo 6.º, n.º 1.

V. Conclusão

85. Atendendo ao exposto, proponho ao Tribunal de Justiça que responda ao Lietuvos vyriausiasis administracinis teismas (Supremo Tribunal Administrativo da Lituânia) nos seguintes termos:

«1. 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), 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:

não permite às autoridades públicas competentes recolherem dados conservados por prestadores de serviços de comunicações eletrónicas que possam facultar informação pormenorizada sobre um utilizador e utilizar esses dados no âmbito de um inquérito relativo a condutas constitutivas de infrações menos graves do que aquelas cujo inquérito tenha podido justificar, à época, o acesso a esses dados.

2. A título subsidiário:

O artigo 9.º, n.º 1, da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, em conjugação com os artigos 6.º e 10.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE, à luz dos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia,

deve ser interpretado no sentido de que:

não se opõe à utilização, num procedimento administrativo de natureza disciplinar, de dados pessoais obtidos lícita e diretamente por uma autoridade pública no âmbito de um inquérito penal, desde que, em conformidade com regras claras, precisas e vinculativas do direito nacional, esse procedimento e esse inquérito estejam relacionados e na medida em que a utilização dos dados tenha uma finalidade legítima e seja necessária e proporcionada, o que compete à autoridade judicial determinar.»