OBTENÇÃO DE INFORMAÇÕES DE OPERADORES DE COMUNICAÇÕES

Nota Prática nº 26/2024

10 de maio de 2024

ÍNDICE

NOTA PRÁTICA nº 26/2024
10 de maio de 2024

OBTENÇÃO DE INFORMAÇÕES DE OPERADORES DE COMUNICAÇÕES

Esta Nota Prática pretende auxiliar os magistrados do Ministério Público na solicitação de informações, em processo penal, a operadores de comunicações.
Descrevem-se sumariamente as informações guardadas pelos operadores que podem vir a ser usadas em investigações criminais e referenciam-se os fundamentos jurídicos que delimitam os pedidos dessas informações.

A. ABORDAGEM GERAL

1. Os dados em posse de operadores de comunicações, sobretudo se permitirem identificar quem efetuou uma determinada comunicação criminosa, constituem informação importantíssima nas investigações criminais modernas.

2. As regras legais a este respeito foram recentemente modificadas, em consequência de jurisprudência constitucional e da publicação da Lei nº 18/2024, de 5 de fevereiro, que introduziu alterações à Lei nº 32/2008, de 17 de julho. Da jurisprudência e do novo quadro legal resulta que:

- se mantém intocado e em vigor o regime anteriormente vigente, de guarda de dados para efeitos de faturação, previsto na Lei nº 41/2004, de 18 de agosto, e do acesso aos mesmos, legitimado pelo artigo 14º da Lei do Cibercrime;
- foi criado um regime adicional de conservação generalizada de dados de subscritor (artigo 6º, nº 1, da Lei nº 32/2008, na nova redação) e
- foi introduzido um procedimento especial, que não de processo penal, de conservação seletiva de dados de tráfego e localização (artigo 6º, nº 2 da Lei nº 32/2008).

B. DADOS DE SUBSCRITOR

3. Por razões comerciais e contratuais, os operadores guardam necessariamente informação respeitante à identificação dos seus clientes: são os chamados dados de subscritor (*dados relativos aos seus clientes ou assinantes*), descritos no artigo 14º, nº 4, da Lei do Cibercrime. Trata-se do

conjunto dos dados que resultam da celebração de um contrato de prestação de serviços entre ambas as partes (prestador de serviços e cliente), que eram tradicionalmente conhecidos, em décadas passadas, no contexto das comunicações telefónicas, em linguagem agora desatualizada, como *dados de base*. Tais dados são guardados, em geral, pelo menos, enquanto dura o contrato de prestação de serviço – portanto, por vezes, durante muitos anos.

No quadro normativo da Convenção de Budapeste e da Lei nº 109/2009, que a transpôs para o direito português, os dados de subscritor abrangem toda a informação respeitante à utilização do serviço de comunicações (com exceção dos dados de tráfego e conteúdo), referentes ao tipo de serviço contratado e utilizado, às medidas técnicas relacionadas com o serviço (as quais possibilitam ao utilizador usufruir do serviço prestado, incluindo os números e endereços técnicos e os números de registo dos aparelhos de comunicações utilizados), o período de subscrição do serviço, os dados que permitam apurar a identidade do subscritor do serviço (como a sua identificação ou a morada postal e geográfica), os dados de faturação e pagamentos e o local onde se encontra instalado o equipamento.

Acesso do Ministério Público aos dados de subscritor

4. A lei portuguesa define, no artigo 14º da Lei do Cibercrime, os "*dados relativos a clientes ou assinantes*" dos fornecedores de serviços, ou seja, aquilo a que a doutrina anglo-saxónica chama "*subscriber information*". O nº 4 do artigo 14º da Lei do Cibercrime define então como *dados de subscritor* dos operadores de comunicações / fornecedores de serviço, os "*dados relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo*".

5. De acordo com esta norma da Lei do Cibercrime, no decurso de uma investigação criminal, a solicitação de tal informação, em posse dos operadores de comunicações, é um ato da competência da autoridade judiciária – portanto, o Ministério Público durante o inquérito.

A mais moderna jurisprudência do Tribunal de Justiça de União Europeia[1] tem-se manifestado genericamente favorável à conservação generalizada de dados relativos à identidade civil dos subscritores de serviços e à sua utilização na investigação de crimes.

6. Anote-se que os dados aqui em causa terão que ser "*dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços*". Quer isto dizer que esta medida processual não se

[1] Neste sentido, veja-se designadamente o Acórdão de 6 de outubro de 2020 (C-511/18, C-512/18 e C-520/18, "*Quadrature du Net*" e outros – https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62018CJ0511).

destina à obtenção de informação resultante de preservação de dados para futuro, prevista no artigo 12º da Lei do Cibercrime, nem à obtenção de informação obtida por via da interceção de comunicações, prevista no artigo 18º da Lei do Cibercrime. Estas duas medidas processuais são proativas e visam a obtenção de dados que, de outra forma não seriam obtidos nem conservados pelos operadores.

Portanto, por via do artigo 14º da Lei do Cibercrime, o operador de comunicações apenas está obrigado a fornecer aqueles dados que efetivamente detenha, dentro dos parâmetros legais.

C. DADOS DE TRÁFEGO E DE CONTEÚDO

7. Os operadores não conservam – estão mesmo proibidos de fazê-lo[2] –, o conteúdo das concretas comunicações. Caso se torne necessário numa investigação criminal obter o conteúdo de comunicações, tal apenas será possível para o futuro e por via da medida processual de interceção de comunicações, em *tempo real*, nos termos do Artigo 18º da Lei do Cibercrime e dos Artigos 187º e 188º do Código de Processo Penal.

8. Já quanto aos chamados *dados de tráfego*[3], no passado existiu no direito português um sistema de retenção sistemática dos mesmos (consagrado na Lei nº 32/2008, de 17 de julho), para efeitos de futura utilização em investigação criminal. Porém o Tribunal Constitucional[4] declarou a inconstitucionalidade com força obrigatória geral do essencial das suas normas – e em particular dos seus artigos 4º e 6º, que obrigavam os operadores de comunicações a guardar todos os dados referentes ao tráfego das comunicações, pelo prazo de um ano.

Como efeito desta declaração de inconstitucionalidade, os operadores de comunicações deixaram de estar sujeitos a tal obrigação passando, pelo contrário, a ter a genérica imposição de eliminar os dados, ou de torná-los anónimos, quando deixarem de ser necessários para efeitos do estabelecimento da comunicação.

9. A proibição genérica de conservação de dados de tráfego está consagrada no artigo 4º, nº 2, da Lei nº 41/2004, de 18 de agosto e é corroborada pelo Artigo 6º, nº 1, da mesma lei, que estipula que, "*os dados de tráfego relativos aos assinantes e utilizadores tratados e armazenados pelas*

[2] Por força do nº 2 do Artigo 1º da Lei nº 32/2008, de 17 de julho, que estipula que "*a conservação de dados que revelem o conteúdo das comunicações é proibida*" e também do nº 2 do Artigo 4º da Lei nº 41/2004, de 18 de Agosto, que proíbe, foram do contexto processual penal, a *escuta*, *interceção* e *armazenamento de comunicações*. Esta proibição decorre também dos Artigos 32º, nº 8 e 34º, nº 4, da Constituição da República.

[3] São definidos no artigo 2º, alínea c) da Lei do Cibercrime, como *"os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente*".

[4] Pelo Acórdão nº 268/2022, de 19 de abril de 2022 (http://www.tribunalconstitucional.pt/tc/acordaos/20220268.html).

empresas que oferecem redes e ou serviços de comunicações eletrónicas devem ser eliminados ou tornados anónimos quando deixem de ser necessários para efeitos da transmissão da comunicação". No quadro legal vigente o princípio geral é, pois, o da obrigação de eliminação dos dados relativos ao tráfego logo que a comunicação terminar.

10. Portanto, no sistema jurídico português, embora com importantes exceções, que de seguida se verão, é genericamente proibido aos operadores de comunicações guardarem, quer o conteúdo das comunicações dos seus clientes, quer os dados de tráfego referentes às mesmas.

D. DADOS DE FATURAÇÃO

11. No entanto, o mesmo artigo 6º da Lei nº 41/2004, nos nºs 2 e 3, introduz exceções a esta proibição geral, estipulando que os dados de tráfego *necessários à faturação dos assinantes e ao pagamento de interligações* podem ser guardados e tratados até ao final do *período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado*.
Este diploma não fixa o *período legal*, durante o qual o pagamento pode ser reclamado. Porém, a Lei nº 23/96, de 26 de julho, diploma legal que define regras respeitantes à prestação de serviços públicos essenciais, fixa no seu artigo 10º, nº 1, que "*o direito ao recebimento do preço do serviço prestado prescreve no prazo de seis meses após a sua prestação*". Esta baliza temporal é corroborada pelo nº 4 do mesmo artigo 10º, que fixa igualmente em 6 meses o prazo para eventual propositura da ação pelo prestador de serviços. O regime deste diploma é aplicável aos serviços de comunicações eletrónicas, por força do respetivo artigo 1º, nº 2, alínea d).

12. Portanto, quanto a serviços de comunicações eletrónicas, é de 6 meses o prazo que o fornecedor de serviço tem para reclamar o respetivo pagamento. Em consequência, somente decorridos esses 6 meses tem efetiva aplicação a obrigação de eliminação dos dados de tráfego, fixada pelo Artigo 6º, nº 1 da Lei nº 41/2004.
É também apenas nessa altura que se torna efetiva a proibição genérica de guarda dos dados de tráfego necessários à faturação, consagrada no Artigo 4º, nº 2, da mesma lei.

13. Esta conservação de dados de tráfego necessários à faturação não é uma imposição legal aos operadores de serviços de comunicações eletrónicas, antes sendo uma permissão: isto é, de acordo com a lei[5], os operadores *podem*, se assim o entenderem, conservar os dados que entenderem, pelo período que entenderem, não tendo qualquer obrigação de o fazer.

[5] Artigo 6º, nº 2 da Lei nº 41/2004.

14. Quando o Acórdão do Tribunal Constitucional nº 268/2021, de 19 de abril de 2022, que acima se referiu, declarou inválidas normas da Lei nº 32/2008, apesar de no seu texto referir a Lei nº 41/2004, de 18 de agosto, nada decidiu quanto a ela. Tem assim de entender-se que este diploma está em vigor e pode – e deve – aplicar-se ao caso concreto.

Esta Lei transpôs para a ordem jurídica nacional a Diretiva nº 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, ela mesma nunca impugnada nas instâncias jurisdicionais da União Europeia. O artigo 6º da Diretiva nº 2002/58/CE, tal como o correspondente artigo 6º da Lei nº 41/2004, permite a recolha e tratamento de "*dados de tráfego necessários para efeitos de faturação dos assinantes*", sendo este tratamento permitido "*até ao final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado*". Como se viu, no ordenamento jurídico português, este período é de 6 meses.

D. a) acesso a dados de faturação e ao endereço IP, até seis meses após a comunicação

15. Já acima se referiu que a jurisprudência do Tribunal de Justiça de União Europeia é favorável à conservação generalizada de dados relativos à identidade civil dos subscritores de serviços. Do mesmo modo, é igualmente favorável à conservação geral e indiscriminada dos endereços de IP na origem de uma comunicação e à sua utilização na investigação de criminalidade grave. A jurisprudência constitucional portuguesa vai no mesmo sentido.

O artigo 14º da Lei do Cibercrime (e em particular os seus nºs 1 e 4) permite ao Ministério Público solicitar a operadores de comunicações dados de que legitimamente disponham (que não sejam dados de tráfego ou conteúdo). Esta norma legitima que, em processo penal, se solicite a operadores de comunicações dados que estes tenham guardado ao abrigo do artigo 6º da Lei nº 41/2004 (portanto, dados conservados até 6 meses após o estabelecimento de uma comunicação).

16. Estes dados incluem informações que permitam apurar a identidade do cliente do fornecedor de serviços que, num determinado contexto temporal (dia e hora) utilizou um determinado endereço IP. O mesmo sucede se a investigação tiver necessidade de saber qual foi o concreto endereço IP utilizado por um determinado cliente de um operador. Apesar de este tipo de informação estar tecnicamente relacionado com tráfego de comunicações, o regime jurídico da sua obtenção, em processo penal, é o mesmo dos *dados de subscritor,* por imposição do artigo 14º, nº 4, alínea b) da Lei do Cibercrime[6].

[6] Está em causa, em particular, o segmento desta alínea que identifica como dados de subscritor "*a identidade, a morada postal ou geográfica e o número de telefone do assinante, e* ***qualquer outro número de acesso***".

Portanto, de acordo com o regime legal que se descreveu, os operadores de comunicações podem guardar registo de endereços de IP utilizados pelos seus clientes e o Ministério Público pode, em investigação criminal, solicitar-lhes esta informação.

D. b) acesso a dados de tráfego até seis meses após a comunicação

17. A categoria dos "*dados de tráfego necessários à faturação dos assinantes e ao pagamento de interligações*", descrita no nº 2 do artigo 6º da Lei nº 41/2004, não é taxativa, dela fazendo parte "*designadamente*", os elementos descritos naquela disposição, tal como vários outros, potencialmente úteis a investigações criminais. É, por exemplo, o caso de eventuais dados de tráfego guardados por serem relevantes para faturação.
O acesso a tais dados não é permitido ao Ministério Público, nos termos do artigo 14º, nº 4 da Lei do Cibercrime. Porém, ainda assim, os mesmos podem ser obtidos no decurso de uma investigação criminal, no contexto do artigo 189º do Código de Processo Penal. Esta norma, no seu nº 2, regula a obtenção em inquérito, entre outros, "*de registos da realização de conversações ou comunicações*", fixando que esta diligência probatória siga o regime procedimental utilizado para as interceções de comunicações telefónicas.

18. Aquando da sua introdução, na reforma processual penal de 2007, esta norma pretendia legitimar a utilização como prova de dados de tráfego ou, no contexto telefónico, da chamada *faturação detalhada*. A norma mantém-se em vigor, permitindo que se obtenham, em processo penal, registos de tráfego de comunicações em geral. A obtenção deste tipo de prova segue o regime (que se aplica por remissão) das interceções telefónicas, previsto no artigo 187º do Código de Processo Penal. Ou seja, desde logo, apenas podem ser obtidos dados de tráfego em investigações de crimes incluídos no catálogo do artigo 187º, nº 1 do Código de Processo Penal. Além disso, esta obtenção terá que ser autorizada pelo juiz de instrução e apenas o pode ser em relação a "*suspeitos ou arguidos, pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido ou a vítimas, mediante o respetivo consentimento*".

E. O NOVO REGIME DE CONSERVAÇÃO DE DADOS ATÉ UM ANO

19. O novo regime introduzido pela Lei nº 18/2024 ao artigo 6º, nº 1 da Lei nº 32/2008 cria uma obrigação específica de guarda de certo tipo de dados: impõe aos operadores de serviços de comunicações que guardem, pelo período de um ano "*os dados relativos à identificação civil dos assinantes ou utilizadores de serviços de comunicações publicamente disponíveis ou de uma rede*

pública de comunicações", "*os demais dados de base*" e os "*os endereços de protocolo IP atribuídos à fonte de uma ligação*". Trata-se de uma opção legislativa equívoca que, na aplicação prática, coloca desafios ao intérprete.

E. a) os dados *dos assinantes* já antes se guardavam

20. Quanto aos "*dados relativos à identificação civil dos assinantes ou utilizadores de serviços de comunicações publicamente disponíveis ou de uma rede pública de comunicações*", na verdade, a nova lei não introduz qualquer alteração substancial ou obrigação adicional.

Efetivamente, por razões contratuais e comerciais, aqueles dados já anteriormente a esta lei tinham de ser guardados pelos operadores, normalmente até mesmo por um tempo muito mais prolongado que um ano. Trata-se de informações e dados excluídos do sigilo de telecomunicações, que são essenciais à execução do contrato entre o prestador de serviços e o cliente e, portanto, têm que ser guardadas, pelo menos, enquanto durar a execução do contrato. Acrescem, além disso, designadamente e entre outras, obrigações fiscais.

Portanto, esta nova obrigação introduzida na Lei nº 32/2008 não se afigura verdadeiramente consequente: não acarreta qualquer obrigação adicional para os operadores de serviços e, por outro lado, não faculta às autoridades de justiça criminal qualquer informação adicional que possa ser útil em investigações criminais.

E. b) não existe um conceito legal de *dados de base*

21. Quanto à obrigação de guardar "*os demais dados de base*", impõe-se uma análise mais circunstanciada. É que a expressão "*dados de base*" não tem consagração legal em Portugal. Portanto, não há nenhum conceito legal a que o intérprete possa recorrer para alcançar a que realidade está o legislador a referir-se.

"*Dados de base*" foi um conceito acolhido pela doutrina nacional na década de 1990, designadamente em pareceres do Conselho Consultivo da Procuradoria-Geral da República, importado de doutrina francófona desse tempo. Nessa época história a lei não densificava ainda – antes desconhecia –, as diversas categorias técnicas de dados, como hoje se identificam.

Assim acontecia com o Decreto-Lei nº 188/81[7], de 2 de fevereiro, que estabeleceu os princípios gerais das comunicações, tal como veio a acontecer com a Lei de Bases das Telecomunicações de 1989 (Lei nº 88/89[8], de 11 de setembro), que revogou aquele diploma de 1981. Da mesma forma, também não continha qualquer definição desta natureza a Lei nº 91/97[9], de 1 de agosto, que

[7] https://diariodarepublica.pt/dr/detalhe/decreto-lei/188-1981-578692.
[8] https://diariodarepublica.pt/dr/detalhe/lei/88-1989-547200.
[9] https://diariodarepublica.pt/dr/detalhe/lei/91-141831.

revogou a Lei nº 88/89 e definiu as bases gerais para o estabelecimento, gestão e exploração de redes de telecomunicações e a prestação de serviços de telecomunicações. Esta Lei nº 91/97 veio a ser revogada pela Lei nº 5/2004[10], de 10 de fevereiro, que por sua vez foi revogada pela Lei nº 16/2022[11], de 16 de agosto (Lei das Comunicações Eletrónicas), a qual é o atual marco normativo em vigor a este respeito.

22. Em nenhum destes sucessivos diplomas normativos encontrou consagração a expressão "*dados de base*". Na Lei nº 91/97, de 1 de agosto, hoje revogada, definiam-se "*telecomunicações*"[12], no artigo 2º, nº 1. Por sua vez, também na atualmente vigente Lei das Comunicações Eletrónicas (Lei nº 16/2022, de 16 de agosto), não se inclui qualquer definição de "*dados de base*". A própria Lei nº 32/2008, que no seu artigo 2º inclui diversas definições (como por exemplo de "*dados*", a este respeito referindo "*dados de tráfego*" e "*dados de localização*", desconhece o conceito de "*dados de base*". Importa recordar que, na Lei nº 41/2004, de 18 de agosto (tratamento de dados pessoais e privacidade no sector das comunicações eletrónicas), se encontram duas definições pertinentes a este propósito: no seu artigo 2º, este diploma define "*dados de tráfego*"[13] e "*dados de localização*"[14]. Importa também referir que a Lei do Cibercrime inclui duas definições próximas: por um lado, no artigo 2º, alínea c), consagra-se a definição de "*dados de tráfego*"[15]; por outro lado, no artigo 14º, nº 4, definem-se "*dados relativos aos clientes ou assinantes*". Estes últimos são descritos como "*qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; a identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços*". Trata-se de uma definição muito ampla e com grande relevância prática.

---

[10] https://diariodarepublica.pt/dr/detalhe/lei/5-2004-581061.
[11] https://diariodarepublica.pt/dr/detalhe/lei/16-2022-187481298.
[12] "*Por telecomunicações entende-se a transmissão, receção ou emissão de sinais, representando símbolos, escrita, imagens, sons ou informações de qualquer natureza por fios, por sistemas óticos, por meios radioelétricos e por outros sistemas eletromagnéticos*".
[13] "*Quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma*".
[14] "*Quaisquer dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações eletrónicas acessível ao público*".
[15] "*Os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente*".

23. Como acima se referiu, "*dados de base*" é um conceito meramente doutrinário, importado da doutrina francófona[16] por Pareceres do Conselho Consultivo do Ministério Público[17], ao qual nunca foi dada consagração legal. Segundo aqueles pareceres, a doutrina incluiria neste conceito os "*dados relativos à conexão à rede, ditos dados de base*", sendo muito relevante considerar que este conceito respeitava apenas (porque era a única realidade relevante na época em que foi desenvolvido) às redes telefónicas – nunca tendo sido aplicado às muito mais complexas e diversas redes de comunicações digitais ou eletrónicas.

Neste contexto, ao não haver uma definição legal de "*dados de base*", não se afigura que possam os operadores de serviços identificar com rigor a que realidade se refere a mesma. Por isso, deste trecho legal da nova redação da Lei nº 32/2008 não é possível retirar efetivamente qualquer nova obrigação de conservação de dados – tanto mais que uma tal conservação, ao ser uma exceção à regra (de não conservação), exigiria uma rigorosa identificação dos dados sobre os quais incidiria.

E. c) a conservação do endereço IP até um ano

24. A nova lei impõe ainda uma última obrigação: a de conservar, pelo período de um ano a contar da data da conclusão da comunicação, "*os endereços de protocolo IP atribuídos à fonte de uma ligação*". Esta sim, é uma inovação legal clara e rigorosa.

De acordo com a alínea c) do nº 1 do novo artigo 6º da Lei nº 32/2008, ficam os operadores de serviços de comunicações obrigados a guardar, *ope legis* e durante um ano após o estabelecimento da comunicação, todos os endereços de IP associados à origem daquela comunicação.

25. Todavia, o acesso a esta informação é legalmente muito limitado e condicionado, no contexto da investigação criminal. Nos termos do artigo 9º da Lei nº 32/2008, o acesso a ela depende sempre de despacho fundamentado de juiz de instrução criminal e apenas pode ser autorizado "*se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter*". Além disso, este acesso é apenas permitido "*no âmbito da investigação, deteção e repressão de crimes graves*" (artigo 9º, nº 1).

[16] Adaptado do pequeno artigo "*Noveaux compléments au service teléphonique et protection des donnés: à la recherche d'un cadre conceptuel*", publicado em 1990 na revista hoje desaparecida "*Droit de l'Informatique et des Télécoms*", da autoria de Francoise Warrant, Yves Poullet e Robert Queck (https://researchportal.unamur.be/fr/publications/nouveaux-compl%C3%A9ments-au-service-t%C3%A9l%C3%A9phonique-et-protection-des-do-2).

[17] Parecer de 24 de junho de 1994 (https://www.dgsi.pt/PGRP.nsf/7fc0bd52c6f5cd5a802568c0003fb410/9696a77a03325c648025829700354b17?OpenDocument&ExpandSection=-3) e parecer de 2 de maio de 1996 (https://www.ministeriopublico.pt/pareceres-pgr/8833).

São crimes graves, de acordo com o artigo 2º, nº 1, alínea g) da mesma Lei nº 32/2008, os "*crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou de títulos equiparados a moeda, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima*".

26. Além destas limitações, o acesso a estes dados (endereços de IP de origem das comunicações, até um ano após o estabelecimento das mesmas) supõe ainda a observação de várias outras regras. De entre elas, sublinham-se a limitação pessoal prevista no nº 3 do artigo 9º: os dados apenas podem ser transmitidos ao Ministério Público se respeitarem a vítimas, mediante o seu consentimento, ou a suspeitos ou arguidos (ou ainda a pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido).

Por outro lado, o despacho judicial de autorização de transmissão dos dados ao Ministério Público tem que ser notificado, no prazo máximo de 10 dias a contar da sua prolação, ao "*titular dos dados*" (artigo 9º, nº 7), embora tal notificação possa ser protelada até ao encerramento da fase de investigação, caso a notificação a ponha em causa, ou "*dificultar a descoberta da verdade ou criar perigo para a vida, para a integridade física ou psíquica ou para a liberdade dos participantes processuais e das vítimas do crime*" (artigo 9º, nº 8).

O artigo 9º, nº 4 da lei ainda acrescenta, sem que verdadeiramente fosse necessário fazê-lo, que a decisão judicial "*deve respeitar os princípios da adequação, necessidade e proporcionalidade, designadamente no que se refere à definição das categorias de dados a transmitir*". Estes critérios sempre teriam que ser observados, de acordo com as regras gerais e constitucionais.

F. O NOVO REGIME DE RETENÇÃO DE DADOS DE TRÁFEGO E LOCALIZAÇÃO

27. A nova redação da Lei nº 32/2008 (após a alteração da Lei nº 18/2024, de 5 de fevereiro), introduziu ainda um procedimento especial, que não de processo penal, de conservação de dados de tráfego e localização (artigo 6º, nº 2 da Lei nº 32/2008). Ao contrário do que sucedia com a anterior versão deste diploma, agora já não se prevê um regime de geral de conservação de dados, apenas se prevendo que possa pontual e especificamente suscitar-se tal retenção.

28. Por via deste novo procedimento, é possível impor aos operadores de comunicações que preservem seletivamente dados de tráfego e de localização e que os mantenham conservados por determinado período. Tal imposição requer autorização judicial e apenas pode ser determinada caso haja necessidade daqueles dados, embora exclusivamente para investigação, deteção e repressão de crimes graves (nº 1 do artigo 3º). Esta específica retenção de dados é feita "*sem prejuízo daqueles conservados (…) por força de disposição legal especial*", tais como por exemplo, no âmbito da Lei nº 41/2004.

Importa anotar que apenas podem ser preservados seletivamente dados de tráfego e localização gerados no contexto de comunicações a partir do momento em que os operadores sejam notificados para iniciar tal preservação (nos termos do nº 4 do artigo 6º da Lei 32/2008) e apenas permanecerão conservados pelo período que venha a ser determinado em caso de decisão de autorização proferida nos termos do nº 2 e do nº 3 do artigo 6º da Lei 32/2008.

No caso da necessidade, num concreto processo de inquérito, de preservar dados de tráfego e localização para efeito de prova, quando estejam em causa dados suficientemente precisos e identificáveis, seja através do interveniente ou dispositivo técnico que sejam conhecidos, tais dados podem ser obtidos através da aplicação do regime de interceção de comunicações eletrónicas (artigo 18º da Lei do Cibercrime e artigo 189º do Código de Processo Penal).

29. Esta nova modalidade de conservação de dados é uma possibilidade legal que não se enquadra no contexto de uma concreta investigação criminal. Isto é, não é suposto que seja suscitada no decurso de uma investigação nem decorre das respetivas necessidades de obtenção de prova. Pelo contrário, é independente da existência de um concreto processo de inquérito e não tem que seguir as fórmulas do processo penal nem as regras de recolha de matéria probatória.

No novo quadro legal agora introduzido não se descrevem os específicos critérios que possam fundamentar o pedido desta retenção de dados nem as regras procedimentais a que o pedido está sujeito. Diz-se (artigo 6º, nº 3) que este pedido tem caráter urgente e deve ser decidido no prazo máximo de 72 horas. Também se diz que a apreciação deste pedido compete a uma formação das secções criminais do Supremo Tribunal de Justiça (artigo 6º, nº 7).

Mas não se indica qual a concreta entidade com competência legal para formular o pedido nem quais são as regras procedimentais a observar, designadamente pela estrutura do Ministério Público, nem os requisitos para a sua formulação ou os critérios judiciais da decisão – para além da genérica necessidade para a "*investigação, deteção e repressão de crimes graves*" (nº 1 do artigo 3º), a que já acima se aludiu.

30. Pelo seu caráter não processual penal e ainda pela necessidade de intervenção reguladora que defina procedimentos internos, não cabe a esta Nota Prática fazer análise mais demorada deste particular procedimento.

G. A VIGÊNCIA E PRODUÇÃO DE EFEITOS DA LEI

31. Nos termos da Lei nº 32/2008, o acesso aos dados conservados no respetivo âmbito (quer os dados conservados generalizadamente, por força do nº 1 do artigo 6º, quer os dados seletivamente conservados, ao abrigo dos nºs 2 a 7 do mesmo artigo 6º) tem que ser feito "*mediante comunicação eletrónica*" – nº 3 do artigo 7º da Lei nº 32/2008, em imposição repetida pelo artigo 10º da Lei. Ainda de acordo com este regime, tal comunicação eletrónica deve efetuar-se "*nos termos e condições técnicas e de segurança fixadas em portaria conjunta dos membros do Governo responsáveis pelas áreas da administração interna, da justiça e das comunicações*".

32. A Lei nº 18/2024, de 5 de fevereiro, entrou em vigor no dia seguinte ao da sua publicação, 6 de fevereiro de 2024 – artigo 5º da Lei. O artigo 18º da Lei nº 32/2008, que a Lei nº 18/2024 não alterou, determina e determinava já anteriormente que este diploma apenas "*produz efeitos 90 dias após a publicação da portaria a que se refere o nº 3 do artigo 7º*" – como se referiu, esta norma impõe que a transmissão dos dados eventualmente conservados, ao abrigo desta lei, se processe "*mediante comunicação eletrónica, nos termos das condições técnicas e de segurança fixadas em portaria*". Estas disposições, sublinha-se, constavam da versão originária da Lei nº 32/2008 e mantiveram-se intocadas após a intervenção da Lei nº 18/2024.
No seu tempo, por via da publicação da Portaria nº 469/2009[18], de 6 de maio, a Lei nº32/2008 passou a produzir plenamente os seus efeitos[19]. Sucede, porém, que aquela portaria foi expressamente revogada, pelo artigo 11º, alínea d), da Lei nº 16/2022[20], de 16 de agosto.

33. Afigura-se que esta opção do legislador contrariou norma expressa: com efeito, o artigo 146º[21] do Código do Procedimento Administrativo determina, no seu número 1, que os "*regulamentos podem ser revogados pelos órgãos competentes para a respetiva emissão*". Isto é, de acordo com o Código do Procedimento Administrativo, uma portaria (corpo normativo que se integra no grupo dos regulamentos) não deveria ter sido revogada por uma Lei formal da Assembleia da República,

[18] https://files.diariodarepublica.pt/1s/2009/05/08700/0261002612.pdf.
[19] Esta Portaria, no seu artigo 1º, "*estabelece os termos das condições técnicas e de segurança em que se processa a comunicação eletrónica para efeitos da transmissão de dados de tráfego e de localização (...) nos termos previstos na Lei nº 32/2008*".
[20] https://diariodarepublica.pt/dr/detalhe/lei/16-2022-187481298.
[21] https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2248&tabela=leis.

uma vez que esta última não tem competência regulamentar. Mais ainda: o número 2 do mesmo artigo 146 estipula que "*os regulamentos necessários à execução das leis em vigor ou de direito da União Europeia não podem ser objeto de revogação sem que a matéria seja simultaneamente objeto de nova regulamentação*". Isto é, para que legalmente tivesse sido permitida a revogação da Portaria nº 469/2009, deveria ter sido publicada, em simultâneo, uma nova portaria, que em substância a substituísse.

Estas normas e princípios não foram respeitadas pelo legislador de 2022. Porém, precisamente para permitir a superação de lacunas e contradições que possam ter origem em situações desta natureza, o Código de Procedimento Administrativo inclui uma norma que pretende conferir eficácia àquelas disposições, ainda que as mesmas sejam violadas: o número 3 do artigo 146º determina que, caso aquelas normas sejam violadas, "*consideram-se em vigor, para todos os efeitos, até ao início da vigência do novo regulamento, as normas regulamentares do diploma revogado de que dependa a aplicabilidade da lei exequenda*". Isto é, mesmo tendo a Portaria nº 469/2009 sido expressamente revogada pela Lei nº 16/2022, de forma automática e por mera operação da lei, devem considerar-se repristinadas as normas nela incluídas das quais dependia a produção de efeitos da Lei nº 32/2008. Serão, pois, tais normas (até publicação de uma nova portaria) que terão que utilizar-se para dar efeito ao artigo 7º da Lei nº 32/2008. Desta solução legal resulta que a Lei nº 32/2008, além de estar em vigor, produz plenamente os seus efeitos.

H. A POSSIBILIDADE GERAL DE PRESERVAÇÃO DE DADOS

34. À margem dos regimes de guarda dos dados pelos operadores de comunicações, importa recordar que a lei prevê a geral possibilidade de as autoridades judiciárias ordenarem a preservação de dados que estejam em risco de "*deixar de estar disponíveis*" (artigo 12º, nº 1, da Lei do Cibercrime). Assim, se numa investigação em concreto se aperceber que determinados dados, incluindo dados de subscritor, tráfego ou faturação, estiverem em *risco de deixar de estar disponíveis*, a autoridade judiciária pode ordenar a "*quem tenha disponibilidade ou controlo desses dados, designadamente a fornecedor de serviço, que preserve os dados em causa*".

Esta possibilidade legal é particularmente útil quando a investigação se apercebe de que o prazo de conservação de dados está próximo do seu termo. Pode mesmo ser desencadeada por iniciativa de órgão de polícia criminal, "*quando haja urgência ou perigo na demora*" (artigo 12º, nº 2 da Lei do Cibercrime).

Legalmente, os dados em causa podem ser preservados por um período máximo de três meses, o qual pode ser renovado por períodos não superiores a três meses, desde que se verifiquem os

respetivos requisitos de admissibilidade, até ao limite máximo de um ano (artigo 12º, nº 3, alínea c) e nº 5 da Lei do Cibercrime).

I. TABELA DE SUMÁRIO

35. Sumariam-se de seguida os diferentes tipos de dados que em investigação criminal se podem solicitar aos operadores de comunicações. Refere-se o universo de inquéritos (com referência ao tipo de crime em investigação) em que é legítimo solicitar os dados. Acrescenta-se o prazo durante o qual os dados estão disponíveis, a partir da data da comunicação. Indica-se ainda a autoridade processual competente para solicitar os dados, bem como o respetivo fundamento legal.

TIPO DE DADOS	ÂMBITO	PRAZO	AUTORIDADE COMPETENTE PARA AUTORIZAR	FUNDAMENTO LEGAL
dados de subscritor[22]	todos os crimes	sem prazo	Ministério Público	artigo 6º, nº 2, da Lei nº 41/2004 e artigo 14º, nº 4, da Lei do Cibercrime
dados de subscritor[23]	crimes graves[24]	um ano	Juiz de Instrução	artigo 6º, nº 1 e artigo 9º da Lei nº 32/2008
endereço IP	todos os crimes	6 meses	Ministério Público	artigo 6º, nº 2, da Lei nº 41/2004 e artigo 14º, nº 4, b) da Lei do Cibercrime
endereço IP	crimes graves[25]	um ano	Juiz de Instrução	artigo 6º, nº 1 e artigo 9º da Lei nº 32/2008
dados de tráfego[26]	catálogo do artigo 187º do CPP	6 meses	Juiz de Instrução	artigos 187º e 189º, nº 2 do CPP
conteúdo de comunicações	catálogos do artigo 187º do CPP e do artigo 18º da Lei do Cibercrime	(interceção de comunicações - futuras)	Juiz de Instrução	artigos 187º e 188º, nº 2 do CPP e artigo 18º da Lei do Cibercrime

[22] Definidos no artigo 14º, nº 4, da Lei do Cibercrime como os "*dados relativos aos clientes ou assinantes*", isto é, "*qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos ou sob qualquer outra forma, detida pelo fornecedor de serviços, e que permita determinar o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas a esse respeito e o período de serviço; a identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso, os dados respeitantes à faturação e ao pagamento, disponíveis com base num contrato ou acordo de serviços; ou qualquer outra informação sobre a localização do equipamento de comunicação, disponível com base num contrato ou acordo de serviços*".
[23] Ver nota anterior.
[24] São crimes graves (artigo 2º, nº 1, alínea g) da Lei nº 232/2008): "*crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou de títulos equiparados a moeda, contrafação de cartões ou outros dispositivos de pagamento, uso de cartões ou outros dispositivos de pagamento contrafeitos, aquisição de cartões ou outros dispositivos de pagamento contrafeitos, atos preparatórios da contrafação e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima*".
[25] Ver nota anterior.
[26] O artigo 2º, alínea c) da Lei do Cibercrime define-os como "*os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente*".