SEPARATA RPDC N.º 3 (2023)

REVISTA PORTUGUESA DE DIREITO CONSTITUCIONAL

PORTUGUESE REVIEW OF CONSTITUTIONAL LAW

AATRIC

*Conservação de Metadados – O Acórdão n.º 268/2022**

Sónia Fidalgo

Professora Auxiliar da Faculdade de Direito da Universidade de Coimbra
sfidalgo@fd.uc.pt

I. Evolução legislativa relativa a metadados

Quando, em 1987, foi aprovado o atual Código de Processo Penal (CPP), nele não se encontrava qualquer norma que se referisse à utilização dos metadados como meio de prova. Tal veio a acontecer apenas com a revisão introduzida no CPP pela Lei n.º 48/2007, de 29 de agosto. O artigo 189.º, n.º 2, do CPP passou então a prever que "a obtenção e junção aos autos de dados sobre a localização celular ou de registos da realização de conversações ou comunicações só podem ser ordenadas ou autorizadas, em qualquer fase do processo, por despacho do juiz, quanto a crimes previstos no n.º 1 do artigo 187.º e em relação às pessoas referidas no n.º 4 do mesmo artigo".

Cerca de um ano depois foi aprovada a Lei n.º 32/2008, de 17 de julho, que transpôs para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações. Esta lei veio regular expressamente a conservação e a transmissão dos dados de tráfego e de localização, para fins de investigação, deteção e repressão de crimes graves (artigo 1º). Manteve-se, porém, inalterado até hoje o disposto no artigo 189.º, n.º 2, do CPP, o que tem gerado diversos problemas de interpretação[1].

---

* Este texto corresponde, com ligeiros desenvolvimentos e algumas alterações essencialmente formais, à conferência apresentada no *V Seminário da Associação dos Assessores do Tribunal Constitucional – Jurisprudência Constitucional Recente*, que decorreu na Sala de Atos do Tribunal Constitucional, no dia 14 de dezembro de 2022. Na conferência, longe de aspirarmos a um tratamento profundo do tema, procedemos apenas a uma análise crítica do Acórdão n.º 268/2022. Nesta publicação mantivemos o nosso propósito inicial, sem qualquer atualização do texto partilhado naquele dia.

[1] Cf. também Rui Cardoso, "A conservação e a utilização probatória de metadados de comunicações eletrónicas após o Acórdão do Tribunal Constitucional n.º 268/2022 – *o que nasce torto...*", *Revista do Ministério Público* 172 (2022), p. 14.

Cerca de um ano depois, foi aprovada a Lei n.º 109/2009, de 16 de setembro (Lei do Cibercrime), transpondo para a ordem jurídica interna a Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção do Conselho da Europa sobre o Cibercrime. Também em 2009, o legislador não se preocupou em harmonizar o disposto nesta nova lei com o que se encontrava já no CPP. A Lei do Cibercrime compreende um regime geral sobre recolha de prova em suporte eletrónico, aplicável em processo por qualquer crime (cf. artigo 11.º, n.º 1, alínea *c*))[2]; não se trata de regras processuais específicas para o sector da cibercriminalidade ou que se estendam também apenas aos processos por crimes praticados por meio de sistemas informáticos. Não se compreende, por isso, por que razão estas regras não foram inseridas no Código de Processo Penal[3].

Por outro lado, é certo que a Lei do Cibercrime não tem normas sobre a conservação dos dados[4], mas tem disposições sobre o acesso e a utilização de dados informáticos, que são de difícil harmonização com o que se encontra na Lei n.º 32/2008[5]. E o artigo 11.º, n.º 2, da Lei do Cibercrime estabelece que "as disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008".

II. O Acórdão do Tribunal Constitucional n.º 268/2022

No contexto nacional e supranacional de todos conhecido, em agosto de 2019, a Senhora Provedora de Justiça requereu a fiscalização abstrata da constitucionalidade dos artigos 4.º, 6.º e 9.º da Lei n.º 32/2008.

Abreviadamente, poderemos dizer que nos termos destas normas: os fornecedores de serviços de comunicações eletrónicas publicamente disponíveis

[2] Sobre a distinção entre prova eletrónica e prova digital, cf. David Silva Ramalho, *Métodos Ocultos de Investigação em Ambiente Digital*, Coimbra: Almedina, 2017, p. 98 e ss.

[3] Refutando os argumentos apresentados na Exposição de Motivos da Proposta de Lei n.º 289/X/4ª para o enquadramento sistemático adotado pelo legislador e defendendo que estas normas processuais deveriam ter sido inseridas no Código de Processo Penal, cf. Paulo Dá Mesquita, "Prolegómenos sobre prova electrónica e intercepção de telecomunicações no Direito Processual Penal Português – o Código e a Lei do Cibercrime", *in*: *Processo Penal, Prova e Sistema Judiciário*, Coimbra: Coimbra Editora, 2010, p. 98 e ss.; cf., ainda, João Conde Correia, "Prova digital: as leis que temos e a lei que devíamos ter", *Revista do Ministério Público* 139 (2014), p. 35.

[4] Note-se que *conservação de dados* (regulada nos termos da Lei n.º 32/2008) é diferente de *preservação expedita de dados* (prevista no artigo 12.º da Lei do Cibercrime). Cf., *infra*, ponto IV.2.

[5] Sobre estas dificuldades de harmonização, cf. Carlos Pinho, "Os problemas interpretativos resultantes da Lei n.º 32/2008, de 17 de Julho (Conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações)", *Revista do Ministério Público* 129 (2012), p. 63 e ss.

têm o dever de conservar os dados de tráfego e de localização de todas as comunicações eletrónicas (artigo 4.º); os dados devem ser conservados pelo período de um ano (artigo 6.º); a conservação é feita para fins de investigação, deteção e repressão de crimes graves, sendo certo que a transmissão dos dados só pode ser autorizada por despacho fundamentado do juiz de instrução, mediante requerimento do Ministério Público ou da autoridade de polícia criminal competente (artigo 9.º).

No Acórdão n.º 268/2022, de 19 abril de 2022, o Tribunal Constitucional decidiu "declarar a inconstitucionalidade, com força obrigatória geral, da norma constante do artigo 4º da Lei n.º 32/2008, de 17 de julho, conjugada com o artigo 6.º da mesma lei, por violação do disposto nos números 1 e 4 do artigo 35.º [direito à autodeterminação informativa] e do n.º 1 do artigo 26.º [direitos à reserva da intimidade da vida privada e familiar], em conjugação com o artigo 18.º, n.º 2, todos da Constituição". Quanto aos dados de base e ao endereço IP, o Tribunal Constitucional decidiu pela inconstitucionalidade das normas, porque a lei não prescreve a obrigatoriedade de os dados serem conservados em território da União Europeia. Quanto aos dados de tráfego e de localização, o Tribunal Constitucional decidiu pela inconstitucionalidade das normas por duas ordens de razões: por um lado, por a lei não prescrever a obrigatoriedade de os dados serem conservados em território da União Europeia; por outro lado, devido ao caráter *generalizado* da conservação dos dados (são conservados os dados de todos os utilizadores e assinantes, atingindo-se assim "sujeitos relativamente aos quais não há qualquer suspeita de atividade criminosa"[6]).

O Tribunal Constitucional decidiu ainda "declarar a inconstitucionalidade, com força obrigatória geral, da norma do artigo 9.º da Lei n.º 32/2008, de 17 de julho, relativa à transmissão de dados armazenados às autoridades competentes para investigação, deteção e repressão de crimes graves, na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, a partir do momento em que tal comunicação não seja suscetível de comprometer as investigações nem a vida ou integridade física de terceiros". Esta norma foi declarada inconstitucional por violação do disposto no n.º 1 do artigo 35.º (direito à autodeterminação informativa) e do n.º 1 do artigo 20.º (direito a uma tutela jurisdicional efetiva), em conjugação com o n.º 2 do artigo 18.º, todos da Constituição.

[6] Acórdão n.º 268/2022, ponto 18.

III. Apreciação do Acórdão

Concordo, em geral, com a decisão do Tribunal Constitucional. Também me parece que a conservação, por parte dos fornecedores de serviço, dos dados de tráfego e de localização de todos os assinantes e utilizadores, pelo período de um ano, para a eventualidade de vir a ser necessário a eles aceder com a finalidade de deteção, investigação e repressão de crimes graves restringe, de modo desproporcionado, o direito à autodeterminação informativa (artigo 35.º, n.ºs 1 e 4, da Constituição da República Portuguesa – CRP) e o direito à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1, da CRP).

Parece-me, porém, que as normas constantes dos artigos 4.º e 6.º da referida Lei n.º 32/2008, ao determinarem a conservação generalizada dos dados de tráfego gerados pelas comunicações entre pessoas (ou a sua tentativa), materializam também uma restrição desproporcionada do direito à inviolabilidade das comunicações, consagrado no artigo 34.º, n.º 4, da CRP. Esta ideia consta, aliás, de uma das declarações de voto conjuntas[7]. A Constituição consagra para a inviolabilidade das comunicações uma garantia constitucional autónoma em relação àquela que decorre do n.º 1 do artigo 26.º da CRP. Encontramos, no artigo 34.º, a proteção de uma esfera de privacidade e de sigilo no domínio específico das comunicações interpessoais, "com um regime de inviolabilidade mais intenso e cujas exceções são constitucionalmente determinadas"[8]. E, de acordo com jurisprudência anterior do próprio Tribunal, esta "defesa constitucional independente quanto à proteção das comunicações" abrange não apenas o *conteúdo* da comunicação, mas também os dados de tráfego gerados a seu propósito[9].

Parece-me, por isso, que deveria ter sido mobilizado como parâmetro do juízo de inconstitucionalidade o direito consagrado nos n.ºs 1 e 4 do artigo 34.º da Constituição.

Quanto à declaração de inconstitucionalidade da norma do artigo 9.º, relativa à transmissão de dados armazenados, na parte em que não prevê uma notificação ao visado de que os dados conservados foram acedidos pelas autoridades de investigação criminal, tenho dúvidas de que deva considerar-se que tal previsão deveria constar expressamente do regime de conservação e transmissão dos dados regulado na Lei n.º 32/2008.

[7] Declaração de voto conjunta (Afonso Patrão, José João Abrantes, Assunção Raimundo, Mariana Canotilho).

[8] *Id*.

[9] Cf. Acórdão n.º 403/2015, referido na declaração de voto conjunta (Afonso Patrão, José João Abrantes, Assunção Raimundo, Mariana Canotilho).

O acesso, por parte do Ministério Público ou das autoridades de polícia criminal aos dados de tráfego e de localização consubstancia, neste contexto, um meio de obtenção de prova em processo penal. E, nos termos da Lei n.º 32/2008, a transmissão destes dados ao processo penal só é admissível mediante despacho fundamentado do juiz de instrução, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter (artigo 9.º, n.º 1). Neste domínio, o juiz de instrução vai intervir precisamente como juiz das liberdades; o controlo da legalidade da transmissão dos dados é feito pelo próprio juiz. É esta a função do juiz de instrução neste contexto; é este o modelo no nosso processo penal.

Por outro lado, estando em causa um meio de obtenção de prova em processo penal, terão, neste domínio, total aplicação as regras do Código de Processo Penal (CPP) relativas à produção e valoração de prova. No caso de se verificar uma violação do regime previsto na Lei n.º 32/2008 – imagine-se, por exemplo, que o fornecedor de serviço transmite os dados diretamente à autoridade de polícia criminal, sem despacho prévio do juiz instrução – entrar-se-á no domínio das proibições de prova, sujeito, por isso, ao regime estabelecido no artigo 126.º do CPP. Tratando-se de uma prova obtida mediante intromissão na vida privada e nas telecomunicações, tal prova será nula e não poderá ser valorada.

Não me parece, por isso, que possa dizer-se que "a inexistência da notificação aos visados de que os seus dados foram acedidos pelos órgãos competentes pela investigação criminal (…) impedirá que estes possam exercer um controlo jurisdicional da legalidade daquela transmissão"[10]. Este acesso aos dados por parte do Ministério Público ou das autoridades de polícia criminal nos termos previstos na Lei n.º 32/2008 ficará sempre a constar dos autos, e o arguido terá acesso a esses elementos, se não antes – dada a possibilidade de sujeição do processo a segredo durante a fase de inquérito – pelo menos, no momento do encerramento do inquérito (e, neste momento, surgirá a possibilidade de requerimento de abertura de instrução).

Além disso, e como se refere no Acórdão[11], a lei que aprovou as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais (Lei n.º 59/2019, de 8 de agosto) determina que o responsável pelo armazenamento dos dados é obrigado a facultar ao titular dos dados pessoais retidos, a seu pedido,

[10] Ponto 19 do Acórdão n.º 268/2022.

[11] Ponto 19.1. do Acórdão n.º 268/2022.

informações sobre a sua transmissão (artigos 13.º e 15.º, n.º 2, alínea *c*)), podendo este apresentar queixa à autoridade de controlo no caso de eventuais violações do regime jurídico (artigo 15.º, n.º 2, alínea *f*)). Estabelecendo a lei expressamente que a informação de que os dados foram transmitidos pode ser recusada para evitar prejuízos para investigações criminais (artigo 16.º, n.º 1)[12], prevêem-se nela mecanismos judiciais e administrativos de controlo de eventuais recusas dessa transmissão (artigo 18.º). Por outro lado, ainda, quer a Lei n.º 32/2008 (artigos 12.º e 13.º), quer a Lei n.º 59/2019 (artigos 52.º a 60.º) preveem contraordenações e crimes para o caso de violação das regras nelas estabelecidas.

Concluindo-se – como, aliás, se conclui no próprio Acórdão – que o ordenamento jurídico português "atribui ao titular dos dados o direito a *conhecer* que estes foram transmitidos às autoridades de investigação criminal" quando essa informação já não for prejudicial para investigações criminais em curso[13], duvido que deva afirmar-se que a ausência de previsão da notificação do visado restringe "de modo desproporcionado o direito à autodeterminação informativa, consagrado no artigo 35.º, n.º 1, da Constituição (na dimensão de controlo do acesso de terceiros a dados pessoais) afetando, igualmente, o direito a uma tutela jurisdicional efetiva (artigo 20.º, n.º 1, da Constituição), por prejudicar a viabilidade prática de exercício de controlo judicial de acessos abusivos ou ilícitos aos dados conservados"[14].

Por todas estas razões, tenho dúvidas que o direito à autodeterminação informativa (artigo 35.º, n.º 1, da CRP) e o direito a uma tutela jurisdicional efetiva (artigo 20.º, n.º 1, da CRP), devessem ter sido mobilizados como parâmetros do juízo positivo de inconstitucionalidade.

IV. Consequências da declaração de inconstitucionalidade

Uma palavra, agora, sobre as consequências, no processo penal, da declaração de inconstitucionalidade das normas referidas. Neste domínio as questões são muito diversas. Selecionei, por isso, algumas áreas problemáticas sobre as quais gostaria que refletíssemos.

[12] Já se previa também a dispensa de obrigação de informação relativa à comunicação de dados por motivos de investigação criminal no artigo 10º, n.º 5, da Lei de Proteção de Dados Pessoais (Lei n.º 67/98, de 26 de outubro).

[13] Ponto 19.2. do Acórdão n.º 268/2022 (itálicos do Acórdão).

[14] Ponto 19.2. do Acórdão n.º 268/2022.

1. O acesso ao endereço IP

Desde que entrou em vigor a Lei do Cibercrime (Lei n.º 109/2009), tem sido muito discutida a questão de saber se a ordem de acesso a um endereço IP deve seguir o regime previsto na Lei n.º 32/2008 – acesso restrito à investigação de crimes graves e mediante autorização do juiz de instrução – ou se, quando o processo se encontra na fase de inquérito, a ordem poderá ser dirigida aos fornecedores de serviço pelo próprio Ministério Público.

No âmbito dos metadados – os dados que não abrangem o conteúdo das comunicações, mas dizem respeito somente às suas circunstâncias (são os dados sobre dados) –, a jurisprudência constitucional tem vindo a fazer uma distinção (que manteve no acórdão agora em análise) entre *dados de base* e *dados de tráfego*. Os *dados de base* referem-se à conexão à rede, independentemente de qualquer comunicação, permitindo a identificação do utilizador de certo equipamento (nome, morada, número de telefone)[15]. Já os *dados de tráfego* são definidos como "os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência)"[16].

O endereço IP tem vindo a ser integrado pela jurisprudência constitucional na categoria dos *dados de base,* por não revelar quaisquer circunstâncias da comunicação, permitindo apenas a identificação do computador que se conectou à rede. Concordo com esta posição que vem sendo assumida pelo Tribunal Constitucional e que foi reiterada no Acórdão agora em análise[17]: a querer manter-se a distinção entre *dados de base* e

[15] Acórdãos n.ºs 241/2002, 486/2009, 403/2015, 420/2017 e 464/2019, todos referido no ponto 6.1. do Acórdão n.º 268/2022.

[16] Acórdão n.º 403/2015, referido no ponto 6.1. do Acórdão n.º 268/2022.

[17] Cf. ponto 17.1. do Acórdão n.º 268/2022. No Acórdão em análise o Tribunal não deixa de reconhecer que "os protocolos IP podem ser *estáticos* (identificando permanentemente um ponto de acesso à rede) ou *dinâmicos* (sendo atribuídos a certo computador *apenas no momento em que se conexiona à rede e durante a sua ligação*). Quer isto dizer que a identificação de um protocolo IP dinâmico envolve informação da sua utilização *num determinado momento,* revelando não apenas o utilizador como também o uso da internet em certo contexto. Neste quadro, a identificação do sujeito a que estava atribuído determinado *protocolo IP dinâmico* não permite, de forma tão clara, obedecer à divisão entre *dados de base* e *dados de tráfego,* pois certas circunstâncias da comunicação (a data e a hora) são inerentes à identificação do protocolo de IP dinâmico" (ponto 6.1.). O Tribunal conclui, porém, que o regime jurídico-constitucional relevante para apreciação da medida de conservação dos endereços de protocolo IP dinâmicos que identificam a *fonte* da comunicação deve ser o dos *dados de base*. Nos termos do Acórdão, "ainda que seja discutível a respetiva categorização (…), a intensidade de agressão aos direitos à reserva da intimidade da vida privada e à autodeterminação informativa é, neste domínio, similar à dos demais dados de base" (ponto 17.1).

dados de tráfego, o regime jurídico-constitucional relevante para a apreciação da medida de conservação dos endereços IP deve ser o dos *dados de base*.

Volto agora à questão que coloquei há pouco: atendendo ao nosso quadro legal, terá o Ministério Público legitimidade para, durante o inquérito, ordenar ao fornecedor de serviço a comunicação do endereço IP utilizado por um cliente ou a identidade do utilizador da fonte da comunicação a quem estava atribuído o endereço IP num certo momento?

Nos termos do artigo 14.º, n.º 4, da Lei do Cibercrime, a autoridade judiciária competente – portanto, na fase de inquérito, o Ministério Público – "pode ordenar aos fornecedores de serviço que comuniquem ao processo dados relativos aos seus clientes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo".

Quer o Gabinete do Cibercrime, quer a jurisprudência dominante[18] têm considerado que neste conjunto de dados está incluída a informação sobre o endereço concreto de IP utilizado numa determinada comunicação, que esteja já identificada numa investigação. Ou seja, tem-se entendido que é da competência do Ministério Público solicitar aos fornecedores de serviço que indiquem a identidade do seu cliente que, num determinado contexto temporal (dia e hora) utilizou um determinado endereço IP. E o mesmo poderá dizer-se da situação em que na investigação há necessidade de saber qual o endereço IP utilizado por um determinado cliente.

Apesar de os dados referidos no artigo 4.º da Lei n.º 32/2008 abrangerem também o endereço IP, tem-se entendido que o acesso ao endereço IP nos termos agora referidos é regulado no artigo 14.º da Lei do Cibercrime (que, aliás, é posterior à lei de 2008). Tudo ponderado, poderá acabar por se concluir que a declaração de inconstitucionalidade das normas da Lei n.º 32/2008 pode não significar a impossibilidade de acesso aos dados de base (incluído o endereço IP) no âmbito do processo penal[19]. Na verdade, a conservação dos dados por parte dos fornecedores de serviço continua a ser admissível para fins de faturação dos serviços. Da conjugação das normas da Lei dos Serviços Públicos (Lei n.º 23/96, de 26 de julho – artigo 10.º, n.ºs 1 e 4) e da Lei que regula a proteção de dados pessoais e a privacidade nas telecomunicações (Lei n.º 41/2004, de 18 de agosto – artigo 4.º, n.º 3,

[18] Cf. Gabinete do Cibercrime, *Nota prática n.º 3/2013*, bem como a súmula de jurisprudência aí referida. Cf., também, a *Nota prática n.º 1/2012.*

[19] Considerando também que continua a ser admissível o acesso ao endereço IP mesmo após a declaração de inconstitucionalidade do Acórdão n.º 268/2022 do Tribunal Constitucional, David Silva Ramalho, "A importância dos metadados", *Jornal i*, 4 de maio de 2022, p. 18, e Rui Cardoso, "A conservação e a utilização probatória de metadados…", *op. cit.*, p. 58.

e artigo 6.º, n.ºs 2 e 3) resulta que certos dados podem ser conservados pelo fornecedor de serviços, pelo período de 6 meses, para fins de faturação dos serviços.

Deste modo, continuará a ser possível, no âmbito de um processo penal, aceder ao endereço IP nos termos descritos, mesmo após a declaração de inconstitucionalidade das normas da Lei n.º 32/2008. Há, porém, a limitação de os dados só serem conservados pelo período de 6 meses.

2. O acesso aos dados de tráfego e de localização

Quanto ao acesso aos dados de tráfego e de localização, na sequência do acórdão do Tribunal Constitucional, a resposta é mais complexa. Desde logo, a solução não se encontra na Lei do Cibercrime.

Não pode encontrar-se o fundamento legal para o acesso aos dados conservados pelos fornecedores de serviços no artigo 12.º da Lei do Cibercrime (*Preservação expedita de dados*), porque esta norma não prevê a possibilidade de acesso a quaisquer dados, prevendo apenas a possibilidade de ser ordenada a preservação de dados (quando houver receio de que possam perder-se, alterar-se ou deixar de estar disponíveis). Saliente-se, ainda, que o que se prevê nesta norma é uma preservação de dados para o futuro. Ou seja, a ordem de preservação expedita de dados pressupõe que os dados tenham sido previamente conservados (trata-se da preservação de dados já *armazenados num sistema informático*)[20].

Também não pode encontrar-se esse fundamento para o acesso aos dados conservados pelos fornecedores de serviços no artigo 18.º da Lei do Cibercrime. O acesso a metadados conservados não é uma interceção de dados. A interceção (que pode incluir os metadados) é sempre de dados que estão a ser transmitidos em tempo real. Tratar-se-á, sempre, por isso, de transmissões de dados que ocorrem em momento posterior ao despacho que autoriza ou ordena a interceção[21].

E também não pode encontrar-se aquele fundamento no artigo 14.º da Lei do Cibercrime. É certo que nos termos desta norma a autoridade judiciária competente "pode ordenar aos fornecedores de serviço que comuniquem ao processo dados relativos aos seus clientes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo", e que permita, designadamente, obter "informação sobre a localização do equipamento de comunicação disponível com base num acordo de prestação

[20] Assim também, Rui Cardoso, "A conservação e a utilização probatória de metadados…", *op. cit.*, p. 40.

[21] Neste sentido também *ibid.*, p. 41.

de serviços" (n.º 4, alínea *c*)). Tem-se entendido, porém – e bem, do meu ponto de vista – que esta "informação sobre a localização do equipamento de comunicação" não diz respeito à localização dos equipamentos móveis em cada momento, durante cada comunicação. Trata-se sim do local onde o equipamento foi instalado (o serviço de televisão, o telefone fixo, o *router* da internet, etc.).[22]

Questiona-se agora se o fundamento normativo para acesso aos dados de tráfego e localização pode, atualmente, ser o artigo 189.º, n.º 2, do CPP. Esta norma constituía o fundamento normativo para a obtenção de tais dados antes da entrada em vigor da Lei n.º 32/2008. Após a entrada em vigor desta lei, o artigo 189.º, n.º 2, do CPP havia sido parcialmente revogado, de modo tácito[23]. Porém, na sequência da declaração de inconstitucionalidade com força obrigatória geral da norma do artigo 9º da Lei n.º 32/2008, a norma do n.º 2 do artigo 189.º terá sido repristinada (cf. artigo 282.º, n.º 1, da CRP).

Deste modo, sendo os dados de tráfego e de localização conservados pelo prazo de seis meses para efeitos de faturação do serviço (cf. artigo 10.º, n.ºs 1 e 4 da Lei dos Serviços Públicos – Lei n.º 23/96, de 26 de julho; artigo 4.º, n.º 3, e artigo 6.º, n.ºs 2 e 3 da Lei que regula a proteção de dados pessoais e a privacidade nas telecomunicações – Lei n.º 41/2004, de 18 de agosto), poderá a eles aceder-se para obtenção de prova no processo penal. Esclareça-se que o facto de a conservação dos dados ao abrigo da Lei n.º 41/2004 se destinar, num primeiro momento, à proteção da relação contratual no contexto das relações estabelecidas entre as empresas fornecedoras de serviços de comunicações eletrónicas e os seus clientes, não impede que possa aceder-se a esses dados para fins de investigação criminal. Os metadados são um meio de prova – prova documental / digital – e o meio de obtenção de prova a utilizar para a eles aceder será a injunção prevista no artigo 189.º, n.º 2, do CPP[24].

3. A ressalva dos casos julgados

Uma outra questão muito discutida na sequência do Acórdão foi a dos efeitos da declaração de inconstitucionalidade. Não tendo sido fixados efeitos

[22] Precisamente nestes termos, com justificação pormenorizada, *ibid*., p. 50-51.

[23] Sobre a questão da revogação / derrogação da norma do artigo 189.º do CPP, cf. Paulo Dá Mesquita, "Prolegómenos sobre prova electrónica…", *op. cit.*, p. 117, Rita Castanheira Neves, *As ingerências nas comunicações electrónicas em processo penal. Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova*, Coimbra: Coimbra Editora, 2011, p. 280, João Conde Correia, "Prova digital…", *op. cit.*, p. 36, e Rui Cardoso, "A conservação e a utilização probatória de metadados…", *op. cit.*, p. 58 e ss.

[24] Precisamente nestes termos, com reflexão pormenorizada sobre o problema e ampla referência a jurisprudência, Rui Cardoso, "A conservação e a utilização probatória de metadados…", *op. cit.*, p. 61 e ss.

mais restritos da declaração de inconstitucionalidade, valerá a regra supletiva: a declaração de inconstitucionalidade com força obrigatória geral produz efeitos desde a entrada em vigor da norma declarada inconstitucional e determina a repristinação das normas que ela eventualmente tenha revogado (artigo 282.º, n.º 1, da CRP). Ficam, porém, ressalvados os casos julgados, salvo decisão em contrário do Tribunal Constitucional quando a norma respeitar a matéria penal (artigo 282.º, n.º 3 CRP).

Não tendo o Tribunal Constitucional decidido expressamente em sentido contrário, devem considerar-se ressalvados os casos julgados.

Outra questão que tem sido levantada neste contexto prende-se com a admissibilidade do recurso de revisão – um recurso interposto depois do trânsito em julgado da decisão – nos termos do artigo 449.º, n.º 1, alínea *f*), do CPP. Nos termos desta norma, a revisão da sentença transitada em julgado é admissível quando "seja declarada, pelo Tribunal Constitucional, a inconstitucionalidade com força obrigatória geral de norma de conteúdo menos favorável ao arguido que tenha servido de fundamento à condenação".

Nos últimos meses, têm sido apresentados no Supremo Tribunal de Justiça vários pedidos de revisão, com fundamento na declaração de inconstitucionalidade das normas resultante do Acórdão em análise. O Supremo Tribunal de Justiça tem entendido – e bem, da minha perspetiva – que a possibilidade de revisão de sentença só existirá nos casos em que o próprio Tribunal Constitucional excluir a ressalva dos casos julgados[25]. Coisa que, como vimos, não aconteceu no Acórdão em análise.

E o Supremo Tribunal de Justiça tem entendido ainda – e bem, também, do meu ponto de vista – que mesmo que o Tribunal Constitucional tivesse afastado expressamente a ressalva dos casos julgados, a revisão da sentença não seria *automática*. Caberia sempre ao Supremo Tribunal de Justiça avaliar caso a caso se a norma de conteúdo menos favorável ao arguido declarada inconstitucional havia servido de "fundamento à condenação" – este é um pressuposto da admissibilidade da revisão de sentença, nos termos do CPP.

[25] Cf., de modo exemplificativo, o Acórdão do Supremo Tribunal de Justiça, de 6 de setembro de 2022 (Processo n.º 4243/17.0T9PRT-K.S1), o Acórdão do Supremo Tribunal de Justiça, de 6 de setembro de 2022 (processo n.º 618/16.0SMPRT-BS, e o Acórdão do Supremo Tribunal de Justiça, de 30 de novembro de 2022 (processo n.º 71/11.4JABRG-G.S1). A este propósito, cf., ainda, J. J. Gomes Canotilho / Vital Moreira, "Anotação ao artigo 282º", *Constituição da República Portuguesa Anotada*, vol. II, 3.ª ed., Coimbra: Coimbra Editora, 1993, p. 1041.

V. As propostas de alteração legislativa

Apesar deste caminho – sinuoso – que pode ser feito no sentido da admissibilidade de conservação e acesso aos dados de tráfego e de localização nos termos referidos, há, claramente, necessidade de intervenção legislativa nesta matéria.

São conhecidas, neste momento, várias iniciativas legislativas apresentadas pelos diversos partidos políticos, que propõem a alteração da Lei n.º 32/2008[26], e também uma proposta de lei do Governo[27], em que se propõe a revogação da Lei n.º 32/2008 e a alteração da Lei n.º 41/2004.

Nos acórdãos do Tribunal de Justiça da União Europeia que são amplamente referidos no Acórdão agora em análise, o Tribunal de Justiça considerou que a conservação de dados só é admissível quando obedecer a três critérios objetivos: *um período temporal*; *uma zona geográfica determinada*; e *um círculo de pessoas determinado*.

A generalidade dos projetos de lei apresentados preocupou-se em acautelar que os dados são conservados em Portugal ou num Estado-Membro da União Europeia; fixa períodos de conservação dos dados mais curtos do que o prazo de um ano (atualmente previsto); e determina ainda o dever de o visado ser notificado de que os seus dados foram acedidos no âmbito de um processo penal.

Não encontramos, porém, nos projetos de lei apresentados pelos diversos partidos, qualquer limitação nem de carácter geográfico, nem quanto ao círculo de pessoas cujos dados devam ser conservados. Esta dificuldade na apresentação das propostas é, porém, compreensível. Na verdade, uma medida legislativa de conservação de dados, geograficamente condicionada, dirigida a um círculo de pessoas determinadas, sem que se tenha verificado já a prática de um facto ilícito típico, será de difícil harmonização com norma constante do n.º 3 do artigo 35.º da CRP, que apenas admite que o legislador autorize o tratamento informático de dados relativos à vida privada *com garantias de não discriminação*. Uma norma que delimite o âmbito subjetivo da conservação dos dados, muito dificilmente não violará, assim, o princípio da igualdade e a proibição de discriminação[28].

Já a proposta de lei do Governo prescinde da existência de bases de dados autónomas para fins de investigação criminal, afirmando, com clareza, a possibilidade de as autoridades judiciárias (juiz e Ministério Público) acederem aos dados conservados nas bases já existentes para efeitos de faturação.

Eu simpatizo com a previsão de um regime que não preveja a conservação generalizada dos dados de tráfego e de localização para efeitos de investigação criminal e não tenho reservas de princípio quanto à possibilidade de acesso, no âmbito de um processo penal, aos metadados conservados pelos fornecedores de serviço para efeitos de faturação. Parece-me, todavia, que na proposta de lei do Governo há um enfraquecimento da tutela dos direitos fundamentais dos cidadãos, por comparação com o regime de conservação de dados previsto na Lei n.º 32/2008, cujas normas foram declaradas inconstitucionais.[29]

Desde logo, o acesso aos metadados por parte do Ministério Público ou das autoridades de polícia criminal pressupunha, nos termos da Lei n.º 32/2008, um despacho de autorização de um juiz de instrução que controlava o cumprimento dos requisitos de legalidade no acesso. Essa exigência desaparece nesta proposta do Governo. Nos termos da proposta, a solicitação dos dados aos fornecedores de serviço pode ser apresentada pelas "autoridades judiciárias" (artigo 2.º). Deste modo, na fase de inquérito, tal "solicitação" poderá ser apresentada diretamente pelo Ministério Publico.

Por outro lado, nos termos desta proposta de lei do Governo, o acesso aos metadados pode ser "solicitado" quando "haja 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, quanto a crimes" cometidos "por meio de sistema informático, puníveis com pena de prisão de máximo igual ou superior a um ano" (artigo 2.º, alínea *c*)). Verifica-se, deste modo, um alargamento do âmbito do acesso aos metadados, em face do previsto na Lei n.º 32/2008, em que apenas se admitia o acesso a tais dados em caso de crime grave.

VI. Conclusão

A descoberta da verdade constitui uma das finalidades do processo penal. Não posso (nem quero) recusar a intervenção das realizações tecnológicas no processo penal. Comprovadas as vantagens da utilização dos novos meios de obtenção de prova em ambiente digital da perspetiva da repressão das formas mais graves de criminalidade, há que encontrar uma forma de eles poderem ser usados no processo penal sem que se perca de vista a proteção dos direitos

[26] Projeto de Lei n.º 70/XV/1ª (PSD); Projeto de Lei n.º 79/VI/1ª (Chega); Projeto de Lei n.º 100/XV/1ª (PCP).

[27] Proposta de Lei n.º 11/XV/1ª.

[28] Este aspeto é, aliás, referido, na declaração de voto de Lino Ribeiro.

[29] Referindo-se também a uma "diminuição das garantias fundamentais dos cidadãos", cf. o Parecer da Comissão Nacional de Proteção de Dados (Parecer 2022/50, de 21 de junho de 2022).

fundamentais das pessoas. Não podemos perder de vista, designadamente, o direito à privacidade e o direito à autodeterminação informativa.

O que se pede ao direito processual penal – que é *direito constitucional aplicado* – não é novo. O que se lhe pede, uma vez mais, é que encontre um equilíbrio – uma *concordância prática*[30] – entre a descoberta da verdade material e a realização da justiça, por um lado, e a proteção dos direitos fundamentais das pessoas, por outro.

[30] Cf. já Jorge de Figueiredo Dias, "Para uma reforma global do processo penal português. Da sua necessidade e de algumas orientações fundamentais", *in*: *Para uma Nova Justiça Penal*, Coimbra: Almedina, 1983, p. 206 e ss.