Recebido na CACDLG a 29-06-2022
Distribuido à CACDLG a 29-06-2022

Projeto de Lei 70/XV/1 (PSD) que procede à segunda alteração à Lei nº 32/2008, de 17 de julho, conformando-a com o Acórdão do Tribunal Constitucional nº 268/2022;

Projeto de Lei 79/XV/1 (Chega) que altera a Lei nº 32/2008, de 17 de julho, por forma a harmonizá-la com os preceitos constitucionais em vigor;

Projeto de Lei 100/XV/1 (PCP) que altera a Lei nº 32/2008, de 17 de julho;

Proposta de Lei 11/XV/1 (Governo) que regula o acesso a metadados referentes a comunicações eletrónicas para fins de investigação criminal.

I. ENQUADRAMENTO

A Assembleia da República, através do Exmo. Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, solicitou a emissão de parecer escrito sobre os seguintes projetos normativos, todos eles sujeitos a discussão conjunta[1] pela Assembleia da República:

- Projeto de Lei 70/XV/1, do PSD, que procede à segunda alteração à Lei nº 32/2008, de 17 de julho, conformando-a com o Acórdão do Tribunal Constitucional nº 268/2022;
- Projeto de Lei 79/XV/1, do Chega, que altera a Lei nº 32/2008, de 17 de julho, por forma a harmonizá-la com os preceitos constitucionais em vigor;
- Projeto de Lei 100/XV/1, do PCP, que altera a Lei nº 32/2008, de 17 de julho e
- Proposta de Lei 11/XV/1, do Governo, que regula o acesso a metadados referentes a comunicações eletrónicas para fins de investigação criminal.

[1] Cfr. https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=121504, consultado a 23 de junho de 2022.

II. O CONTEXTO DAS INICIATIVAS

1. As iniciativas que se analisam pretendem superar as dificuldades criadas à investigação criminal pelo Acórdão nº 268/2022[2] do Tribunal Constitucional, de 19 de abril de 2022, que declarou a inconstitucionalidade com força obrigatória geral das normas dos artigos 4º, 6º e 9º da Lei n.º 32/2008, de 17 de julho.

Até agora, aquelas disposições obrigavam os operadores de comunicações a guardar, de forma sistemática, dados referentes a comunicações, para que os mesmos (embora sob muitas condições e limitações) pudessem vir a ser utilizados na investigação da prática de crimes.

Como efeito desta declaração de inconstitucionalidade, os operadores deixaram de estar sujeitos a tal obrigação passando, pelo contrário, a ter a geral imposição (embora com exceções), de eliminar os dados, ou de torná-los anónimos, quando deixem de ser necessários para efeitos da transmissão da comunicação (artigo 6º, nº 1, da Lei nº 41/2004, de 18 de agosto).

2. Não será propósito de nenhuma destas propostas legislativas interferir nos efeitos desta jurisprudência obrigatória do Tribunal Constitucional. Pelo contrário, interpretam-se as mesmas, como iniciativas que pretendem resolver o problema prático e operacional gerado para o futuro pela doutrina do Acórdão.

Com efeito, a indisponibilidade de alguns dos dados de tráfego impossibilita, na prática, investigar a generalidade dos crimes praticados em ambiente digital. Em particular, o endereço do protocolo IP de uma determinada comunicação é essencial em milhares de inquéritos. A falta de informação sobre o mesmo torna inviável dar início a numerosas investigações, uma vez que este tipo de dados comunicacionais é fundamental para que se consigam identificar os autores de crimes *online*.

[2] http://www.tribunalconstitucional.pt/tc/acordaos/20220268.html.

3. Face à jurisprudência constitucional, afigura-se que apenas uma solução legislativa, alinhada com os limites da doutrina do Tribunal Constitucional, pode clarificar as dúvidas e incertezas que o Acórdão trouxe ao atual quadro normativo. Assim, a via da superação da fragilidade em que se encontra a investigação criminal, ao ser legalmente impedida de aceder a dados de tráfego, é a da alteração das normas em vigor.

Por isso, saúda-se liminarmente o surgimento destes Projetos de Lei e desta Proposta de Lei.

III. A NECESSIDADE LEGISLATIVA E A JURISPRUDÊNCIA CONSTITUCIONAL

4. A doutrina do Tribunal Constitucional aponta claramente no sentido de ser contrária ao direito constitucional português (e ao direito da União Europeia) a retenção sistemática, generalizada e indiferenciada de dados.

Não obstante, é sabido que os dados de tráfego podem ser importantes provas de infrações criminais. Como acima se referiu, o endereço de IP utilizado para estabelecer uma comunicação é um elemento crucial para se conseguirem identificar os autores de crimes que ocorrem na Internet, tais como difusão de pornografia infantil, venda de drogas ou armas na *Darkweb*, difusão de discurso de ódio, devassa da intimidade ou burlas *online*.

A falta de disponibilidade, em particular dos endereços de IP de concretas comunicações, impossibilita investigar um enorme número de crimes: sem o endereço de protocolo IP não é viável, sequer, iniciar milhares de investigações – as vítimas verão os seus direitos violados sem que haja permissão legal para que os autores dos crimes sejam identificados, a partir de dados comunicacionais.

5. Após a declaração de inconstitucionalidade os operadores deixaram de ter qualquer obrigação de guardar dados de tráfego, tendo mesmo a genérica obrigação de os apagar após a comunicação. Podem, porém, alguns desses dados continuar a ser conservados, nos termos do Artigo 6º da Lei nº 41/2004. Tal conservação é uma opção que os operadores de comunicações exercem ou não (portanto, não é obrigatória) sendo somente "*permitido o tratamento de dados de tráfego necessários à faturação dos assinantes e ao pagamento de*

interligações". Esse tratamento apenas é "*lícito até final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado*".

6. Não é consensual que a possibilidade legal conferida pelo Artigo 6º da Lei nº 41/2004 abranja a retenção do endereço de IP das comunicações.
Todavia, o Tribunal Constitucional reconheceu, quanto a este específico tipo de dados, a sua essencialidade na investigação criminal moderna. Mais ainda, expressamente afirmou a conformidade da sua retenção com a Constituição, pelo menos em termos de *lege ferenda*, desde que uma futura lei observasse dois requisitos atualmente em falta: a expressa obrigação de os dados serem conservados em território da União Europeia e a previsão de notificação ao titular dos dados, quando os mesmos forem fornecidos às autoridades públicas.

7. Por outro lado, na lei, mantém-se em vigor a possibilidade conferida ao Ministério Público, pelo artigo 14º da Lei do Cibercrime, de solicitar a fornecedores de serviço "*dados relativos aos seus clientes ou assinantes, neles se incluindo 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 serviço*". Tais dados relativos aos clientes incluem, entre outros, "*a identidade, a morada postal ou geográfica e o número de telefone do assinante, e qualquer outro número de acesso*" – artigo 14º, nº 4, alínea b) da Lei do Cibercrime.
É pacificamente entendido que esta última disposição (no segmento "*número de acesso*") confere legitimidade ao Ministério Público para solicitar a operadores de comunicações informações sobre a identificação de concretos utilizadores de endereços de protocolo IP.

IV. PROJETOS DE LEI 70/XV/1 (PSD), 79/XV/1 (CHEGA) E 100/XV/1 (PCP)

8. Deixando-se para momento ulterior a análise da Proposta de Lei 11/XV/1 (Governo), comentam-se agora os Projetos de Lei 70/XV/1 (PSD), 79/XV/1 (Chega) e 100/XV/1 (PCP). Justifica-se a abordagem em conjunto por duas razões: por um lado, porque embora diferentes, todos eles optam por proceder a muito pequenas alterações, quase pontuais, à

Lei nº 32/2008, de 17 de julho; por outro, porque (embora com abordagens diferenciadas), todos o fazem procurando exclusivamente introduzir naquele diploma as exigências normativas apontadas pelo Acórdão do Tribunal Constitucional nº 268/2022.

9. Desde logo, os três projetos avançam com soluções quanto à **limitação territorial ao local da conservação dos dados**.

O Projeto de Lei 70/XV/1 (PSD) altera o nº 1 do artigo 4ª da Lei 32/2008, que passa a exigir que os dados sejam conservados "*em Portugal ou em outro Estado-Membro da União Europeia*". O Projeto de Lei 100/XV/1 (do PCP) vai mais além relativamente à doutrina do Tribunal Constitucional, exigindo que os dados se conservem em Portugal (numa alteração que propõe fazer ao artigo 6º). Por último, o Projeto de Lei 79/XV/1 (Chega), propondo um novo nº 2 para o mesmo artigo 6º da Lei nº 32/2008, avança com uma formulação que se afigura pouco precisa e algo equívoca ("*os dados devem ser armazenados em local compatível com o exercício das garantias constitucionais de proteção e com a intervenção da CNPD*").

10. Da mesma forma, os três projetos avançam com uma solução para a exigência da doutrina constitucional, respeitante à **notificação dos titulares dos dados**.

O Projeto de Lei 70/XV/1 (PSD) propõe a introdução de um novo nº 7 no existente artigo 9º da Lei nº 32/2008, criando um detalhado regime de notificação, a cargo do operador de comunicações, mas dependente de autorização do juiz de instrução. Afigura-se um modelo complexo, difícil de levar à prática e por isso pouco interessante, porque requer diversos trâmites processais e transfere para entidades privadas a execução de uma notificação que depende de uma decisão pública (de um juiz). Por outro lado, não se prevê a intervenção neste procedimento do Ministério Público, titular da ação penal. Esta não previsão poderá ter impacto seriamente negativo em investigações penais. Além disso, a não intervenção (ou ao menos a não audição) do Ministério Público numa decisão em processo penal contraria frontalmente a lógica e a filosofia do modelo português.

O Projeto de Lei 79/XV/1 (Chega) também propõe a introdução de um novo nº 7 para o mesmo artigo 9º da Lei nº 32/2008. Nesta proposta, impõe um dever de informar os titulares dos dados. Todavia, esta nova norma não define quem efetua essa notificação (refere

apenas "*as autoridades competentes*") nem fornece critérios objetivos suficientes para a determinação do momento dessa notificação (indicando apenas o "*momento em que essa comunicação não seja suscetível de comprometer as investigações levadas a cabo por essas autoridades*"). Afigura-se uma proposta demasiado vaga, que criará dificuldades na aplicação ao caso concreto.

O Projeto de Lei nº 100/XV/1 (do PCP), por via da introdução de um novo artigo 9º-A à Lei nº 32/2008, também cria um regime específico de notificação, cuja responsabilidade é do "*juiz de instrução que autorizou a transmissão de dados*" e que deve ser materializado "*a partir do momento em que considere que essa comunicação não seja suscetível de comprometer a investigação criminal ou de constituir risco para a vida ou integridade física de terceiros*". Anota-se que esta proposta faz depender de uma decisão judicial o juízo sobre a conveniência, ou não, de revelar a terceiros informação de uma determinada investigação, sem que se preveja a intervenção do Ministério Público no respetivo procedimento. Esta proposta merece pois a mesma censura que acima se formulou quanto ao Projeto de Lei 70/XV/1 (PSD): além de poder ter um impacto muito negativo em concretas investigações criminais não é consequente com o modelo processual penal português.

Em suma, afigura-se que os modelos de notificação das três propostas normativas apresentam vícios de sistema e podem ser potenciadoras de grandes dificuldades na aplicação ao caso concreto.

11. Outra das vertentes que todos estes três Projetos de Lei pretendem regular é o do **prazo da conservação de dados retidos**, ao abrigo desta Lei nº 32/2008.

Com efeito, o Projeto de Lei 70/XV/1 (PSD) propõe-se alterar o artigo 6º da Lei nº 32/2008, consagrando que a generalidade dos dados retidos deverá ser conservada pelo prazo de um ano (como sucede no modelo atual, negativamente sancionado pelo Tribunal Constitucional), mas o prazo respeitante a dados de tráfego e de localização deverá ser reduzido a 12 semanas – é, para o efeito, introduzido um novo nº 2 ao artigo 6º.

Também o Projeto de Lei 79/XV/1 (Chega) altera o artigo 6º da Lei nº 32/2008, o qual passa a consagrar que o prazo de conservação de dados é de seis meses.

Por último, o Projeto de Lei 100/XV/1 (PCP), também altera este mesmo artigo 6º, o qual passa a estipular que o prazo de conservação de dados é de "*90 dias a contar da data da conclusão da comunicação*".

12. Anote-se que as disposições da Lei nº 32/2008 que foram sujeitas à apreciação do Tribunal Constitucional (e decretadas inconstitucionais) estipulavam que os dados a conservar deveriam ser genericamente conservados pelos operadores pelo período de um ano.

Todos estes projetos reduzem esse período, ao menos parcelarmente, mas nenhum deles avança razões para justificar o critério temporal que adota. Não se alcança, pois, por que motivo um dos projetos prefere 90 dias, outro, seis meses e outro um ano, para os dados em geral, mas apenas 12 semanas para dados de tráfego e localização.

Fica a impressão de que houve a preocupação de todos os projetos de redução da bitola de um ano, consagrada na Lei nº 32/2008 (antes da declaração de inconstitucionalidade). Porém, nenhum dos projetos esclarece o motivo ou o critério pelo qual escolheu um determinado limite temporal e não qualquer outro.

13. Além destas considerações mais específicas, importa, porém, deixar uma apreciação de âmbito mais geral quanto a estas três iniciativas legislativas, os Projetos de Lei 70/XV/1 (PSD), 79/XV/1 (Chega) e 100/XV/1 (PCP).

Como se disse, todos optaram por introduzir pequenas alterações à Lei nº 32/2008. Porém, não se afigura que esta opção, de operar pequenas alterações à Lei nº 32/2008, consubstancie a alternativa legislativa, mais adequada. Este diploma legal tem vindo a ser objeto de muitas críticas. Assim aconteceu logo desde o momento da sua aprovação, por este conjunto normativo revelar muitas inconsistências técnicas. As fragilidades jurídicas e técnicas vieram, aliás, a determinar a sua muito tardia e deficitária entrada em vigor. A doutrina tem salientando desde então estas fragilidades e deficiências, que, ousamos dizer, vão muito para além dos aspetos que foram declarados inconstitucionais.

Por outro lado, mais recentemente, após a eclosão da corrente jurisprudencial do Tribunal de Justiça da União Europeia que deu origem a toda esta problemática, ouviram-se

renovadamente vozes da doutrina enfatizando a necessidade de rever de forma profunda este diploma. Tal revisão profunda nunca foi efetuada, não sendo também proposta pelas das iniciativas legislativas ora em análise.

Ou seja, afigura-se que se estes Projetos de Lei forem aprovados, a Lei nº 32/2008 continuará a manter fragilidades e inconsistências, as quais os projetos legislativos apresentados não vêm sanar. Todas elas propõem mudanças pontuais e circunscritas, que procuram responder ao vazio criado pela jurisprudência constitucional, não solucionando muitas outras questões, que permanecem.

14. Acresce que uma das mais marcantes notas da jurisprudência do Tribunal de Justiça da União Europeia (e também do Tribunal Constitucional) é a da recusa de um mecanismo de generalizada e indiscriminada retenção de dados.

Todos estes projetos legislativos vão precisamente em sentido contrário: embora fazendo-lhe ajustamentos pontuais, mantêm intocado o modelo existente, de generalizada e indiscriminada retenção de dados, limitando-se a introduzir-lhe *cirurgicamente* alguns dos requisitos da jurisprudência constitucional.

No que respeita ao Projeto de Lei 79/XV/1 (Chega), apenas retira da lista dos dados a reter os dados de localização (artigo 4º), diminui, não explicitando a razão, o prazo de conservação de dados (artigo 6º) e introduz um dever de informação (artigo 9º, nº 7).

Quanto ao Projeto de Lei 100/XV/1 (do PCP), a intervenção legislativa proposta é do mesmo teor, reduzindo o prazo de conservação dos dados, sem o justificar, condiciona a sua conservação ao território nacional, também não explicando a opção de ir tão longe (no artigo 6º), introduzindo por outro lado a obrigação de notificação aos titulares dos dados (no novo artigo 9º-A).

Por último, o Projeto de Lei 70/XV/1 (PSD), mantendo a geral obrigação de conservação de dados por um ano (que sempre foi a matriz da Lei nº 32/2008), apenas reduz o prazo de conservação dos dados de tráfego e localização (no novo nº 2 do artigo 6º), introduzindo também a obrigação de notificação (no novo nº 7 do artigo 9º) e condicionando a conservação ao espaço da União Europeia (artigo 4º, nº 1).

Isto é, todos os projetos de lei pretendem manter viva a estrutura e a filosofia da Lei nº 32/2008: a geral e indiscriminada retenção de dados. Este é, porém, precisamente, o aspeto mais censurado pela jurisprudência europeia e constitucional.

15. A retenção de dados é um tema que tem gerado ativas discussões na comunidade jurídica europeia. Porém, quer a Comissão Europeia, quer as restantes comunidades jurídica, judiciária e académica europeias, não foram ainda capazes de encontrar uma solução consensual para esta problemática, que logre acomodar, de um lado, as exigências da investigação criminal e, do outro, a doutrina do Tribunal de Justiça da União Europeia.
Estes três Projetos de Lei pretendem reintroduzir na lei um regime respeitante a um assunto que, no contexto europeu não está de modo nenhum resolvido – pelo contrário, têm-se registados evoluções constantes na jurisprudência sem que, todavia, exista suficiente sedimentação doutrinária.
Introduzir na lei um renovado regime de retenção de dados, por via de uma reconfiguração de alguns detalhes da Lei nº 32/2008, apresenta-se como uma solução de um alcance e conformidade controvertível, à luz da jurisprudência constitucional.

V. A PROPOSTA DE LEI 11/XV/1 (GOVERNO)

16. Ao contrário do que sucede com as propostas de alteração normativa que acima se referiram, a Proposta de Lei 11/XV/1 (Governo), opta pela revogação da Lei nº 32/2008, que faz de forma expressa (artigo 9º).
Por outro lado, esta Proposta assume que dados já anteriormente recolhidos pelos operadores de comunicações, noutra sede, podem vir a ser utilizados para fins de investigação criminal.
Reitera-se que alguns dos dados a que se referem todos estes projetos normativos são essenciais na investigação criminal. Sem o acesso a tais dados, muitos dos crimes cometidos *online* não podem ser investigados. Por isso, entende-se que esta iniciativa legislativa é importante e merece apoio, sem prejuízo dos comentários que de seguida se deixam. Desde já se adianta que se considera uma boa opção a atualização do artigo 6º da Lei nº 41/2004.

Quanto às restantes normas introduzidas no ordenamento jurídico, poderia porventura ponderar-se a adequação da sua inserção sistemática.

a. O regime da Lei Nº 41/2004

17. O artigo 6º da Lei nº 41/2004 permite aos operadores de comunicações conservar alguns dados de tráfego, sendo tal conservação uma opção que os operadores de comunicações exercem ou não. Como acima se referiu, este tratamento destina-se a garantir a "*faturação dos assinantes*", não podendo o mesmo ultrapassar o "*período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado*".

Inclui, portanto, o quadro normativo, uma possibilidade de conservação de alguns dados (por um período de seis meses – pela conjugação do artigo 6º, nº 3, da Lei 41/2004 com o artigo 10º, nºs 1 e 4, da Lei 23/96, de 26 de julho, diploma legal que define regras respeitantes à prestação de serviços públicos essenciais). Trata-se, naturalmente, de um conjunto muito reduzido de dados cuja recolha, pela sua natureza, não colide com interesses ou direitos fundamentais, como a privacidade, o sigilo de comunicações ou a autodeterminação informacional.

A declaração de inconstitucionalidade do Tribunal Constitucional não abrangeu este regime normativo, nem incidiu sobre a específica conservação de endereços do protocolo IP usados em comunicações concretas. Não questionou a vigência da Lei nº 41/2004, nem pôs em causa a prática corrente, de pedido de informações aos operadores de comunicações pelo Ministério Público, neste quadro legal.

18. Estando em vigor um regime minimalista de guarda de dados, que podem ser utilizados na investigação criminal, afigura-se que a sua manutenção em vigor beneficiará de um ajustamento às exigências da doutrina do Tribunal Constitucional.

Tais exigências afiguram-se sobretudo ao nível da localização dos dados e ao nível da notificação da utilização dos mesmos: o Tribunal Constitucional expressou a necessidade de se estatuir a obrigação de os dados serem conservados em território da União Europeia e a

previsão de notificação ao titular dos dados, quando os mesmos forem fornecidos às autoridades públicas.

b. A alteração ao artigo 6º da Lei nº 41/2004

19. Refira-se novamente que o artigo 6º, nº 2, da Lei nº 41/2004 permite aos operadores de comunicações conservar alguns dados de tráfego: os "*dados de tráfego necessários à faturação dos assinantes e ao pagamento de interligações*". É o mesmo nº 2 que, a título exemplificativo elenca alguns desses dados.

Trata-se de um elenco elaborado no início da década de 2000, estando a exemplificação dos tipos de dados tecnologicamente desatualizada. É o caso, por exemplo, da informação referente ao "*tipo de posto do assinante*" ou da referente às "*unidades a cobrar para o período de contagem*".

Por isso, saúda-se como positiva a atualização desta listagem exemplificativa de dados que podem ser guardados.

20. Pelas considerações que já acima se fizeram, entende-se como particularmente importante a inclusão de dados referentes a "*códigos de utilizador, identidade internacional de assinante móvel (IMSI) e a identidade internacional do equipamento móvel (IMEI)*", na alínea a), bem como a adição do grupo data/hora à alínea c). Igualmente importante é a introdução da nova alínea d), que deixa claro ser permitido tratar dados respeitantes ao "*número de telefone, endereço de protocolo IP utilizado para estabelecimento da comunicação, porto de origem de comunicação, bem como os dados associados ao início e fim do acesso à Internet*".

Toda esta informação é naturalmente relevante para que os operadores procedam à faturação do serviço prestado – sendo, em contraponto, igualmente necessária para que os consumidores possam reclamar dessa faturação, se incorreta. Será porventura também importante em sede de investigação criminal, como já se deixou dito.

c. A finalidade do tratamento dos dados

21. Além de alterar o teor do artigo 6º da lei nº 41/2004, esta Proposta de Lei integra diversas normas que compõem um pequeno regime de natureza processual penal, de caráter

especial, estabelecendo "*as regras de acesso, para fins de investigação criminal, a dados tratados pelas empresas que oferecem redes e ou serviços de comunicações eletrónicas*" (alínea a) do artigo 1º).

Com este regime afirma-se não pretender ser um sucedâneo da Lei nº 32/2008, antes se desenhando como um regime especial que, sem criar qualquer obrigação de conservação de dados, apenas visa regular a utilização em processo penal de certos dados, guardado por motivos diversos.

Afigura-se positiva esta vertente, por conferir uma regulação de base legal a uma prática de décadas.

22. Um dos benefícios positivos da criação deste quadro normativo é o da consagração expressamente feita na alínea a) do Artigo 1º da Proposta de Lei, de que os dados tratados pelos operadores de comunicações podem ser acedidos para fins de investigação criminal.

Fica clara na lei esta possível finalidade do tratamento dos dados, deixando assim expressos, de forma mais explícita¸ os princípios que já resultam do artigo 14º, nºs 4 da Lei do Cibercrime.

d. A inserção sistemática

23. Como se disse, esta Proposta de Lei cria um regime processual penal especial, plasmado nos respetivos artigos 1º a 5º. Além disso, introduz no ordenamento jurídico diversas outras normas, não especifica ou diretamente relacionadas com processo penal ou a investigação criminal, mas antes relacionadas com a normal atividade dos operadores de comunicações, no contexto do fornecimento de informação às investigações criminais. É designadamente o caso dos artigos 6º e 7º.

A opção da Proposta foi a de criar um regime particular, num diploma muito específico e avulso, que disciplina o acesso, para efeitos de investigação criminal, a dados tratados pelos operadores de comunicações, incluindo todas estas normas.

24. Afigura-se que esta técnica legislativa possa ser menos eficiente, uma vez que consagra num diploma avulso normas muito relevantes, quer para a investigação criminal, quer para

o exercício da regular atividade dos operadores. Afigura-se como melhor opção a de inserir estas normas nos existentes diplomas setoriais que regem cada uma das respetivas atividades.

Assim, mostrar-se-ia preferível condensar e distribuir pela Lei do Cibercrime, fonte normativa da generalidade das medidas de obtenção da chamada prova digital, as normas dos artigos 2º e 5ª (porventura, a inserir sistematicamente após o respetivo artigo 14º, que respeita exatamente a esta mesma temática).

As normas respeitantes à recolha de estatísticas e a avaliação, em nada se relacionam com processo penal, uma vez que regulam obrigações dos operadores de comunicações e da respetiva supervisão. Por isso, afigura-se que seriam mais bem consideradas e interpretadas se inseridas na Lei nº 41/2004 (porventura, a seguir ao respetivo artigo 6º, a que se vem fazendo alusão).

e. A transmissão e destruição dos dados

25. A Proposta de Lei 11/XV/1ª prevê duas normas operativas, nos artigos 4º (condições da transmissão de dados) e 5º (destruição dos dados). A abordagem destas duas normas exige diferenciação, embora ambas revistam natureza processual penal.

Quanto à norma do artigo 5º (destruição dos dados), como se disse, afigura-se que a mesma deveria ser integrada na Lei do Cibercrime. Nesta sede normativa, onde se guardam as regras da chamada prova eletrónica, ou prova digital, esta norma seria a equivalente a uma outra, prevista para a prova em geral (dita prova *física*), do Código de Processo Penal: o nº 12 do artigo 188º, previsto para as interceções de comunicações telefónicas.

26. Já a norma prevista no artigo 4º merece crítica mais focada na respetiva substância.

O regime da Lei nº 32 /2008 previa (artigos 7º, nº 3 e 10º) que a transmissão de dados, do operador à autoridade judiciária, se processaria mediante comunicação eletrónica. À época, não existiam ainda as estruturas e plataformas tecnológicas que atualmente se utilizam. A consagração desta forma de transmissão, que era inovadora e original, pretendia introduzir segurança nas remessas de dados, dos operadores ao juiz. Esta exigência tecnológica gerou na altura entropias, que dilataram de sobremaneira a entrada em vigor da lei, uma vez que

nem o sistema judiciário nem os operadores estavam preparados para este requisito técnico.

No tempo que corre, existem já diversas plataformas de comunicação e transmissão de dados na área da justiça. Estão, pois, já em funcionamento diversas formas de comunicação segura por via eletrónica. Aliás, uma delas é justamente aquela que os próprios operadores de comunicações desenvolveram para poderem cumprir os requisitos da Lei nº 32/2008, a qual veio a ter uma utilização numericamente reduzidíssima.

Portanto, o contexto atual não é o mesmo de 2008: além daquelas que estão em funcionamento, desenvolvem-se atualmente outras plataformas, especificamente orientadas para a área da justiça criminal, destinadas a gerir digitalmente o processo-crime. Afigura-se, pois, que a forma de transmissão do tipo de dados que agora aqui estão em causa não deve ser encarada de modo isolado e diferenciado, num diploma avulso: antes deve ser integrada no processo global de reformulação e digitalização da marcha do processo-crime. Criar nesta sede uma forma específica de transmissão de dados é suscetível de gerar, como aconteceu com a Lei nº 32/2008, entropias. Com este entendimento, o artigo em causa deveria ser suprimido.

27. Acresce que relegar para uma portaria as condições técnicas para a transmissão deste tipo de dados dos operadores às autoridades judiciárias, significa igualmente relegar para mais tarde a criação de condições, de facto, para a entrada em vigor da presente iniciativa normativa.

Afigura-se que essa será uma opção deveras inadequada, num momento em que, por colapso do sistema anterior, existe uma emergência de criação de um modelo alternativo de acesso a dados.

f. O âmbito de aplicação

28. O artigo 2º da Proposta de Lei determina o âmbito de aplicação da mesma, descrevendo os crimes em relação aos quais podem ser solicitados os dados a que se reporta esta iniciativa legislativa.

Como acima se explicitou, esta é uma matéria de direito processual penal, a qual deveria ser devidamente enquadrada na Lei do Cibercrime. Se assim fosse, este artigo tornar-se-ia desnecessário, uma vez que aquele diploma normativo, que compreende diversas medidas processuais, inclui também uma norma (a do artigo 11º), que define o respetivo âmbito de aplicação.

Esta opção de inserção sistemática, que já acima se abordou e explanou, garantiria uma resposta coerente do sistema, que ficaria mais consolidado.

g. A notificação

29. Por outro lado, esta Proposta pretende ir ao encontro do requisito da notificação, incluído na *lista de exigências* do Tribunal Constitucional. Assim, no respetivo artigo 3º, prevê-se um regime de notificação, que inclui prazos concretos para proceder à mesma, salvaguardando situações em que tal notificação possa "*pôr em causa a investigação, dificultar a descoberta da verdade ou criar perigo para a vida, para a integridade física ou psíquica ou para a liberdade dos participantes processuais, das vítimas do crime ou de outras pessoas*". Em tais situações, a notificação ao titular dos autos pode ser feita mais tarde ("*logo que a razão do protelamento deixar de existir*"), devendo, em todo o caso, ser feita "*no prazo máximo de 10 dias a contar da data em que for proferido despacho de encerramento do inquérito*", o qual é, aliás, a única fase processual durante a qual este protelamento pode ter lugar.

30. Este regime de notificação é claro quanto à entidade que determina a notificação: a "*autoridade judiciária que determinar a solicitação dos dados*". Afigura-se que esta solução é coerente com o regime processual penal em geral, por fazer depender da competente autoridade judiciária a gestão de cada fase processual.

De seguida, far-se-ão mais comentários sobre este aspeto em particular.

h. Referência especial à "*autoridade judiciária competente*"

31. Uma outra das virtudes deste projeto normativo é a de não interferir nas regras gerais e fundamentais do processo penal, não tendo alterado a função e o equilíbrio de poderes dos diversos intervenientes processuais.

Prevê-se a solicitação de dados pela *autoridade judiciária*, expressão que no contexto geral do Código de Processo Penal está completamente integrada e é pacificamente interpretada desde o início da vigência deste diploma, em 1988. A função de *autoridade judiciária* pode ser desempenhada quer pelo Ministério Público, quer pelo juiz, consoante a fase processual e as respetivas atribuições na mesma fase.

Existe um aspeto específico que importa clarificar a este respeito, o qual é o do regime da obtenção de informação quanto ao utilizador de um determinado endereço de IP.

32. Não existe na lei um estatuto do endereço IP. Também não é expressamente determinado em nenhum texto legal se o endereço IP é, ou não, um dado de tráfego. Não obstante, esta discussão tem sido importante na jurisprudência, que dela retira consequências importantes quanto à possibilidade de se obterem informações desta natureza em processo-crime.

No inquérito penal, a obtenção de dados de tráfego de comunicações eletrónicas está sujeita ao regime do artigo 18º da Lei do Cibercrime, que é também aplicável à obtenção de dados de conteúdo das comunicações (artigo 18º, nº 1 e nº 3). Em termos muito sintéticos, essa obtenção depende de autorização judicial e apenas é permitida na fase de inquérito, em casos similares àqueles em que se permite realizar interceções telefónicas.

Quanto aos restantes dados informáticos (que não de tráfego, nem de conteúdo), podem ser obtidos em todas as fases processuais, nos termos do artigo 14º da Lei do Cibercrime, por via da injunção. A injunção, no decurso do inquérito, é uma diligência da competência do Ministério Público, que pode ser ordenada sempre que a obtenção dos dados em causa seja necessária à descoberta da verdade.

Em termos práticos, qualificar o endereço IP como dado de tráfego tem a consequência, por um lado, de a sua solicitação ter que ser autorizada pelo juiz de instrução; por outro, de a sua obtenção não ser permitida em todos os casos, apenas o sendo quando se investiguem crimes mais graves – apenas é permitido obter tais dados em situações em que também poderiam ser realizadas interceções telefónicas, para cujo regime remete a Lei do Cibercrime (artigo 18º, nº 1, alínea b) e nº 4). Além disso, esta possibilidade está legalmente limitada à fase de inquérito.

33. Sublinha-se que caso se considerasse o endereço IP sujeito ao regime dos dados de tráfego, não seria possível obter informação que lhe dissesse respeito num conjunto numérica e sociologicamente muito expressivo de investigações. Ou dito de outra forma, haveria um obstáculo legal à investigação de uma grande parcela dos crimes cometidos nas redes, por via das redes de comunicações: assim aconteceria, por exemplo, com as burlas em vendas na Internet, com as injúrias por via de mensagens de email, ou em blogs ou outras páginas na Web, ou em redes sociais ou, ainda, com ameaças transmitidas por comunicação eletrónica.

34. A identificação de um determinado endereço IP, conjugada com a identidade de quem o utilizou num dado dia e hora, não revela informação sobre o percurso dessa comunicação nem sobre outro eventual tráfego comunicacional da pessoa em causa. Apenas comprova que essa mesma comunicação (e apenas essa) foi efetuada por via daquele número técnico de acesso à Internet. Portanto, com esta informação, apenas se estabelece a ligação entre uma determinada comunicação, que se conhece já, e a respetiva origem. O mesmo não acontecerá quando se pretende obter, numa investigação, informação sobre um alargado período de tempo ou sobre as múltiplas comunicações efetuadas por um suspeito: nesse caso, está-se claramente já no âmbito do tráfego.
Por isso, estando em causa, apenas a obtenção da identificação de um utilizador de um endereço IP ou o número de IP usado por um determinado indivíduo, em circunstâncias temporais determinadas, não é suscetível de revelar informação privada ou confidencial e apenas permite confirmar que uma comunicação – que a investigação conhecia já – ocorreu.

35. O conceito legal de dados de tráfego para efeitos criminais (artigo 2º, alínea c) da Lei do Cibercrime), é muito alargado e abrangente. Além disso, como se referiu, o regime da obtenção de dados de tráfego, em investigação criminal, é muito mais restritivo que o da obtenção de todos os restantes dados (que não sejam de conteúdo). Por isso, a jurisprudência tem insistido na discussão sobre a natureza do endereço IP. Porém, esta discussão teórica, sobre se o endereço IP é ou não um dado de tráfego, não é determinante

para a definição do seu estatuto processual penal: é que o artigo 14º da Lei do Cibercrime consagra expressamente o regime de pedido do endereço IP aos operadores de comunicações, por via da criação de um regime especial, no seio da figura da injunção.

Por via da injunção é permitido ao Ministério Público, no decurso do inquérito, solicitar aos fornecedores de serviço os dados informáticos que estes tenham armazenados, excluindo-se, porém, expressamente, os dados de tráfego (cuja obtenção, como se disse, está sujeita ao regime do artigo 18º). Porém, embora sem o enquadrar em nenhuma das categorias de dados, o nº 4, alínea b) do artigo 14º da Lei do Cibercrime regula expressamente o procedimento de solicitação do endereço IP aos operadores de comunicações. Trata-se de um regime especial e independente da categorização de dados definida pela lei.

Assim, no nº 4 diz-se ser permitida à autoridade judiciária a obtenção de dados "*relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos (...) e que permita determinar*". Tais dados incluem, entre outros "*qualquer número de acesso*". Este "*número de acesso*" a que a lei se refere é precisamente o endereço IP. Nas comunicações digitais não há nenhum outro "*número de acesso*" nem realidade de natureza alguma que possa preencher este conceito, sendo legítimo e seguro concluir que esta referência foi expressamente consagrada na lei para aludir ao endereço IP.

36. A solução legal consagrada na Lei do Cibercrime foi diretamente traduzida do artigo 18º, nº 3 da Convenção sobre Cibercrime do Conselho da Europa, ou Convenção de Budapeste, da qual Portugal é parte[3]. Nessa sede menciona-se a obtenção, por via da injunção, de "*subscriber's identity, postal or geographic address, telephone and other access number*".

Esclarece-se depois, no relatório explicativo (parágrafo 179)[4] que estão aqui em causa todas as medidas técnicas que "*enable a subscriber to enjoy the communication service offered. Such provisions include the reservation of a technical number or address (telephone number, web site address or domain name, e-mail address, etc.)*". Acrescenta ainda o relatório explicativo (parágrafo 180) que "*subscriber information (...) also means any information, other than traffic*

[3] http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.
[4] http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

data or content data, by which can be established the user's identity, postal or geographic address, telephone and other access number". E conclui (parágrafo 182) que "*for example, on the basis of the provision of a particular name (...) a particular associated telephone number or email address may be requested. On the basis of a particular telephone number or e-mail address, the name and address of the subscriber concerned may be ordered*".

37. Neste contexto, é indiferente que se trate de um endereço IP fixo, atribuído a título permanente a um só utilizador, ou de um endereço dinâmico, sucessivamente atribuído a múltiplos utilizadores: ambos são o tal "*número de acesso*" e em nenhum dos casos a entidade que conduz a investigação fica na posse de dados suscetíveis de revelar informação do foro pessoal ou íntimo. Para estes efeitos, a diferença entre ambos está na forma como o operador obtém a informação que lhe é solicitada: em caso de endereço IP dinâmico, o fornecimento do mesmo à entidade investigadora supõe que o operador consulte dados de tráfego. Todavia, desde que os dados consultados tenham sido tratados nos limites legais, não estão os operadores impedidos de aceder aos mesmos. Aliás, embora noutro foco, é mesmo exigido aos operadores que monitorizem o tráfego das suas redes, para que possam garantir, como exige o Artigo 3º da Lei 41/2004, a segurança dos serviços que prestam e a segurança da própria rede. Além disso, é inevitável que os operadores acedam aos dados de tráfego, no normal exercício da sua atividade, para poderem cobrar aos seus clientes a utilização do serviço fornecido (ou reclamar o não pagamento do mesmo). Esta possibilidade é permitida pelo já referido artigo 6º, nº 2 da mesma Lei nº 41/2004. Portanto, nada impede os operadores de, para fornecerem informação sobre um determinado endereço IP, ou sobre quem o utilizou num determinado dia e hora, consultarem dados de tráfego.
Como se disse, neste aspeto particular a lei portuguesa reproduz o texto da Convenção sobre Cibercrime. Em ambas as fontes normativas se omitiu um estatuto específico do endereço IP, mas também em ambas se consagrou uma norma que tem em vista disciplinar a sua obtenção em processo-crime.

38. Em suma: na lei vigente, quer por aplicação dos princípios gerais, quer por via da referência específica da alínea b) do nº 4 do artigo 14º da Lei do Cibercrime, o endereço IP

pertence ao conjunto de dados informáticos que podem ser solicitados por via de uma injunção para apresentação ou concessão de acesso a dados.

A ordem deve ser emitida pela autoridade judiciária e depende de, no caso concreto, "*se tornar necessário à produção de prova, tendo em vista a descoberta da verdade, obter dados informáticos específicos e determinados*". Emitida a ordem, "*quem tenha disponibilidade ou controlo desses dados*" deve comunicá-los ao processo, sob pena de punição por desobediência (artigo 14º, nº 1).

De tudo resulta que, no decurso do inquérito, a injunção é a forma processual apropriada para que o Ministério Público solicite aos fornecedores de serviço a identificação do endereço IP utilizado por um determinado indivíduo e, na vertente oposta, a identificação do cliente que usou um determinado endereço IP em determinadas circunstâncias de tempo.

Por sua vez, nas subsequentes fases processuais, a competência para ordenar esta diligência pertence ao juiz.

39. Por estas razões afigura-se correta, no artigo 2º e no artigo 3º, nº 1 da Proposta de Lei, a referência a "*autoridade judiciária*", não se discriminando a qual delas pretende aludir-se.

*

Em conformidade com o exposto, o Projeto de Lei em análise não nos merece outro juízo ou sugestão.

*

Eis pois, o parecer do CSMP.

Lisboa, 24 de junho de 2022