SEPARATA RPDC N.º 3 (2023)

REVISTA PORTUGUESA DE DIREITO CONSTITUCIONAL

PORTUGUESE REVIEW OF CONSTITUTIONAL LAW

AATRIC

Serviços de Informações, Dados de Tráfego e Revisão Constitucional – Uma Análise Crítica dos Projetos de Revisão Constitucional n.º 7/XV/1.ª e n.º 3/XV

João Narciso

Assistente Convidado da Faculdade de Direito da Universidade de Coimbra
joao.narciso@fd.uc.pt

Resumo: No âmbito da possível alteração do artigo 34.º da Constituição, para efeitos de legitimar o acesso a dados de tráfego pelo Sistema de Informações da República Portuguesa, os projetos de revisão constitucional apresentados pelos dois maiores partidos com assento parlamentar oferecem margem para dúvidas. Entende-se que os mesmos deveriam delimitar, sem que suscite incertezas, as entidades competentes para esse acesso, a terminologia que mais rigorosamente delimita as circunstâncias da comunicação, as quais não devem estar submetidas ao mesmo regime dos dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação. Não estando isentas de controvérsia as finalidades que no âmbito da prevenção justificam a restrição do direito ao sigilo das telecomunicações, não deve o direito português passar de um regime excecional em matéria de acesso ao tráfego da comunicação para uma utilização alargada e desmesurada.

Abstract: Within the scope of the possible amendment of article 34 of the Constitution for the purpose of legitimizing access to traffic data by the Intelligence System of the Portuguese Republic, the constitutional revision projects brought forward by the two major parties with parliamentary representation raise doubts. It is argued that they should delimit, without raising uncertainties, the entities that are competent for such access, the terminology

that more rigorously delimits the circumstances of the communication, which should not be subject to the same regime as that which applies to basic data and equipment location data, when they do not support a concrete communication. Since the purposes that justify the restriction of the right to secrecy of telecommunications are not without controversy, Portuguese law should not move from an exceptional regime of access to communication traffic to an extended and disproportionate one.

Palavras-chave: "serviços de informações"; "dados de tráfego"; "direito ao sigilo das telecomunicações"; "Constituição"; "revisão constitucional".

Keywords: "intelligence services"; "traffic data"; "right to secrecy of telecommunications"; "Constitution"; "constitutional revision".

1. A possibilidade de acesso a dados de tráfego de telecomunicações pelo Sistema de Informações da República Portuguesa (SIRP) continua a ser alvo de debate, assumindo, no processo de revisão constitucional em curso, maior vigor ao nível de uma hipotética alteração do artigo 34.º da Constituição da República Portuguesa (CRP)[1]. Conquanto esta não seja a única necessidade operacional reclamada pelos serviços que compõem a orgânica do SIRP, a verdade é que, num quadro legal lacunoso, a mesma tem, nos últimos anos, ocupado, na sua quase totalidade, a discussão ao nível do reforço dos seus meios de atuação. Como principais argumentos, invoca-se a adequação daquele acesso para efeitos de prevenção do fenómeno do terrorismo, bem como a situação de inferioridade em que, no âmbito da cooperação, as agências portuguesas de inteligência se encontram em relação às congéneres.

Alvo de atividade parlamentar abundante, a inclusão desse método oculto de investigação no elenco de meios de atuação do SIRP não tem, no entanto, deixado de levantar fundadas interrogações sob o prisma da sua compatibilidade com o direito à inviolabilidade das telecomunicações. Neste sentido, o Tribunal Constitucional, numa jurisprudência que apresenta uma inequívoca linha de continuidade, pronunciou-se, no Acórdão n.º 403/2015, pela inconstitucionalidade da norma do n.º 2 do artigo 78.º do Decreto n.º 426/XII da Assembleia da República, por violação do artigo 34.º, n.º 4 da CRP, entendimento que foi posteriormente reiterado, no Acórdão n.º 464/2019,

[1] O artigo 34.º, n.º 1 enuncia que "o domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis", declarando-se, no n.º 4, que "é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal".

que declarou a inconstitucionalidade da norma constante do artigo 4.º da Lei Orgânica n.º 4/2017, de 25 de agosto, por violação do disposto no mesmo normativo constitucional.

Nesta medida, tendo presente que os obstáculos suscitados naquela linha jurisprudencial apenas podem ser ultrapassados através de uma revisão do texto da Constituição, o Partido Social Democrata (PSD) apresentou o Projeto de Revisão Constitucional n.º 7/XV/1.ª, que, à atual configuração da norma do artigo 34.º, pretende adicionar um novo número, o n.º 5, dispondo que: "A lei pode autorizar o acesso do sistema de informações da República aos dados de contexto resultantes de telecomunicações, sujeito a decisão e controlo judiciais". A este debate juntou-se o Partido Socialista (PS), que, no Projeto de Revisão Constitucional n.º 3/XV, pretende adicionar um n.º 6, nos termos do qual: "Excetua-se do disposto no número anterior o acesso, mediante autorização judicial, pelos serviços de informações a dados de base, de tráfego e de localização de equipamento, bem como a sua conservação, para efeitos de produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna de prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada, nos termos a definir pela lei".

O facto de, nos termos do artigo 286.º, n.º 1 da CRP, as alterações da Constituição serem aprovadas por maioria de dois terços dos Deputados em efetividade de funções, bem como a circunstância de estarem em causa Projetos dos dois maiores partidos com assento parlamentar – com a consequente possibilidade de serem convertidos em direito vigente – motivam-nos a empreender uma análise crítica de algumas das soluções ali preconizadas. Assim, privilegiando as coordenadas que assumem maior relevo, ter-se-á em conta, dentro dos limites que esta reflexão pretende respeitar, o relevo da preferência por uma designação como a de "sistema de informações da República" face a uma como a de "serviços de informações"; o rigor que, em termos de terminologia, representa um enunciado como o de "dados de tráfego", bem como a diferenciação de regime que entre os mesmos tem de existir e os dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação; as perplexidades que origina a autorização do seu acesso para, no âmbito da salvaguarda da segurança interna, a prevenção de atos de sabotagem e da criminalidade altamente organizada; não esquecendo, por último, um elenco de alguns dos principais problemas que para o legislador ordinário podem surgir ao nível da reserva de lei e da reserva de juiz caso a norma constitucional seja alterada.

2. A começar, importa esclarecer que, integrando o SIRP, na sua arquitetura legal, o Serviço de Informações Estratégicas de Defesa (SIED) e o Serviço de Informações de Segurança (SIS)[2], estes não são, todavia, os únicos organismos, em Portugal, com responsabilidades no domínio da recolha, análise e difusão de informações. Com efeito, sendo as informações ali produzidas classificadas como estratégicas, não se pode olvidar que, para além destas e assumindo pontos de contacto com as mesmas, existem as categorias das informações militares, que servem de apoio às operações militares; das informações policiais, que auxiliam a atividade policial no âmbito das suas operações de segurança interna; e das informações criminais, que representam os conhecimentos que os órgãos de polícia criminal armazenam nos termos específicos da investigação criminal que realizam no processo criminal[3].

Assim, dando, sucintamente, conta da situação existente neste âmbito, no setor das informações militares, o Decreto-Lei n.º 19/2022, de 24 de janeiro, que estabelece a Lei Orgânica do Estado-Maior-General das Forças Armadas e altera as Leis Orgânicas dos três ramos das Forçadas Armadas, disciplina, no artigo 42.º, a missão e atribuições do Centro de Informações e Segurança Militares (CISMIL). Mesmo nas leis orgânicas das polícias não é difícil encontrar, dentro da categoria das informações policiais e criminais, referências a sistemas, unidades, departamentos e direções de informações. A benefício de ilustração, o Decreto-Lei n.º 137/2019, de 13 de setembro, que aprova a nova estrutura organizacional da Polícia Judiciária, prevê a existência de um Sistema de informação criminal, de uma Unidade de Informação Financeira e de uma Unidade de Informação Criminal, nos artigos 10.º, 27.º e 36.º, respetivamente. Por seu turno, a Lei n.º 53/2007, de 31 de agosto, que aprova a orgânica da Polícia de Segurança Pública, dispõe, no artigo 29.º, que uma das áreas compreendidas na unidade orgânica de operações e segurança é a das informações policiais, regulamentando a Portaria n.º 383/2008, de 29 de maio, no artigo 5.º, as competências do Departamento de Informações Policiais. Do mesmo modo, a Lei n.º 63/2007, de 6 de novembro, que aprova a orgânica da Guarda Nacional Republicana, refere, no artigo 32.º, que o

[2] Nos termos dos artigos 20.º e 21.º da Lei n.º 30/84, de 5 de setembro, e do artigo 3.º, n.ºs 2 e 3 da Lei n.º 9/2007, de 19 de fevereiro, o primeiro é o organismo incumbido da produção de informações que contribuam para a salvaguarda da independência nacional, dos interesses nacionais e da segurança externa do Estado Português, sendo o segundo o organismo incumbido da produção de informações que contribuam para a salvaguarda da segurança interna e a prevenção da sabotagem, do terrorismo, da espionagem e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido.

[3] Acompanhamos de perto, nesta matéria, Jorge Bacelar Gouveia, *Direito da Segurança – Cidadania, Soberania e Cosmopolitismo*, 1.ª ed., Coimbra: Almedina, 2018, pp. 700-701.

Comando Operacional compreende a área das informações, sendo que é no Decreto Regulamentar n.º 19/2008, de 27 de novembro, que são definidas, no artigo 7.º, as competências da Direção de Informações.

Do exposto decorre, como corolário, que, contrariamente ao que sucede no Projeto de Revisão Constitucional apresentado pelo PS, uma norma constitucional neste âmbito não pode optar, para efeitos de concretização das entidades competentes para o acesso aos dados, pela referência genérica a "serviços de informações", em detrimento da referência a "sistema de informações da República", já presente no atual texto constitucional. A Constituição, embora seja "minimalista" na matéria da produção de informações[4], já consagra, no âmbito da reserva absoluta de competência legislativa, no artigo 164.º, alínea q), uma alusão ao "sistema de informações da República"; além de que, deste modo, evita-se uma eventual confusão com outras realidades presentes nos diplomas normativos do âmbito militar e policial.

3. Delimitado este ponto, é tempo de clarificar qual a designação a ser utilizada para efeitos de delimitar, rigorosamente, a realidade representada pelo circunstancialismo do processo comunicacional. Como se não desconhece, representando o tráfego da comunicação um conjunto de informação que, contraposta ao conteúdo, abrange a espécie, hora, duração e intensidade de utilização – sendo um exemplo completo a faturação detalhada[5] – é comum, entre outros aspetos, a referência a metadados, dados de contexto resultantes de telecomunicações, dados de comunicação, circunstâncias do processo de comunicação e elementos funcionais da comunicação. Contudo, se é verdade que é de recusar o designativo de metadados – pela sua amplitude, pois estes são referidos como "dados sobre dados" – não menos certo é que mais acertada seria a utilização da fórmula "dados de tráfego" – em detrimento da fórmula "dados de contexto resultantes de telecomunicações", tal como sucede no Projeto apresentado pelo PSD –, por ser aquela que, contraposta aos dados de conteúdo, dados de base e dados de localização, mais comummente é utilizada para designar as circunstâncias exteriores da comunicação[6].

[4] Reconhecendo-o, *idem*, p. 685.

[5] A qual permite o conhecimento das condições factuais em que decorreu a comunicação, tais como todas as chamadas feitas, a partir de um número de telefone, por terceiros, familiares ou outros e, bem assim, os seus destinatários, números chamados, hora, duração, custos, entre outros. Veja-se António Pinto Monteiro, "A Protecção do Consumidor de Serviços Públicos Essenciais", *in*: António Pinto Monteiro (Dir.), *Estudos de Direito do Consumidor – Centro de Direito do Consumo*, N.º 2 (2000), pp. 345-346.

[6] Foi adotada, nos Acórdão do TC n.ºs 241/02, 486/2009, 403/2015 e 420/2017, a designada "classificação

4. Existindo, por parte do Projeto do PS, a intenção de submeter, conjuntamente, os dados de base, os dados de tráfego e os dados de localização de equipamento ao âmbito de proteção do artigo 34.º, reclama, pois, uma análise separada o recorte do perímetro da tutela constitucional do direito à inviolabilidade das telecomunicações, por contraposição ao âmbito normativo de outros direitos constitucionalmente consagrados, como é o caso do direito à reserva da intimidade da vida privada, previsto no artigo 26.º, n.º 1.

Nesta sede, há, desde logo, que enfatizar que, sendo a inviolabilidade do domicílio, da correspondência e dos outros meios de comunicação um "regime especial de tutela do direito à reserva da intimidade da vida privada"[7], é possível, porém, autonomizar a realidade que é juridicamente tutelada pelo

tripartida" do Parecer do Conselho Consultivo da Procuradoria-Geral da República n.º 16/94, votado em 24/06/94, III, 1, que distingue entre os dados relativos à conexão à rede, ditos dados de base; os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (p. ex. localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência), dados de tráfego; dados relativos ao conteúdo da comunicação ou da mensagem, dados de conteúdo. Contudo, no Acórdão do TC n.º 464/2019, tomando como alicerce a LO n.º 4/2017, enveredou-se por uma outra compartimentação, distinguindo-se entre os dados associados a um ato de comunicação (consumado ou tentado) entre duas pessoas (nos quais foram inseridos os dados de telecomunicações e os dados de tráfego de internet ligados às circunstâncias da comunicação interpessoal) e os dados que não estão associados a uma comunicação efetiva ou tentada entre dois sujeitos (onde se incluem os dados de identificação do sujeito, os dados de localização do equipamento, quando não deem suporte a uma concreta comunicação, e os dados de tráfego que apenas pressuponham uma comunicação entre um sujeito e uma máquina, como é o caso da consulta de sítios na internet). Mais tarde, no Acórdão do TC n.º 268/2022 operou-se a distinção entre os dados de base e os dados de tráfego, enquadrando-se a informação relativa aos dados de localização nos dados de base ou nos dados de tráfego. Na doutrina, identificando as circunstâncias da comunicação com os dados de tráfego, Manuel da Costa Andrade, "artigo 194.º", *in*: Jorge de Figueiredo Dias (dir.), *Comentário Conimbricense do Código Penal – Parte Especial* – Tomo I – Artigo 131.º a 201.º, 2.ª ed., Coimbra: Coimbra Editora, 2012, pp. 1095-1096. Na Lei n.º 41/2004, de 18 de agosto, sobre a proteção de dados pessoais e privacidade nas telecomunicações, os dados de tráfego são definidos, no artigo 2.º como "quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos de faturação da mesma" (alínea d)), entendendo-se, por seu lado, os dados de localização como "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" (alínea e)). Já na Lei n.º 109/2009, de 15 de setembro, os dados de tráfego são compreendidos, no artigo 2.º, alínea c), 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". Para além destas categorias, a Lei n.º 32/2008, de 17 de julho, acrescenta, ainda, os dados conexos necessários para identificar o assinante ou o utilizador (artigo 2.º, n.º 1, a)). Incluindo nos dados de telecomunicações e internet os dados de base, os dados de localização de equipamento e os dados de tráfego, cf., por fim, o artigo 2.º, n.º 2 da Lei Orgânica n.º 4/2017, de 25 de agosto.

[7] Assim, Germano Marques da Silva / Fernando Sá, anotação ao artigo 34.º, *in*: Jorge Miranda / Rui Medeiros, *Constituição Portuguesa Anotada* – vol. I – *Preâmbulo – Princípios Fundamentais – Direitos e Deveres Fundamentais* – Artigos 1.º a 79.º, 2.ª ed., rev., Lisboa: Universidade Católica Editora, 2017, ponto I, p. 549.

primeiro. Para enquadrar devidamente, não é despiciente clarificar, de modo sucinto, que na telecomunicação existe uma "relação triádica", identificando-se um emitente, um destinatário e um terceiro, isto é, o mediador que oferece o serviço de transmissão. E, dada a posição de domínio que este último detém sobre o processo comunicacional, que lhe assegura a possibilidade fática de intromissão arbitrária, sem o controlo dos comunicadores, aponta-se que daqui surge uma "específica situação de perigo" para quem comunica à distância[8].

É por isso que, em boa verdade, o regime jurídico do sigilo das telecomunicações visa proteger, não a confiança na reserva e confidencialidade dos outros interlocutores, mas a confiança na segurança e reserva dos sistemas de telecomunicações[9]. Ou, para continuar a sufragar a opinião da doutrina e jurisprudência mais autorizada, não uma compreensão material da privacidade/intimidade – como é aquela a que o artigo 26.º, n.º 1 empresta reconhecimento e sancionamento –, mas uma tutela da privacidade em sentido formal. Para concretizar, asseverar-se-á que, ao passo que no primeiro conceito está em causa a reserva sobre as coisas, os eventos, as doenças ou os lugares sobre a qual a pessoa tem um interesse legítimo; no segundo, por seu turno, aquilo que está em jogo não é a proteção do interesse material do outro na preservação do segredo, mas antes a pretensão do outro em que sejam respeitadas as barreiras preordenadas à tutela da sua esfera bem como o seu direito à disposição sobre a mesma[10].

Uma vez que quem comunica à distância tem de contar com as particularidades técnicas de um meio de comunicação e com os diferentes dispositivos de comunicação que neles se interpõem, já não é, no atual momento, difícil de representar que tanto o conteúdo, como as circunstâncias estão expostas à "intromissão facilitada" daquele terceiro[11]. Fácil é concluir

[8] Para um maior desenvolvimento das particularidades em que decorrem as telecomunicações, consulte-se Manuel da Costa Andrade, "artigo 194.º", *op. cit.*, p. 1095.

[9] Neste sentido, *idem*, "*Bruscamente no Verão Passado*", *A Reforma do Código de Processo Penal – Observações críticas sobre uma lei que podia e devia ter sido diferente*, Coimbra: Coimbra Editora, 2009, p. 158.

[10] Sobre isto, *idem*, *Liberdade de Imprensa e Inviolabilidade Pessoal – Uma Perspectiva Jurídico-Criminal*, Coimbra: Coimbra Editora, 1996, pp. 92-93, e *idem*, "A utilização e valorização do resultado de escutas telefónicas em processos disciplinares desportivos" (Parecer), *in*: *Desporto & Direito – Revista Jurídica do Desporto*, Ano VI, N.º 18 (maio/agosto 2009), p. 378. Entendendo o primeiro como um "*concepto de carácter objetivo o material*", em que a proteção é destinada à área que cada um reserva para si e para os seus íntimos, e o segundo como um "*concepto rigurosamente formal*", em que a proteção é dispensada pela evidente vulnerabilidade das comunicações realizadas num canal cerrado através da intermediação técnica de um terceiro, cf., no Tribunal Constitucional de Espanha, a STC 170/2013, de 7 de outubro, FJ 4.

[11] Novamente, Manuel da Costa Andrade, "Métodos ocultos de Investigação (*plädoyer* para uma teoria geral)", *in*: Mário Ferreira Monte (dir.), Maria Clara Calheiros / Fernando Conde Monteiro / Flávia Noversa Loureiro (coord.) *Que Futuro para o Direito Processual Penal? – Simpósio em Homenagem a Jorge de Figueiredo Dias, Por*

que, à luz do exposto, radicando o fundamento do caráter autónomo e separado do reconhecimento deste direito fundamental e da sua específica proteção constitucional na especial vulnerabilidade da confidencialidade destas comunicações – já que, repita-se uma vez mais, são possibilitadas mediante a intermediação técnica de um terceiro alheio à comunicação –, a confidencialidade da comunicação telefónica compreende, por isso, não apenas o segredo do conteúdo do comunicado, como ainda a confidencialidade das circunstâncias ou dados externos da conexão telefónica[12]. Como na forma particularmente sugestiva da literatura jurisprudencial alemã, a inviolabilidade da privacidade das telecomunicações procura evitar que a troca de opiniões e informação através dos meios de telecomunicações cesse ou seja modificada porque as partes da comunicação esperam que o Estado interfira na sua comunicação ou tire nota das circunstâncias ou do conteúdo[13].

Excluídos do âmbito de proteção deste parâmetro estão, porém, o conteúdo e as circunstâncias das telecomunicações armazenadas após a conclusão da comunicação na esfera do assinante, na medida em que este possa tomar as suas precauções de proteção contra o acesso secreto. E isto porque, de acordo com o que se viu, a tutela constitucional do sigilo das telecomunicações restringe-se aos "dados emanados de um processo de telecomunicação em curso"[14]. Da mesma forma com que também não são objeto de proteção deste direito fundamental os dados de base (como, por exemplo, o número de contacto telefónico, endereço eletrónico e contrato de ligação à rede), bem como os dados de localização de equipamento, quando não dão suporte a uma concreta comunicação[15]. Na verdade, em posição que tem vindo a ser reiterada pelo Tribunal Constitucional Português, se o objeto de proteção é uma comunicação individual, então os dados que não façam parte do processo de comunicação não são abrangidos pelo âmbito da tutela do sigilo das telecomunicações. Estão, isso sim, como o mesmo Tribunal também assinala, sujeitos à proteção concedida pelo direito à reserva da intimidade da vida privada, consagrado, como já salientámos, no artigo 26.º da CRP[16].

Ocasião dos 20 anos do Código de Processo Penal Português, Coimbra: Coimbra Editora, 2009, p. 538.

[12] Cf. STC 123/2002, de 20 de maio, FJ 5 e 6.

[13] Veja-se, nesta linha, na jurisprudência do Tribunal Constitucional Federal Alemão (BVerfG), a Decisão de 14.07.1999 – 1 BvR 2226/94, 162-163, e a Decisão de 24.01.2012 – 1 BvR 1299/05, 111.

[14] Nesta conclusão, a Decisão do BVerfG de 27.02.2008 – 1 BvR 370/07, 1 BvR 595/07, 185 e 190.

[15] Note-se que o Acórdão do TC n.º 486/2009, ponto 2.3, catalogou como dados de tráfego os dados de localização celular que fornecem a posição geográfica do equipamento móvel com base em atos de comunicação, mencionando que são "tratados para permitir a transmissão das comunicações".

[16] Cf. Acórdão do TC n.º 403/2015, ponto 15; Acórdão do TC n.º 420/2017, ponto 13; Acórdão do TC n.º 464/2019, ponto 8; e Acórdão do TC n.º 268/2022, ponto 10.

Se as coisas se antolham deste jeito, não se compreende a intenção, atualmente existente, de submeter os dados de tráfego, os dados de base e os dados de localização de equipamento ao mesmo denominador comum em termos de regime jurídico constitucional. Em primeiro lugar, porque na compreensão que fez vencimento no Tribunal Constitucional Português – acompanhando, de resto, a doutrinal nacional e a mais relevante jurisprudência estrangeira –, o mesmo sempre foi perentório em esclarecer que, ao contrário do que sucede com os dados de tráfego – que comungam, sem margem para dúvidas, da específica proteção constitucional da inviolabilidade das telecomunicações –, o acesso aos dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação, não materializa uma violação do artigo 34.º, n.º 4. Estes estão, pelos argumentos expostos, cobertos pelo parâmetro do artigo 26.º, n.º 1. Depois, porque se a tal presidir o objetivo de ultrapassar alguma objeção em termos de conformidade com a CRP, nem esse argumento será compreensível, na medida em que, depois da Lei Orgânica n.º 4/2017 – já aqui referida – o SIED e o SIS já podem aceder, legitimamente, a dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação[17].

5. Sinalizadas as dificuldades existentes ao nível da terminologia que mais rigorosamente representa o circunstancialismo da comunicação e as diferenças de regime que devem interceder entre o seu acesso e outros métodos ocultos de investigação, é agora o momento de destacar as maiores perplexidades que o articulado do PS suscita do ponto de vista das finalidades que justificam as restrições ao direito ao sigilo das telecomunicações. Antes, porém, é necessário empreender uma curta descrição das particularidades do campo em que se desenvolvem as diligências administrativas pró-ativas dos serviços de informações, de modo a que, com esse suporte, as considerações posteriores se prestem a um melhor entendimento.

Assim, e cumprindo o objetivo proposto, é correto mencionar que, partindo do pressuposto de que é a prática de atos de execução o marco de

[17] Inversamente ao que sucedeu com a norma do artigo 4.º da Lei Orgânica 4/2017, que, na parte em que previa o acesso a dados de tráfego que envolvam comunicação intersubjetiva para efeitos de produção de informações necessárias à prevenção de atos de espionagem e de terrorismo, foi declarada inconstitucional pelo Acórdão do TC n.º 464/2019, por violação do preceituado no artigo 34.º, n.º 4 da CRP; a norma do artigo 3.º, na parte em que prevê o acesso a dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação, para efeitos da produção de informações necessárias à prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada, não foi declarada inconstitucional pelo mesmo Acórdão.

referência que situa o início da investigação criminal – uma vez que, nos termos do Código Penal, os atos preparatórios não são puníveis, salvo disposição em contrário, sendo que apenas a tentativa de cometimento do crime em princípio o é, enquanto prática de atos de execução de um crime que decidiu cometer sem que este chegue a consumar-se (cf. o artigo 21.º e o artigo 22.º, n.º 1) –, é numa fase antecedente a essa que as investigações preventivas do SIED e do SIS encontram o seu lugar[18]. De modo a concretizar, importa esclarecer que, num domínio radicalmente oposto ao da fase de inquérito do Código de Processo Penal (CPP), os seus objetivos consistem, essencialmente, em observar e reportar ameaças que possam desestabilizar a comunidade como um todo, em ordem a permitir uma avaliação da situação de segurança a nível político. Situam-se no campo avançado (*Vorfeld*) da ocorrência de factos criminosos – enquanto campo privilegiado da sua atuação –, pelo que, não estando dependentes de qualquer suspeita concreta e individualizada da prática do crime, as suas investigações secretas e ocultas, para além de serem marcadas pelo alargamento do universo de pessoas a serem alvo de observação, podem também – diga-se de um modo claro – estender o seu raio de ação a comportamentos perfeitamente legais, já que não estão limitadas a ações ilícitas[19].

No que fica dito estão já elencadas algumas das principais coordenadas que perpassam a atuação das agências do SIRP. Destarte, retomando o ponto que nos trouxe até aqui, cabe agora enunciar que, se este é um domínio que, estando situado numa fase antecedente à do início do processo penal, é marcado pelo alargamento dos alvos das ações de vigilância e não está balizado a comportamentos ilícitos, não pode, então, deixar de ser encarada com dificuldades a recolha de dados de tráfego para a prevenção de atos de sabotagem. Embora, na regulamentação jurídica que para esta matéria teceu o legislador português, a produção de informações para a salvaguarda

[18] Sobre a demarcação entre as ações de investigação criminal e as atividades de prevenção, cf. Helena Morão, "Início da tentativa e detenção em flagrante delito", *in*: Maria Fernanda Palma / Augusto Silva Dias / Paulo de Sousa Mendes / Carlota Almeida (coord.), *Direito da Investigação Criminal e da Prova*, Coimbra: Almedina, 2014, p. 40, e *idem*, «Autoria e participação no "crime contratado"», *in*: Associação Sindical dos Funcionários de Investigação Criminal da Polícia Judiciária (ASFIC/PJ), Instituto de Direito Penal e Ciências Criminais da Faculdade de Direito da Universidade de Lisboa (IDPCC/FDUL) (org.), Maria Fernanda Palma / Augusto Silva Dias / Paulo de Sousa Mendes (coord.), *2.º Congresso de Investigação Criminal*, Coimbra: Almedina, 2010, pp. 60-61.

[19] Consulte-se, na jurisprudência alemã, a Decisão do BVerfG de 24.04.2013 – 1 BvR 1215/07, 118, e, na doutrina portuguesa, Manuel da Costa Andrade, "Bruscamente no Verão Passado", *op. cit.*, p. 130; *idem*, "Métodos ocultos de Investigação (*plädoyer* para uma teoria geral)", *op. cit.*, pp. 530-531, e *idem*, "Processo penal e polícia – fenomenologia da metamorfose", *in*: *Revista de Legislação e de Jurisprudência* 151, n.º 4035 (julho-agosto 2022), pp. 343-344.

da prevenção da sabotagem seja uma das finalidades de que o SIS está expressamente incumbido, não se pode, ainda assim, deixar de alertar que a consagração de meios fortemente restritivos de direitos fundamentais neste domínio tão sensível levanta sérias e fundadas reservas. Sendo a área em que se movem os serviços de informações um campo largamente indeterminado, não é fácil estabelecer a fronteira entre a prática de atos perfeitamente lícitos, que representam o exercício de certas liberdades, como a liberdade de expressão, de manifestação e o direito à greve, e a prática de atos potencialmente subversivos do Estado de direito constitucionalmente estabelecido. Embora este não seja o momento para formular uma resposta acabada e completa a esta questão, não é despiciente perguntar, como alguém já perguntou, se, no âmbito da amplitude da área em que, segundo vimos, os serviços de inteligência se movem, perante agitação académica e social, protestos como o "fecho a cadeado" das portas de uma universidade ou o "corte" (temporário) de uma estrada já podem, neste âmbito, justificar o início de uma ação de vigilância[20].

E se este é um ponto que causa perplexidades, a complexidade sobe de tom quando se considera a possibilidade de acesso a dados de tráfego para a prevenção da criminalidade altamente organizada. Embora não exista um consenso quanto a este último conceito a nível europeu e a nível internacional[21], em Portugal, para a sua concretização já conta o intérprete com a noção plasmada na alínea m) do artigo 1.º do CPP, na qual se dispõe que aquela abrange as condutas que integrem crimes de associação criminosa, tráfico de órgãos humanos, tráfico de pessoas, tráfico de armas, tráfico de estupefacientes ou de substâncias psicotrópicas, corrupção, tráfico de influência, participação económica em negócio ou branqueamento. Esta não é uma área isenta de controvérsia em sede de processo penal, na medida em que, em tema que não desenvolveremos, já se colocou tanto a interrogação de quais as respostas que a lei, a doutrina e a jurisprudência vão dar aos problemas colocados pela criminalidade altamente organizada[22], bem como o problema de saber se pode

[20] Levantando estas interrogações, cf. a Declaração de Voto de Pedro Machete ao Acórdão do TC n.º 464/2019, ponto 4.1.

[21] Afirmando-o, Hans-Jörg Albrecht, "Criminalidade organizada na Europa: perspectivas teorética e empírica", *in*: org. Associação Sindical dos Funcionários de Investigação Criminal da Polícia Judiciária, Instituto de Direito Penal e Ciências Criminais da Faculdade de Direito da Universidade de Lisboa; Maria Fernanda Palma / Augusto Silva Dias / Paulo de Sousa Mendes (coord. cient.), *2º Congresso de investigação criminal*, Coimbra: Almedina, 2010, p. 76.

[22] Veja-se Maria João Antunes, "Direito Processual Penal – Direito Constitucional Aplicado", *in*: *Que Futuro para o Direito Processual Penal?* – Simpósio em Homenagem a Jorge de Figueiredo Dias, Por Ocasião dos 20 anos do Código de Processo Penal Português, Coimbra: Coimbra Editora, 2009, pp. 753-754.

haver criminalidade altamente organizada sem que existam indícios do crime de associação criminosa[23].

Contudo, no campo avançado da colheita de informações – onde, como já tivemos a oportunidade de ver, estão situados os serviços de informações – a maior questão que se coloca é a de saber como admitir aí o acesso a dados de tráfego para a prevenção da criminalidade altamente organizada. É certo que este é um setor onde as agências de inteligência congéneres têm, tradicionalmente, competências na recolha e tratamento de informações. Mas, em Portugal, não se pode escapar ao dado inevitável de que, albergando a alínea m) do artigo 1.º do CPP um vasto conjunto de crimes que se inserem na categoria da criminalidade económico-financeira, aqueles ilícitos-criminais não encontram correspondência nas atribuições que, nos respetivos diplomas, foram legalmente cometidas ao SIRP[24].

6. Mesmo que a consagração do acesso para a prossecução daquelas finalidades não levantasse objeções, oferecia, ainda assim, margem para dúvidas saber se, num sentido oposto ao propugnado pelo Projeto do PS, aquela não é, antes, matéria da incumbência do legislador ordinário e não do legislador constitucional. E, acolhendo-nos à lição do direito comparado, o que é facto é que um breve percurso pelas normas constitucionais congéneres força-nos, de imediato, à conclusão de que noutros ordenamentos jurídicos não se foi ao ponto de discriminar, nos textos constitucionais, os interesses a serem prosseguidos com a restrição do direito ao sigilo das telecomunicações.

A Constituição da República Federativa do Brasil de 1988 – que, nesta matéria, optou por uma forma similar à portuguesa – preceitua, no artigo 5.º, XII, que "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal". Não é muito diferente

[23] Esta não é uma interrogação desprovida de relevo, mesmo para a realidade que temos em vista, pois caso se admita a existência de criminalidade organizada sem que haja crime de associação criminosa, poder-se-á questionar se, bastando a verificação de indícios de qualquer um dos crimes elencados, existe criminalidade altamente organizada no caso em que A, que conduz o seu automóvel com excesso de velocidade, oferece um suborno a um agente policial numa operação stop para que não lhe seja aplicada nenhuma sanção. Sobre isto, Cláudia Santos, *O Direito Processual Penal Português em Mudança – Rupturas e Continuidades*, Coimbra: Almedina, 2020, p. 48.

[24] Cf., num sentido semelhante, a propósito de algumas soluções contidas no Projeto de Lei n.º 480/XIII/2ª e na Proposta de Lei n.º 79/XIII, o parecer sobre o Projeto de Lei n.º 480/XIII/2ª e sobre a Proposta de Lei n.º 79/XIII da Procuradoria-Geral da República de 2017, ponto 4.1.1.2. Sobre as atribuições legalmente atribuídas ao SIRP, cf. *supra*, nota 2.

a formulação adotada noutros textos constitucionais que, ao contrário deste último, não limitaram a possibilidade da ocorrência de restrições ao sigilo das telecomunicações às hipóteses subsumíveis no âmbito do processo criminal[25]. A Constituição Espanhola de 1978 dispõe, no artigo 18. 3., que "é garantido o segredo das comunicações e, em especial, das postais, telegráficas e telefónicas, salvo decisão judicial". Por seu turno, a Constituição da República Italiana de 1947 preceitua, no artigo 15., que "a liberdade e o segredo da correspondência e de outras formas de comunicação são invioláveis" e que "só podem ser restringidas por ato fundamento da autoridade judiciária com as garantias estabelecidas na lei". Já a Lei Fundamental da República Federal da Alemanha estatui, no artigo 10 (1), que o sigilo da correspondência, das comunicações postais e das telecomunicações é inviolável e, no (2), que "as restrições só podem ser ordenadas nos termos da lei" e ainda que "se restrição servir para proteger a ordem básica democrática livre ou a segurança da Federação ou de um *Land*, a lei pode prever que a pessoa afetada não seja informada da restrição e que o recurso para os tribunais seja substituído por uma revisão do caso por agências ou agências auxiliares nomeadas pelos representantes do povo". Na mesma matéria, na Áustria, a Lei Básica do Estado de 21 de dezembro de 1867 sobre os direitos gerais dos cidadãos nos Reinos e *Länder* representados no Conselho do Reino enuncia, no artigo 10a (1), que "o sigilo das telecomunicações não deve ser violado" e, no (2), que "as exceções ao disposto no parágrafo anterior só são admissíveis com base numa autorização judicial de acordo com as leis existentes". Por fim, apenas para elencar mais um exemplo, a Constituição da Dinamarca de 1953 determina, no artigo 72.º, a "busca domiciliária, apreensão e exames de cartas e outros documentos, bem como qualquer violação do sigilo a ser observado nos assuntos postais, telegráficos e telefónicos só pode ter lugar sob ordem judicial, a menos que uma exceção particular seja autorizada por lei"[26].

7. Para, finalmente, fechar o ciclo das nossas reflexões, cabe ainda assinalar, dentro do escopo desta reflexão, que, a dar-se a modificação da norma do artigo 34.º, conferindo-se, assim, legitimamente o acesso a dados de tráfego pelo SIED e pelo SIS, surgirá, inevitavelmente, um conjunto de

[25] Se é verdade que em matéria de negação da possibilidade de restrição do direito ao sigilo das telecomunicações para a consecução das finalidades legalmente cometidas aos serviços de informações Portugal está isolado no contexto do espaço europeu, não deixa, porém, de ser igualmente certo que, no Brasil, a Agência Brasileira de Inteligência (ABIN), criada pela Lei n.º 9.883, de 7 de dezembro de 1999, também não está autorizada a quebrar o sigilo telefónico.

[26] Tradução livre.

questões com as quais o legislador ordinário terá, no futuro, de se confrontar em vista da concretização daquele acesso.

Atendendo a que o SIRP alberga dois serviços distintos com responsabilidades na produção de informações – um serviço "interno", com a delimitação da sua competência territorial aos poderes soberanos do Estado português (o SIS), e um serviço "externo", responsável pela recolha e análise de informações fora do território nacional (o SIED)[27] – fica por responder como compatibilizar com a Constituição a recolha de dados de tráfego no âmbito da vigilância estratégica ocorrida fora do território português. Este é, segundo nos parece, um tema que ainda não foi alvo de debate na doutrina e na jurisprudência nacionais, mas já mereceu, em arestos significativos, a atenção do BVerfG. Assim, na Decisão de 14.07.1999, este órgão jurisdicional entendeu, naquilo que mais pretendemos destacar, que a criação de uma agência de vigilância no que respeita aos países estrangeiros é da competência do artigo 73.º, n.º 1 da Lei Fundamental[28]. Mais recentemente, na Decisão de 19.05.2020, o Tribunal abordou o tema sob o enfoque da vinculação do Estado alemão pelos direitos fundamentais, mesmo quando em causa estejam ações tomadas fora das fronteiras nacionais. Prevaleceu aí o entendimento de que a ligação entre os direitos fundamentais e as garantias dos direitos humanos é incompatível com a noção de que a aplicabilidade dos direitos fundamentais da Lei Fundamental termina na fronteira nacional, o que isentaria as autoridades alemãs de aderir aos direitos fundamentais e aos direitos humanos quando atuam no estrangeiro em relação a estrangeiros[29].

Ademais, em matéria de exigências de reserva de lei – que devem ser cumpridas por todos os meios ocultos de investigação[30] – sabendo que os serviços de informações desenvolvem as suas atividades de prevenção antes da aquisição da notícia do crime – antes, portanto, de um inquérito aberto em sede de processo penal –, coloca-se a questão de saber como criar uma regulamentação que preveja um grau de suspeita que se apoie em factos

[27] Delimitando as competências do SIS ao aos poderes soberanos do Estado português, cf. o artigo 34.º da Lei n.º 9/2007, de 19 de fevereiro.

[28] Cf. Decisão de 14.07.1999 – 1 BvR 2226/94, 198.

[29] Cf. Decisão de 19.05.2020 – 1 BvR 2835/17, 96. Com efeito, a designada "vigilância estratégica" é já uma realidade presente noutros ordenamentos jurídicos. A título de exemplo, em França, o *Code de la sécurité intérieure* consagra, no Capítulo IV do Título V, as "*mesures de surveillance des communications électroniques internationales*"; no Reino Unido, o *Investigatory Powers Act* de 2016 disciplina, na Parte 6, os "*Bulk warrants*"; e, na Alemanha, a Lei sobre a restrição do sigilo das cartas, correios e telecomunicações (*Artikel 10-Gesetz - G 10*) regulamenta, na Secção 3, a "Restrição Estratégica" (*Strategische Beschränkungen*).

[30] Sobre isto, paradigmaticamente, cf. Manuel da Costa Andrade, "Métodos ocultos de Investigação (*plädoyer* para uma teoria geral)", *op. cit*., p. 539 e ss.

objetivos, factos esses que não existem nas investigações de campo avançado; qual o propósito de um catálogo de crimes numa área em que ainda não há um facto ilícito típico; como balizar o âmbito de aplicação da medida a um universo de pessoas bem definido numa área em que não existem as categorias do processo penal do suspeito, do arguido, da pessoa que sirva de intermediário e da vítima; e, pela ausência destas categorias, quais as garantias a firmar em sede de eliminação de dados. Por fim, em sede de reserva de juiz, tendo presente que as variáveis consagradas em sede de reserva de lei serão, pelas caraterísticas da área da prevenção, inevitavelmente menos densas do que as que estão previstas no regime das escutas telefónicas dos artigos 187.º a 190.º do CPP, como garantir a intensidade do controlo desses mesmos pressupostos por parte do juiz e, sabendo que esta é uma área dominada pelo segredo de Estado, como garantir, depois da execução do método, o contraditório, por parte do visado, do despacho judicial autorizante da ingerência[31].

8. Numa breve e conclusiva síntese, partindo do pressuposto de que o acesso a dados de tráfego pelo SIRP é uma realidade que veio para ficar – à qual já manifestámos, numa outra oportunidade, uma total e frontal oposição[32] – resta, ainda assim, esperar que sejam ultrapassados alguns dos principais aspetos problemáticos contidos nos Projetos de Revisão Constitucional estudados.

Deste modo, para efeitos de concretização das entidades competentes para esse acesso, o legislador constitucional não pode optar pela terminologia de "serviços de informações", em detrimento da referência, já contida no texto da Constituição, a "sistema de informações da República", de modo a evitar qualquer confusão com outros domínios do contexto militar e policial. Da mesma forma com que, a nível terminológico, mais correta será uma fórmula como "dados de tráfego" e não uma como "dados de contexto resultantes de telecomunicações", uma vez que é a primeira aquela que é utilizada com maior frequência para designar o circunstancialismo da comunicação. Além disso, estes, comungando da proteção constitucional da inviolabilidade das

[31] Sobre estes problemas, mais desenvolvidamente, João Narciso, *O acesso a dados de tráfego pelo Sistema de Informações da República Portuguesa*, Coimbra: Gestlegal, 2022, p. 103 e ss. Para demonstrar a relevância da densidade e determinabilidade da lei restritiva, veja-se Jorge Reis Novais, *As restrições aos direitos fundamentais não expressamente autorizadas pela Constituição*, 2.º ed., Coimbra: Wolters Kluwer Portugal | Coimbra Editora, 2010, p. 843, para quem a intensidade do controlo judicial sobre a atividade administrativa está ela mesma dependente daquela densidade normativa.

[32] Cf. João Narciso, *O acesso a dados de tráfego pelo Sistema de Informações da República Portuguesa*, *op. cit*., p. 85 e ss.

telecomunicações do artigo 34.º, n.º 4, não podem estar sujeitos ao mesmo regime dos dados de base e de localização de equipamento, quando não dão suporte a uma concreta comunicação, os quais estão cobertos pelo parâmetro do direito à reserva da intimidade da vida privada do artigo 26.º, n.º 1. Por último, no âmbito das finalidades, oferece margem para dúvidas a possibilidade do acesso a dados de tráfego para a prevenção de atos de sabotagem e da criminalidade altamente organizada. Se no primeiro caso, dada a amplitude da atuação dos serviços de informações – que não está balizada a comportamentos ilícitos – não é fácil estabelecer a fronteira entre a prática de atos que representam o exercício de certas liberdades e atos potencialmente lesivos do Estado de direito constitucionalmente protegido, no segundo são abrangidos ilícitos criminais que não correspondem às atribuições legais do SIRP. Tudo isto para afirmar, refira-se numa última nota, que o legislador deve evitar que o acesso ao circunstancialismo do processo comunicacional deixe de ser um método excecional e passe a receber uma utilização alargada e desmesurada.