Artigo 6.º

Outras obrigações de registo

O cumprimento das obrigações em matéria de registo constantes do presente Regulamento não prejudica o cumprimento das obrigações de registo aplicáveis por força de legislação especial, nomeadamente as relativas ao movimento transfronteiriço de resíduos e às matérias de estatísticas de resíduos.

Artigo 7.º

Entidades responsáveis por sistemas de fluxos específicos de resíduos

As entidades responsáveis por sistemas de fluxos específicos de resíduos, coletivos ou individuais, na qualidade de utilizadores, preenchem mapas de registo específicos cujo conteúdo incide sobre a atividade objeto de licença ou autorização.

Artigo 8.º

Entidades responsáveis por sistemas de gestão de resíduos urbanos

As entidades responsáveis por sistemas de gestão de resíduos urbanos, na qualidade de utilizadores, preenchem os Mapas de Registo de Resíduos Urbanos, cujo conteúdo incide sobre a atividade objeto de licença ou autorização.

Artigo 9.º

Gestão do SIRER

1 — Compete à APA, I. P. praticar os atos necessários a garantir o regular funcionamento do SIRER, o cumprimento das obrigações legais aplicáveis e a observância de adequados níveis de qualidade e segurança.

2 — A APA, I. P. é a entidade responsável pela verificação e tratamento da informação constante dos mapas de registo.

Artigo 10.º

Acesso ao SIRER

1 — A APA, I. P. faculta o acesso aos dados às entidades com competências em matéria de resíduos, nomeadamente entidades inspetivas e fiscalizadoras e entidades licenciadoras, nos termos do RGGR.

2 — A APA, I. P. disponibiliza os dados ao Instituto Nacional de Estatística para produção de estatísticas nacionais sobre resíduos.

Artigo 11.º

Relatórios síntese dos mapas de registo

A APA, I. P. elabora relatórios de síntese da informação constante dos mapas de registo até ao dia 31 de dezembro de cada ano civil, com a informação relativa ao ano anterior.

Artigo 12.º

Taxas

1 — Os utilizadores do SIRER procedem ao pagamento da taxa de registo anual, prevista no artigo 57.º do RGGR, antes de enviarem os mapas de registo de resíduos.

2 — O envio dos mapas de registo de resíduos só é admissível após o pagamento da taxa de registo, devendo a sua regularização ser solicitada na plataforma eletrónica da ANR.

3 — O pagamento da taxa de registo pode efetuar-se através de transferência bancária, débito em conta, ou qualquer outro meio de pagamento admitido, fazendo o atraso no pagamento incorrer o sujeito passivo em juros de mora, nos termos da lei tributária.

Artigo 13.º

Responsabilidade criminal

A prestação de falsas declarações e o acesso indevido ao sistema informático são passíveis de gerar responsabilidade criminal, nos termos previstos na lei.

TRIBUNAL CONSTITUCIONAL

Acórdão do Tribunal Constitucional n.º 403/2015

Processo n.º 773/15

Acordam, em Plenário, no Tribunal Constitucional

I — *Relatório.* — 1 — O Presidente da República requereu, em 7 de agosto de 2015, ao abrigo do n.º 1 do artigo 278.º da Constituição da República Portuguesa (CRP) e do n.º 1 do artigo 51.º e do n.º 1 do artigo 57.º da Lei de Organização, Funcionamento e Processo do Tribunal Constitucional, aprovada pela Lei n.º 28/82, de 15 de novembro (LTC), que o Tribunal Constitucional aprecie a conformidade com o disposto no n.º 4 do artigo 34.º da CRP da norma constante do n.º 2 do artigo 78.º do Decreto n.º 426/XII da Assembleia da República, que «Aprova o Regime Jurídico do Sistema de Informações da República Portuguesa», revogando as Leis n.os 30/84, de 5 de setembro, e 9/2007, de 19 de fevereiro, e os Decretos-Leis n.os 225/85, de 4 de julho, e 254/95, de 30 de setembro, recebido na Presidência da República no dia 6 de agosto de 2015, para ser promulgado como Lei.

O pedido assenta nos seguintes fundamentos:

«[…]

1.º Pelo Decreto n.º 426/XII, a Assembleia da República aprovou o Regime Jurídico do Sistema de Informações da República Portuguesa.

2.º No n.º 2 do artigo 78.º do referido Decreto estabelece-se que 'os oficiais de informações do SIS e do SIED podem, para efeitos do disposto na alínea *c*) do n.º 2 do artigo 4.º, e no seu exclusivo âmbito, aceder a informação bancária, a informação fiscal, a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização, sempre que sejam necessários, adequados ou proporcionais, numa sociedade democrática, para o cumprimento das atribuições legais dos serviços de informações, mediante a autorização prévia e obrigatória da Comissão de Controlo Prévio, na sequência de pedido devidamente fundamentado'.

3.º A justificação para o regime aprovado pode encontrar-se na exposição de motivos que acompanhava a proposta de lei do Governo segundo a qual 'no contexto da recente Estratégia Nacional de Combate ao Terrorismo [...] e dos desafios colocados pelas novas ameaças à segurança nacional, surge como incontornável o acesso a meio operacionais consagrados pela primeira vez de modo transparente e expresso na lei positiva, indo ao encontro do padrão de garantias quer da Carta Europeia dos Direitos Fundamentais quer da Convenção Europeia dos Direitos do Homem. Neste contexto, e em linha com a maior parte dos Estados-Membros da União Europeia, prevê-se o acesso aos metadados, isto é, o acesso a dados conservados pelas operadoras de telecomunicações, o que se rodeia de especiais regras para salvaguardar integralmente os direitos dos cidadãos, em especial o direito à privacidade.'

4.º Não está em causa, assim, o mérito e a necessidade deste regime, o qual, de resto, foi aprovado por uma expressiva maioria, superior a dois terços dos Deputados em efetividade de funções.

5.º Coloca-se, todavia, a questão de saber — não tendo esta dúvida sido ignorada pelo legislador na referida exposição de motivos, sendo, por outro lado, amplamente sublinhada nos diversos pareceres que constam dos trabalhos preparatórios — se a norma em causa, sendo justificada pelas novas ameaças à segurança nacional, é conforme com o disposto na Constituição em matéria de privacidade das telecomunicações.

6.º Com efeito, estabelece-se no n.º 4 do artigo 34.º da Constituição que 'é proibida toda a ingerência das autoridades públicas na correspondência nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo criminal'.

7.º Em face da norma constitucional citada surgem duas dúvidas fundamentais quanto ao problema em análise: *i*) deve o acesso aos metadados considerar-se uma ingerência nas telecomunicações para os efeitos previstos na norma constitucional? e *ii*) pode considerar-se que a autorização prévia e obrigatória da Comissão de Controlo Prévio equivale ao controlo existente no processo criminal?

8.º Por um lado, em face da evolução tecnológica das últimas décadas, pode questionar-se a inclusão dos metadados no conceito de telecomunicações, tendo presente que a norma constitucional em causa foi aprovada num momento em que tais desenvolvimentos se encontravam ainda em fase inicial.

9.º Por outro lado, o legislador, porventura consciente das dificuldades de conformidade constitucional que a proposta suscitava, fez depender o acesso aos metadados de autorização prévia e obrigatória da Comissão de Controlo Prévio a qual, nos termos do disposto no artigo 35.º do mesmo Decreto, é 'composta por três magistrados judiciais, designados pelo Conselho Superior da Magistratura, de entre juízes conselheiros do Supremo Tribunal de Justiça, com, pelo menos, três anos de serviço nessa qualidade'.

10.º Coloca-se, pois, a questão de saber se esta autorização prévia concedida por uma Comissão com a mencionada composição satisfaz a exigência constante da última parte do n.º 4 do artigo 34.º da Constituição.

[…]»

2 — O requerimento deu entrada neste Tribunal no dia 7 de agosto de 2015 e o pedido foi admitido na mesma data.

3 — Notificada para o efeito previsto no artigo 54.º da LCT, a Presidente da Assembleia da República veio apresentar resposta na qual oferece o merecimento dos autos. Já após a fixação da orientação do Tribunal, foi apresentada pelo Governo uma Nota Explicativa, a qual foi apensa, por linha, ao processo.

4 — Elaborado o memorando a que alude o artigo 58.º, n.º 2, da LCT e fixada a orientação do Tribunal, importa decidir conforme dispõe o artigo 59.º da mesma Lei.

II — *Fundamentação.* — 5 — A única questão que o Tribunal deve apreciar refere-se à norma constante do n.º 2 do artigo 78.º do Decreto n.º 426/XII da Assembleia da República, que estatui o seguinte:

«Artigo 78.º

Acesso a dados e informações

1 — Os diretores e os dirigentes intermédios de primeiro grau do SIS e do SIED têm acesso a informação e registos relevantes para a prossecução das suas competências, contidas em ficheiros de entidades públicas, nos termos de protocolo, ouvida a Comissão Nacional de Proteção de Dados no quadro das suas competências próprias.

2 — Os oficiais de informações do SIS e do SIED podem, para efeitos do disposto na alínea *c*) do n.º 2 do artigo 4.º, e no seu exclusivo âmbito, aceder a informação bancária, a informação fiscal, a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização, sempre que sejam necessários, adequados e proporcionais, numa sociedade democrática, para cumprimento das atribuições legais dos serviços de informações, mediante a autorização prévia e obrigatória da Comissão de Controlo Prévio, na sequência de pedido devidamente fundamentado.»

Para bem se compreender o alcance do n.º 2 do artigo 78.º agora introduzido pelo Decreto n.º 426/XII e ajuizar da sua validade constitucional, há que ter presente o sentido prescritivo dos preceitos para que remete, nomeadamente a alínea *c*) do n.º 2 do artigo 4.º e os artigos 20.º, 35.º a 38.º, que criam e regulam a «Comissão de Controlo Prévio», os quais estatuem o seguinte:

«Artigo 4.º

Atribuições

1 — . . . . . .

2 — Os serviços de informações desenvolvem atividades de recolha, processamento, exploração e difusão de informações:

a) Necessárias à salvaguarda da independência nacional, dos interesses nacionais e da segurança interna e externa do Estado Português;

b) Que contribuam para garantir as condições de segurança dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade e pelos princípios do Estado de Direito; e

c) Adequadas a prevenir a sabotagem, a espionagem, o terrorismo, e sua proliferação, a criminalidade altamente organizada de natureza transnacional e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido.

Artigo 20.º

Disposições gerais

Sem prejuízo das atribuições próprias da Assembleia da República e dos demais órgãos de soberania, a atividade do SIRP é objeto de fiscalização externa especializada da competência exclusiva das seguintes entidades independentes:

a) O Conselho de Fiscalização do SIRP;
b) A Comissão de Fiscalização de Dados do SIRP;
c) A Comissão de Controlo Prévio.

Artigo 35.º

Comissão de Controlo Prévio

A Comissão de Controlo Prévio é composta por três magistrados judiciais, designados pelo Conselho Superior da Magistratura, de entre juízes conselheiros do Supremo Tribunal de Justiça, com pelo menos três anos de serviço nessa qualidade.

Artigo 36.º

Competência

1 — A Comissão de Controlo Prévio é a entidade competente para a concessão de autorização prévia de acesso à informação e aos dados previstos no n.º 2 do artigo 78.º

2 — O pedido para a concessão de autorização prévia prevista no número anterior é decidido ponderando a relevância dos seus fundamentos e a salvaguarda dos direitos, liberdades e garantias constitucionalmente previstos.

3 — A Comissão de Controlo Prévio elabora anualmente um relatório de atividades, que remete à comissão parlamentar competente para os assuntos constitucionais, direitos, liberdades e garantias e ao Conselho de Fiscalização do SIRP.

Artigo 37.º

Procedimento

1 — O pedido para a concessão da autorização prévia prevista no número anterior é da competência dos diretores do SIS ou do SIED, ou de quem os substitua em caso de ausência ou impedimento, com conhecimento ao Secretário-Geral.

2 — O pedido previsto no número anterior é apresentado por escrito e contém os seguintes elementos:

a) Indicação concreta da ação operacional a realizar e das medidas requeridas;
b) Factos que suportam o pedido, finalidades que o fundamentam e razões que aconselham a adoção das medidas requeridas;
c) Identificação da pessoa ou pessoas, caso sejam conhecidas, envolvidas nos factos referidos na alínea anterior e afetadas pelas medidas e indicação do local onde as mesmas devam ser realizadas;
d) Duração das medidas requeridas, que não pode exceder o prazo máximo de três meses, prorrogáveis mediante autorização expressa.

3 — A decisão é da competência do juiz a quem tenha sido distribuído o pedido, podendo haver decisões do coletivo em matérias de particular complexidade.

4 — O juiz outorga a decisão de concessão ou de denegação da autorização, por despacho fundamentado proferido no prazo máximo de 72 horas.

5 — Em situações de urgência devidamente fundamentadas no pedido dos serviços de informações, pode ser solicitada ao juiz a redução para 24 horas do prazo previsto no número anterior.

6 — O procedimento previsto no presente artigo é coberto pelo regime do segredo de Estado nos termos do artigo 15.º

7 — O Secretário-Geral ordena a destruição imediata de todos os dados e informação recolhidos mediante a autorização prevista no presente artigo, sempre que não tenham relação com o objeto ou finalidades da mesma.

8 — Por decisão do coletivo de juízes, pode ser determinado o cancelamento de quaisquer procedimentos de acesso a informação e a dados previstos no n.º 2 do artigo 78.º, bem como participados à Comissão de Fiscalização de Dados do SIRP os elementos conducentes à destruição imediata dos respetivos dados ou informações.

Artigo 38.º

Extensão de regime à Comissão de Controlo Prévio

Aplica-se à Comissão de Controlo Prévio, com as necessárias adaptações e naquilo que não for incompatível com o Estatuto dos Magistrados Judiciais, o disposto nos artigos 25.º a 27.º, em matéria de imunidades, deveres, direitos e regalias.»

6 — Importa começar por delimitar o objeto do recurso, uma vez que o Requerente termina o pedido solicitando a fiscalização preventiva da constitucionalidade dirigida à norma do n.º 2 do artigo 78.º do Decreto n.º 426/XII, preceito que transcreve na sua integralidade, no artigo 2.º do requerimento.

Assim, tomado em toda a sua amplitude semântica, o pedido parece apontar no sentido de que se pretende ver apreciada a conformidade constitucional dos vários tipos de acesso admitidos aos oficiais de informações do SIS e do SIED para efeitos do disposto na alínea *c*) do n.º 2 do artigo 4.º do Decreto n.º 426/XII, a saber, o acesso a *informação bancária*, o *acesso a informação fiscal* e o acesso a *dados de tráfego*, de *localização* ou outros *dados conexos* das comunicações. Porém, uma leitura conjugada do pedido com os fundamentos exarados nos artigos 3.º a 10.º do requerimento conduz a outro entendimento, mais restrito.

Com efeito, o Requerente transcreve no artigo 3.º o segmento da Exposição de Motivos da Proposta de Lei n.º 345/XII — na origem do Decreto em análise — , em que se alude tão-somente ao acesso aos *metadados*, enquanto dados — estruturais ou descritivos — produzidos no âmbito ou em conexão com um processo de telecomu-

nicação, registados e conservados pelas respetivas operadoras, conceito que é retomado nos artigos 7.º, 8.º e 9.º do requerimento. Por outro lado, nenhuma menção é feita à possibilidade de acesso dos oficiais do SIS e do SIED a informação de outra natureza, nem às condicionantes respetivas.

Mostra-se, assim, seguro considerar que o pedido de fiscalização preventiva da constitucionalidade da normação contida no n.º 2 do artigo 78.º não abrange a possibilidade de acesso dos oficiais de informações do SIS e SIED a informação bancária e fiscal, prevista no Decreto n.º 426/XII.

Importa ainda ter desde já em atenção que a conexão que é estatuída entre os dados a que os mesmos oficiais de informação podem ter acesso — condicionado e funcionalmente orientado à identificação da fonte, destino, data, hora, duração e tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização — , e um processo comunicacional — realizado ou tentado — permite estabelecer uma relação de correspondência entre tais *dados* e aqueles compreendidos no conceito de *dados de tráfego*, tal como acolhido na Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto, diploma de transposição da Diretiva n.º 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho (*JO,* n.º L201, de 31 de julho de 2002). Releva especialmente o considerando (15) da Diretiva (*JO,* n.º L201/38), explicitando o sentido e alcance dos *dados de tráfego*, nos seguintes termos:

> «Uma comunicação pode incluir qualquer informação relativa a nomes, números ou endereços fornecidos pelo remetente de uma comunicação ou pelo utilizador de uma ligação para efetuar a comunicação. Os dados de tráfego podem incluir qualquer tradução desta informação pela rede através da qual a comunicação é transmitida, para efeitos de execução da transmissão. Os dados de tráfego podem ser, nomeadamente, relativos ao encaminhamento, à duração, ao tempo ou ao volume de uma comunicação, ao protocolo utilizado, à localização do equipamento terminal do expedidor ou do destinatário, à rede de onde provém ou termina a comunicação, ao início, fim ou duração de uma ligação. Podem igualmente consistir no formato em que a comunicação é enviada pela rede.»

Nesta aceção, o tratamento dos *dados de localização* que fornecem a posição geográfica do equipamento terminal de um utilizador e que se destinam a permitir a transmissão das comunicações, mormente no âmbito de sistemas de telecomunicações móveis, encontra-se abrangido pelo conceito de *dados de tráfego*, aplicando-se-lhes o disposto nos artigos 6.º da Diretiva n.º 2002/58/CE [cf. considerando (35)] e da Lei n.º 41/2004, de 18 de julho.

Diferentemente, outros *dados de localização*, decorrentes da capacidade de tratamento que as redes móveis digitais possam deter [referida pelo considerando (35)] como «a capacidade de tratar dados de localização que são mais precisos do que o necessário para a transmissão de comunicações, tais como serviços que prestam aos condutores, informações e orientações individualizadas sobre o tráfego», previstos nos artigos 9.º da Diretiva n.º 2002/58/CE e 7.º da Lei n.º 41/2004, de 18 de julho, porque não conexos com a transmissão de comunicações, não se encontram compreendidos na norma objeto do pedido e, correspondentemente, no âmbito da cognição deste Tribunal.

Assim, constitui objeto do presente pedido de fiscalização preventiva da constitucionalidade, sobre a qual cumpre emitir pronúncia, a norma, constante do n.º 2 do artigo 78.º do Decreto n.º 426/XII, nos termos da qual, *os oficiais de informações do SIS e do SIED podem, para efeitos do disposto na alínea c*) *do n.º 2 do artigo 4.º, e no seu exclusivo âmbito, aceder a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização, sempre que sejam necessários, adequados e proporcionais, numa sociedade democrática, para cumprimento das atribuições legais dos serviços de informações, mediante a autorização prévia e obrigatória da Comissão de Controlo Prévio, na sequência de pedido devidamente fundamentado.*

7 — Inserindo-se a norma objeto do presente recurso no âmbito de um diploma que visa estabelecer um novo Regime Jurídico do Sistema de Informações da República Portuguesa, começaremos por apresentar uma breve evolução histórica do quadro jurídico-normativo do Sistema de Informações da República (SIRP).

A Lei de Defesa Nacional publicada na sequência da primeira revisão constitucional — operada em 1982 — veio prever a criação de um sistema de informações nacional. Nesse propósito, foi publicada a Lei-Quadro do Sistema de Informações da República Portuguesa (LQSIRP) — a Lei n.º 30/84, de 5 de setembro, sucessivamente alterada pelas Leis n.os 4/95, de 21 de fevereiro, 4/95, de 21 de fevereiro, 15/96, de 30 de abril, 75-A/97, de 22 de julho, e pela Lei Orgânica n.º 4/2004, de 6 de novembro — na qual se consagraram os principais princípios em matéria de recolha e tratamento de informações.

A Lei-Quadro n.º 30/84 estabeleceu as bases gerais das informações em Portugal e definiu as regras relativas ao funcionamento, direção e controlo de todos os respetivos órgãos, procedendo ao enquadramento de acordo com um fluxo de poder e dependência tutelar, determinando ainda a sujeição dos mesmos a estruturas de fiscalização, com enunciação de missões, deveres e responsabilidades dos serviços propriamente ditos e também das entidades fiscalizadoras. Formalmente, o SIRP definia-se como estrutura orgânica de serviços públicos que tinha por incumbência, em regime de exclusividade e no quadro democrático do Estado de Direito, «a produção de informações necessárias à salvaguarda da independência nacional e à garantia da segurança interna» (artigo 2.º, n.º 2, da LQSIRP). A lei previa, no âmbito da sua estrutura, a criação de três serviços de informações: o Serviço de Informações Estratégicas de Defesa (SIED), o Serviço de Informações Militares (SIM) e o Serviço de Informações e Segurança (SIS). A regulamentação destes serviços foi aprovada pelos Decretos-Leis n.os 224/85 (que estabeleceu a orgânica do SIED), 225/85 (que regulamentava o SIS) e 226/85 (que veio regulamentar o SIM), todos publicados em 4 de julho de 1985.

As décadas de oitenta e noventa foram, de resto, prolíficas do ponto de vista legislativo na área da segurança interna, com reflexos no Sistema de Informações da República: assim, foi publicada a Lei de Segurança Interna (Lei n.º 20/87, de 12 de junho) e a Lei do Segredo de Estado (Lei n.º 6/94, de 7 de abril). E também a Lei-Quadro do

SIRP foi objeto de alterações várias, a primeira das quais em 1995, com a extinção do Serviço de Informações Militares e a atribuição da componente militar ao SIED, que passou a denominar-se SIEDM — Serviço de Informações Estratégicas e de Defesa Militar (Lei n.º 4/95, de 21 de fevereiro). Ainda em 1995, em 30 de setembro, foi publicado o Decreto-Lei n.º 254/95, para regulamentar o SIEDM.

Posteriormente, a Lei Orgânica n.º 4/2004, de 13 de agosto, reestruturou o Sistema de Informações da República Portuguesa, colocando os dois Serviços de Informações na dependência direta do Primeiro-Ministro e criando o cargo de Secretário-Geral do SIRP, para coordenar e conduzir superiormente a atividade dos Serviços de Informações. O SIEDM perdeu a componente militar e recuperou a designação original de SIED (Serviço de Informações Estratégicas de Defesa).

Na sequência da dita Lei Orgânica n.º 4/2004, foi publicada a Lei n.º 9/2007, de 19 de fevereiro (alterada pela Lei n.º 50/2014, de 13 de agosto), cumprindo-se uma meta essencial da reforma do Sistema de Informações da República Portuguesa (SIRP). Esta Lei estabelece a orgânica do Secretário-Geral do SIRP, do Serviço de Informações Estratégicas de Defesa (SIED) e do Serviço de Informações de Segurança (SIS), criando uma estrutura bipolar unificada por um vértice de condução superior, inspeção, superintendência e coordenação, sendo um dos ângulos o SIED e o outro o SIS, com vértice no Secretário-Geral do SIRP. Consagrou-se, assim, um quadro regulador unitário do SIRP, que concretiza os pormenores de organização e funcionamento do Secretário-Geral, do SIED e do SIS, e das estruturas comuns necessárias para assegurar o cumprimento da missão, que se traduz na produção de informações necessárias à salvaguarda da independência nacional e à garantia da segurança interna.

Neste quadro legal, a atividade do SIRP está especificamente limitada por alguns princípios inscritos nos n.os 1 e 3 do artigo 3.º e n.º 1 do artigo 4.º da LQSIRP: (*i*) o *princípio da constitucionalidade e da legalidade*: a atividade dos serviços de informações está sujeita ao escrupuloso respeito pela Constituição e pela lei, designadamente em matéria de proteção dos direitos fundamentais das pessoas, especialmente frente à utilização de dados informatizados; (*ii*) o *princípio da exclusividade*: a atividade dos serviços está rigorosamente limitada às suas atribuições, não podendo desenvolver uma atividade de produção de informações em domínio que não lhe tenha sido concedido; (*iii*) o *princípio da especialidade*: a atividade dos serviços de informações reduz-se ao seu estrito âmbito, não podendo a sua atividade confundir-se com a atividade própria de outros organismos, como no domínio da atividade dos tribunais ou da atividade policial (cf. Jorge Bacelar Gouveia, «Os Serviços de Informações de Portugal: Organização e fiscalização», in *Estudos de Direito e Segurança,* Almedina, 2007, pp. 181-182).

É ainda de salientar a importância dada à proteção dos direitos, liberdades e garantias dos cidadãos, como resulta, ainda que implícito, daquele princípio da constitucionalidade ou legalidade, reforçado pelo disposto no artigo 6.º, n.º 1, da Lei n.º 9/2007: «O Secretário-Geral, os membros do seu Gabinete e os funcionários e agentes do SIED, do SIS e das estruturas comuns não podem desenvolver atividades que envolvam ameaça ou ofensa aos direitos, liberdades e garantias consignados na Constituição e na lei.» De resto, o mesmo artigo 6.º dispõe ainda, nos seus n.os 2 e 3, de várias estatuições que inculcam nos princípios suprarreferidos: «[...] é vedado exercer poderes, praticar atos ou desenvolver atividades do âmbito ou da competência específica dos tribunais, do Ministério Público ou das entidades com funções policiais [...] [bem como] [...] é ainda expressamente proibido proceder à detenção de qualquer pessoa ou instruir inquéritos e processos penais».

Finalmente, refira-se que a separação da atividade de informações das atividades policial e de investigação criminal resulta, além de fatores históricos, de princípios e valores eminentes da nossa ordem jurídica.

8 — O Decreto n.º 426/XII da Assembleia da República, que aprova o Regime Jurídico do Sistema de Informações da República Portuguesa, visa, desde logo, reunir no mesmo diploma aspetos que se encontram dispersos por vários dos diplomas mencionados. Assim, propõe a revogação das atuais redações da Lei n.º 30/84, de 5 de setembro, da Lei n.º 9/2007, de 19 de fevereiro, do Decreto-Lei n.º 225/85, de 4 de julho, do Decreto-Lei n.º 370/91, de 7 de outubro, sobre regime contributivo do SIS, e do Decreto-Lei n.º 254/95, de 30 de setembro, com a introdução de um novo regime orgânico-funcional. É de referir que a Lei n.º 9/2007 já havia expressamente revogado, no respetivo artigo 72.º, os Decretos-Leis n.os 225/95 e 254/95, tendo estes perdurado, residualmente, em função do regime transitório estabelecido no artigo 71.º dessa mesma Lei, sendo essa a razão pela qual o Decreto n.º 426/XII, agora aprovado revoga, «adicionalmente», no artigo 175.º, os referidos Decretos-Leis de 1995.

Outro dos objetivos da proposta de lei que deu origem ao mencionado Decreto consiste na atualização do regime do SIRP às atuais exigências de informação e segurança. No que toca à orgânica do SIRP, prevê-se a constituição de três categorias de órgãos: (*i*) órgãos independentes de fiscalização (Conselho de Fiscalização do SIRP; Comissão de Fiscalização de Dados do SIRP e Comissão de Controlo Prévio); (*ii*) órgãos de direção e controlo (Primeiro-Ministro, Secretário-Geral); (*iii*) órgãos de coordenação e consulta (Conselho Superior de Informações; Conselho Consultivo). Especificamente no que toca à fiscalização, importa mencionar que se prevê a composição do Conselho de Fiscalização do SIRP por três cidadãos de reconhecida idoneidade, eleitos pela Assembleia da República, a composição da Comissão de Fiscalização de Dados do SIRP por três magistrados do Ministério Público nomeados pelo Procurador-Geral da República, com sede na Procuradoria-Geral da República, e, finalmente, a composição da Comissão de Controlo Prévio, por três magistrados judiciais, designados pelo Conselho Superior da Magistratura, de entre juízes conselheiros do Supremo Tribunal de Justiça, com, pelo menos, três anos de serviço nessa qualidade (artigos 20.º, 21.º, 29.º e 35.º do Decreto n.º 426/XII).

Em relação à norma que é objeto de fiscalização preventiva — o n.º 2 do artigo 78.º do Decreto n.º 426/XII —, o pensamento legislativo que esteve na sua base vem descrito na Exposição de Motivos da Proposta de Lei n.º 345/XII, nos seguintes termos:

> «No contexto da recente Estratégia Nacional de Combate ao Terrorismo, aprovado pela Resolução do Conselho de Ministros n.º 7-A/2015, de 20 de fevereiro, e dos desafios colocados pelas novas ameaças à segurança nacional, surge como incontornável o acesso a meios operacionais consagrados pela primeira vez de modo transparente e expresso na lei positiva, indo ao encontro do padrão de garantias quer da Carta Europeia

dos Direitos Fundamentais quer da Convenção Europeia dos Direitos do Homem.

Neste contexto, e em linha com a maior parte dos Estados-Membros da União Europeia, prevê-se o acesso aos metadados, isto é, o acesso a dados conservados pelas operadoras de telecomunicações, o que se rodeia de especiais regras para salvaguardar integralmente os direitos dos cidadãos, em especial o direito à privacidade. Efetivamente, admite-se, no artigo 78.º da presente proposta de lei, a possibilidade de acesso a dados de base, de localização e de tráfego, eventualmente considerados 'dados pessoais' para os efeitos do artigo 35.º da Constituição (CRP), mas não a 'ingerência nas comunicações', prevista no n.º 4 do artigo 34.º da CRP, do domínio do processo penal (âmbito, este, vedado aos serviços de informações, indiretamente, atentos os limites que a lei impõe à atividade do SIRP, ao impedir os serviços de informações de desenvolver ações próprias dos tribunais, do Ministério Público e das polícias).

O regime de acesso garante a finalidade vinculada à prevenção de fenómenos graves, como o terrorismo, a espionagem, a sabotagem e a criminalidade altamente organizada, e, mesmo nestes casos, é limitada ao estritamente adequado, necessário e proporcional numa sociedade democrática. Para o efeito, é criada uma entidade própria, a Comissão de Controlo Prévio (cf. os artigos 35.º a 38.º), que concede a autorização prévia do acesso à informação e dados necessários, numa dada operação, segundo um exigente procedimento legal, que visa a sindicância do acesso a dados pessoais que possa pôr em causa a reserva da intimidade da vida privada, a efetuar por três juízes.

O que se pretende é, não um acesso a conteúdos de comunicações (escritas ou de voz), por intrusão ou ingerência nas comunicações, mas o acesso autorizado a dados (de base, de localização e de tráfego), que são solicitados às entidades legitimamente responsáveis pelo seu tratamento, que os fornecem por determinação, e apenas nesse caso, daquela comissão de juízes, nos termos da presente lei, matéria que tem melhor inserção sistemática em sede do artigo 78.º (Acesso a dados e informação).»

O artigo 78.º está sediado na secção IV (Meios Legais) do capítulo I (Direção, coordenação e consulta) do título II (Do Secretário-Geral, das Estruturas Comuns, do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa), a parte do Diploma que estabelece e regulamenta os *meios de atuação* dos dois serviços integrados no SIRP: *meios operacionais* (artigo 74.º), *identidade e registos codificados* (artigo 75.º), *uso e porte de arma* (artigo 76.º), *utilização de meios de transporte* (artigo 77.º), *acesso a dados e informações* (artigo 78.º) e *passaporte especial e livre-trânsito* (artigo 79.º).

No confronto com o regime revogado, aquela secção IV sistematiza e define concretamente aquilo que, na estrutura da Lei n.º 30/84, aparecia algo descontextualizado, num quadro sistemático referido a «princípios gerais» (o capítulo I dessa Lei), onde convergiam, sempre num enunciado muito generalizador (*rectius*, pouco preciso), a definição do objeto da Lei (artigo 1.º), as finalidades do SIRP (artigo 2.º), o limite das atividades dos serviços de informações (artigo 3.º), a delimitação do âmbito de atuação destes (artigo 4.º), o acesso a dados e informações por estes (artigo 5.º), a exclusividade funcional dos serviços de informações (artigo 7.º) e a orgânica do SIRP (artigo 7.º).

9 — A norma do n.º 2 do artigo 78.º do Decreto n.º 426/XII atribui aos oficiais de informação do SIRP o poder funcional de aceder a *dados de comunicação* que permitam identificar o assinante ou utilizador, a fonte, o destino, data, hora, duração e o tipo de comunicação, bem como identificar o equipamento de telecomunicações ou a sua localização.

Considerando que o objeto do presente recurso diz respeito, especificamente, ao acesso aos dados relativos às telecomunicações por parte dos oficiais de informações, em primeiro lugar, convém caracterizar o tipo de dados em causa e saber se o acesso aos mesmos é merecedor de proteção constitucional.

A exposição de motivos que acompanhava a proposta de lei do Governo que esteve na origem do Decreto n.º 426/XII (cf. o artigo 3.º do pedido), em linguagem informática, qualifica-os como «metadados», usualmente definidos como «dados sobre dados», por dizerem respeito a circunstâncias das comunicações, e não ao próprio conteúdo da comunicação.

Numa concreta comunicação é possível separar do núcleo duro da informação fornecida ou transmitida um conjunto de marcos ou pontos de referência que lhe dão o respetivo suporte e que permitem circunscrever a informação sob todas as formas. Tais dados são «informações» que acrescem aos dados e que têm como objetivo informar sobre eles, em princípio, para tornar mais fácil a sua organização. Sendo dados sobre dados («informação sobre informação»), acabam por fornecer informação sobre a localização, tempo, tipo de conteúdo, origem e destino, entre outras, dos atos comunicacionais efetuados através de telecomunicações ou por outros meios de comunicação.

Como categoria que tem por fim um efeito jurídico é de usar a designação «dados de tráfego», não só por ser o enunciado linguístico que vem referido na norma objeto de fiscalização, mas sobretudo porque no nosso ordenamento jurídico já há uma definição legal desse enunciado. Com efeito, o artigo 2.º, n.º 1, alínea *d*), da Lei n.º 41/2004, de 18 de agosto, sobre Segurança nas Telecomunicações, define «dados de tráfego» como «quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma».

A este propósito, o Tribunal Constitucional acolheu, desde o Acórdão n.º 241/2002, de 29/05/2002, uma classificação tripartida (louvando-se, então, nos Pareceres do Conselho Consultivo da Procuradoria-Geral da República n.º 16/94, votado em 24/06/94, na base de dados da DGSI, n.º 16/94 — complementar, votado em 2/05/1996, in *Pareceres,* vol. VI, pp. 535 a 573, e n.º 21/2000, de 16/06/2000, no *Diário da República*, 2.ª série, de 28/08/2000) dos dados resultantes do serviço de telecomunicações. Ali se distinguiram:

> «[...] 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 (por exemplo, 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.»

Tal classificação tripartida foi retomada pelo Tribunal — assinalando que se mantinha, então, «consensual» — no Acórdão n.º 486/2009:

> «Não obstante a evolução legislativa acabada de enunciar, a verdade é que, relativamente ao tipo de dados envolvidos no serviço de telecomunicações, continua a ser consensual, no seio da doutrina e jurisprudência nacionais, a classificação adotada pelo Conselho Consultivo da Procuradoria-Geral da República, que distingue entre dados de base, dados de tráfego e dados de conteúdo (v. Parecer n.º 16/94/complementar, acessível em www.dgsi.pt, e Parecer n.º 21/2000, no *Diário da República,* 2.ª série, de 23 de julho de 2002).
>
> Assim, de harmonia com esses pareceres, no serviço de telecomunicações podem distinguir-se as seguintes espécies de dados:
>
> Nos serviços de telecomunicações podem distinguir-se, fundamentalmente, três espécies ou tipologias de dados ou elementos: 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 (por exemplo, localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência), dados de tráfego; e os dados relativos ao conteúdo da comunicação ou da mensagem, dados de conteúdo.
>
> Sendo os vários serviços de telecomunicações utilizados para a transmissão de comunicações verbais ou de outro tipo (mensagens escritas, dados por pacotes), os elementos inerentes à comunicação podem, por outro lado, estruturar-se numa composição sequencial em quatro tempos: a fase prévia à comunicação, o estabelecimento da comunicação, a fase da comunicação propriamente dita e a fase posterior à comunicação.
>
> No primeiro tempo relevam essencialmente os dados de base, enquanto que nos restantes importa essencialmente a consideração dos dados de tráfego e de conteúdo.
>
> Os dados de base constituem, na perspetiva dos utilizadores, os elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respetivo serviço: interessa aqui essencialmente o número e os dados através dos quais o utilizador tem acesso ao serviço.
>
> [...]
>
> Diversamente dos elementos de base (elementos necessários ao estabelecimento de uma base para comunicação), que estão aquém, antes, são prévios e instrumentos de qualquer comunicação, os chamados elementos de tráfego (elementos funcionais da comunicação), como os elementos ditos de conteúdo, têm já a ver diretamente com a comunicação, quer sobre a respetiva identificabilidade, quer relativamente ao conteúdo propriamente dito da mensagem ou da comunicação.
>
> Os elementos ou dados funcionais (de tráfego), necessários ou produzidos pelo estabelecimento da ligação da qual uma comunicação concreta, com determinado conteúdo, é operada ou transmitida, são a direção, o destino *(adressage)* e a via, o trajeto *(routage)*.
>
> [...]
>
> Estes elementos funcionalmente necessários ao estabelecimento e à direção da comunicação identificam, ou permitem identificar, a comunicação: quando conservados, possibilitam a identificação das comunicações entre o eminente e o destinatário, a data, o tempo, e a frequência das ligações efetuadas.
>
> Constituem, pois, elementos já inerentes à própria comunicação, na medida em que permitem identificar, em tempo real ou *a posteriori*, os utilizadores, o relacionamento direto entre uns e outros através da rede, a localização, a frequência, a data, hora e a duração da comunicação, devem participar das garantias a que está submetida a utilização do serviço, especialmente tudo quanto respeite ao sigilo das comunicações.
>
> Finalmente, os elementos de conteúdo — dados relativos ao próprio conteúdo da mensagem, da correspondência enviada através da utilização da rede.»

Ora, importa enquadrar os dados em causa na norma objeto do presente recurso numa das categorias enunciadas. Reportando-se os mesmos aos «dados de tráfego», «dados de localização» ou a outros «dados conexos» das comunicações — como a própria lei enuncia — necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, data, hora, duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização, dúvidas não restam que os mesmos se podem qualificar como *dados de tráfego*, por respeitarem «aos próprios elementos funcionais da comunicação, reportando-se à direção, destino, via e trajeto de uma determinada mensagem». São dados, pois, que identificam ou permitem identificar a comunicação e, uma vez conservados, possibilitam a identificação das comunicações entre emitente e destinatário, a data, o tempo e a frequência das ligações efetuadas.

No que toca aos dados de localização, consistem em dados tratados numa rede de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de telecomunicações, podendo incidir sobre a latitude, longitude ou altitude do equipamento, sobre a direção da deslocação, sobre a identificação da célula de rede em que o equipamento está localizado em determinado momento e sobre a hora de registo da informação de localização. Como acima se referiu, ao delimitar o objeto do recurso, tem-se considerado que os mesmos estão também incluídos no conceito mais amplo de «dados de tráfego» (assim, Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, Almedina, 2005, p. 181). E é nesse sentido que a Lei n.º 32/2008, de 17 de julho, que regula a conservação e transmissão dos dados de tráfego e de localização, reserva a mesma disciplina jurídica para ambos.

10 — O acesso a dados relativos a comunicações encontra-se, entre nós, sujeito a ampla regulamentação legal, impulsionada sobretudo pelo direito comunitário.

Após o primeiro diploma, que estabeleceu os princípios gerais das comunicações — o Decreto-Lei n.º 188/81, de 2 de julho —, as ulteriores Leis de Bases das Redes e Prestação de Serviços de Telecomunicações — Lei n.º 88/89, de 11 de setembro, e Lei n.º 91/97, de 1 de agosto — preocuparam-se em regular o tratamento dos dados pessoais gerados pelas telecomunicações. Nesta última Lei previa-se expressamente, no n.º 2 do artigo 17.º, uma cláusula destinada a garantir a inviolabilidade e o sigilo dos serviços de telecomunicações de uso público, nos termos da lei.

Entretanto, foi aprovada a Lei de Proteção de Dados Pessoais — Lei n.º 67/98, de 26 de outubro —, que se destinou a transpor para a ordem jurídica portuguesa a Diretiva 95/46/CE do Parlamento e do Conselho, de 24 de

outubro de 1995, relativa à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Posteriormente, a Lei n.º 69/98, de 28 de outubro — que transpôs a Diretiva 97/66/CE, do Parlamento Europeu e do Conselho —, veio regular o tratamento de dados pessoais e a *proteção da privacidade* no setor das telecomunicações, especificando e complementando as disposições da Lei da Proteção de Dados. Esse diploma impõe ao prestador de serviços de telecomunicações o dever de adotar todas as medidas técnicas e organizacionais necessárias para garantir a segurança desses serviços de telecomunicações, impondo também aos operadores de rede o dever de garantir a confidencialidade e o sigilo das telecomunicações, através dos serviços acessíveis ao público e das redes públicas de telecomunicações.

Os Decretos-Leis n.os 290-A/99 e 290-B/99, ambos de 30 de julho, vieram consagrar, como «obrigações dos operadores de redes públicas de telecomunicações», a proteção de dados e o *sigilo das comunicações* suportadas na rede que exploram e a de assegurar o sigilo das comunicações do serviço prestado, bem como o disposto na legislação de proteção de dados.

A introdução de novas tecnologias digitais nas redes de comunicações públicas trouxe consigo uma grande capacidade e possibilidade de tratamento de dados pessoais, e determinou a necessidade de acautelar novos requisitos específicos de proteção de dados pessoais e da privacidade dos utilizadores. De facto, os novos meios de comunicação, disponíveis a um custo cada vez menor e acessíveis a um número cada vez maior de pessoas, vieram multiplicar os riscos para a privacidade dos seus utilizadores. Tal facto justificou que a Diretiva 97/66/CE fosse revogada e substituída pela Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.

O objetivo deste novo regime foi estender a proteção oferecida pela anterior Diretiva aos utilizadores de serviços de comunicações publicamente disponíveis, independentemente das tecnologias utilizadas. Especificamente no que respeita aos *dados de tráfego*, a Diretiva define-os como «quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma, e podem ser, nomeadamente, relativos ao encaminhamento, à duração, ao tempo ou ao volume de uma comunicação, ao protocolo utilizado, à localização do equipamento terminal do expedidor ou do destinatário, à rede de onde provém ou onde termina a comunicação, ao início, fim ou duração de uma ligação, ou ao formato revestido pela mesma». A normativa europeia estabelece, em particular, regras referentes à eliminação dos dados, exigindo, para a sua conservação, o respeito pelo princípio da proporcionalidade. Nesse ponto, refere-se que «a eliminação dos dados de tráfego justifica-se pela sua especial sensitividade, que poderia permitir elaborar e revelar o perfil da comunicação, dando a conhecer, v. g., a sua origem geográfica» (Catarina Sarmento e Castro, *ob. cit.,* p. 172).

E, assim, mercê do dever de transposição desta nova diretiva europeia, a referida Lei n.º 69/98 foi revogada pela Lei n.º 41/2004, de 18 de agosto, a qual veio aprovar o regime jurídico do tratamento de dados pessoais e da proteção da privacidade no setor das comunicações eletrónicas. Este último diploma legal preocupou-se especialmente com a faturação detalhada e a localização celular. Em conformidade com a diretiva europeia transposta, a Lei n.º 41/2004 não prejudica a possibilidade de existência de legislação especial que restrinja a sua aplicação no que respeita à inviolabilidade das comunicações, nomeadamente para efeito de investigação e repressão de infrações penais (artigo 1.º, n.º 4).

Assim, na sequência desse diploma, foi aprovada a Lei n.º 32/2008, de 17 de julho, que transpôs para a ordem jurídica interna a Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15/03, 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, que estabelece amplas garantias no que toca ao acesso e conservação dos dados de tráfego e de localização das comunicações para fins de investigação, deteção e repressão de crimes graves por parte das autoridades.

11 — Para além da ampla regulamentação legal no que toca ao acesso aos dados, são ainda vários os *instrumentos internacionais* que protegem o acesso a dados deste tipo.

Não obstante alguns desses instrumentos não preverem normas detalhadas expressamente referentes à proteção de dados, garantem em várias normas a proteção da vida privada, onde se inserem, de forma inquestionável, limites ao acesso a dados pessoais, entre eles relativos a comunicações dos indivíduos, como, aliás, tem sido afirmado pelos órgãos de garantia dos respetivos instrumentos.

Assim, desde logo, o artigo 12.º da Declaração Universal dos Direitos do Homem declara que «ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência [...]». A mesma redação é retomada pelo artigo 17.º do Pacto Internacional Relativo aos Direitos Civis e Políticos. Ambos os textos prescrevem que o indivíduo tem direito à proteção da lei contra tais intervenções ou tais atentados.

O artigo 8.º da Convenção Europeia dos Direitos do Homem (CEDH), por seu turno, estabelece que «qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência». Nos termos do n.º 2, «não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros». O Tribunal Europeu dos Direitos do Homem (TEDH) tem desenvolvido uma ampla jurisprudência sobre a proteção do acesso a dados de comunicações, afirmando expressamente que os mesmos se encontram abrangidos pela proteção de «vida privada e familiar» ínsita no n.º 1 do artigo 8.º da CEDH. Assim, no caso *Malone c. Reino Unido*, referiu que o acesso e uso de dados respeitantes a tráfego de comunicações constituem matéria que é abrangida pelo âmbito de proteção do n.º 1 do artigo 8.º da CEDH (Acórdão de 02/08/1984, queixa n.º 8691/79).

Por fim, no contexto da União Europeia, cabe mencionar os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia. Note-se que, antes de a mesma produzir efeitos vinculativos, o Tribunal de Justiça da União Europeia já havia proclamado a existência de um «princípio geral de direito comunitário que consagra a proteção contra as intervenções arbitrárias e desproporcionadas do po-

der público na esfera da atividade privada de uma pessoa singular ou coletiva» (Acórdão de 22/10/2002, *Roquette Frères*, processo n.º C-94/00). Atualmente, o artigo 7.º da Carta dos Direitos Fundamentais consagra o respeito pela vida privada e familiar, dispondo, inspirado nas demais normas internacionais, que «todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações». Este direito vale, nos termos do artigo 52.º, n.º 3, da Carta, com o mesmo sentido que é conferido ao artigo 8.º da CEDH. Por seu turno, o artigo 8.º da Carta contém uma norma específica relativa à proteção de dados pessoais, proteção essa que recebe, assim, uma consagração expressa e autónoma face ao artigo 7.º A norma em causa estabelece que «todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito». O Tribunal de Justiça da União referiu que este direito está «indissociavelmente relacionado com o direito ao respeito pela vida privada» (Acórdão de 09/11/2010, *Volkerund Markus Schecke*, processos n.os C-92/09 e C-93/09). Por outro lado, esclareceu que a proteção de dados de tráfego das comunicações se encontra abrangida pelo âmbito de proteção deste direito fundamental (assim, o Acórdão de 08/04/2014, *Digital Rights Ireland Ltd*., processos n.os C-293/12 e C-594/12, que anulou a Diretiva 2004/26/CE, por violação dos artigos 7.º e 8.º da Carta dos Direitos Fundamentais).

12 — O acesso aos dados das comunicações efetivamente realizadas ou tentadas põe em causa direitos fundamentais das pessoas envolvidas no ato comunicacional. E não é apenas a invasão ou intromissão no conteúdo informacional veiculado pelos meios de transmissão (*dados de conteúdo*), que os afetam, mas também as circunstâncias em que a comunicação foi realizada (*dados de tráfego*).

Com efeito, mesmo que não haja acesso ao conteúdo, a interconexão entre dados de tráfego pode fornecer um perfil complexo e completo da pessoa em questão — com quem mais conversa, que lugares frequenta, quais os seus horários, etc. A verdade é que, como refere Costa Andrade, «no seu conjunto, os dados segregados pela comunicação e pelo sistema de telecomunicações se revelam, muitas vezes, mais significativos que o próprio conteúdo da comunicação em si. O que, de resto, bem espelha o interesse com que, reconhecidamente, a investigação criminal procura maximizar a recolha de *dados ou circunstâncias da comunicação*, também referenciados como *dados de tráfego*» (cf. «'Bruscamente no verão passado' — A Reforma do Código de Processo Penal», *Revista de Legislação e Jurisprudência,* ano 137.º, julho-agosto 2008, p. 338).

Isto mostra claramente que a manipulação ilegal ou ilegítima do conteúdo e das circunstâncias da comunicação pode violar a *privacidade* dos interlocutores intervenientes, atentando ou pondo em risco esferas nucleares das pessoas, das suas vidas, ou dimensões do seu modo de ser e estar. De sorte que a possibilidade de se aceder aos dados das comunicações colide com um conjunto de valores associados à *vida privada* que fundamentam e legitimam a proteção jurídico-constitucional.

Desde logo, a *liberdade de ação*, enquanto vertente do direito ao desenvolvimento da personalidade, de acordo com a qual, na interação com os outros, a condução da vida de cada um é *autoconformada* pela sua atuação, o que pressupõe, como referem Gomes Canotilho e Vital Moreira, «a exigência de *proibição de ingerências* dos poderes públicos [...] como, por exemplo, [...] 'o direito a não ser espiado'» (*Constituição da República Portuguesa Anotada,* 2.ª ed., vol. I, p. 465).

Depois, com a *esfera íntima* e a *esfera privada* da pessoa humana, seja enquanto pretensão de isolamento, tranquilidade e exclusão do acesso dos outros a si próprio (*direito à solidão*), seja, enquanto impedimento à ingerência dos outros (*direito ao anonimato*), seja ainda, mais modernamente, e perante a insuficiência protetora das referidas dimensões, enquanto controlo das informações que lhe dizem respeito e de subtração ao conhecimento dos outros os factos reveladores do modo de ser do sujeito na condução da sua vida privada (*autodeterminação informacional*). Como refere Joaquim Sousa Ribeiro, esta última dimensão, hoje a de maior relevo, «impede que o 'eu' seja objeto de apropriação pelos outros, como matéria de comunicação na esfera pública. Nela conjuga-se o *direito ao segredo* (à intromissão dos outros na esfera privada, com tomada de conhecimento de aspetos a ela referentes) e um *direito à reserva* (proibição de revelação)» — cf. «A tutela de bens da personalidade na Constituição e na jurisprudência constitucional portuguesas», in *Estudos de Homenagem ao Prof. Doutor José Joaquim Gomes Canotilho,* vol. III, Coimbra Editora, p. 853).

Estes direitos encontram-se hoje expressamente consagrados no artigo 26.º da CRP e são intimamente interligados, constituindo a reserva da intimidade da vida privada uma dimensão do direito, mais amplo, referente ao desenvolvimento da personalidade. Mas, não obstante se qualificar como um direito especial de personalidade, o direito à reserva da intimidade da vida privada não se esgota nele, pois está consagrado constitucionalmente como um direito autónomo. E neste ponto, não se confunde com o direito à *privacy* anglo-saxónica, que tem assumido contornos mais amplos, surgindo como expressão paradigmática de todos os direitos pessoais (cf. Jorge Miranda e Rui Medeiros, *Constituição da República Portuguesa Anotada,* t. I, 2.ª ed., Coimbra, 2010, p. 619).

O Tribunal Constitucional formulou, pela primeira vez, uma definição do conteúdo do direito à reserva da vida privada no Acórdão n.º 128/92, como constituindo o direito de cada um a ver protegido o espaço interior ou familiar da pessoa ou do seu lar contra intromissões alheias*, i. e.,* como um direito a uma esfera privada onde ninguém pode penetrar sem autorização do respetivo titular. No entender do Tribunal, esse direito compreende, por um lado, *a autonomia*, ou seja, o direito a ser o próprio a regular, livre de ingerências estatais e sociais, essa esfera de intimidade e, por outro, o direito a não ver difundido o que é próprio dessa esfera de intimidade, a não ser mediante autorização do interessado («direito ao segredo do ser»). E no que toca aos *lugares da vida* onde a vida privada pode ser manifestada, o Tribunal afirmou ainda que ela abrange «a vida pessoal, a vida familiar, a relação com outras esferas de privacidade [...] o lugar próprio da vida pessoal ou familiar [...] e, bem assim, os meios de expressão e de comunicações privados (a correspondência, o telefone, as conversas orais, etc.». De modo que, na jurisprudência constitucional, as *comunicações privadas*, englobando o *conteúdo* e *circunstancialismos* em que as mesmos têm lugar, são reconhecidas como um meio através do qual se manifestam aspetos da vida privada da pessoa e que, por isso, caem no âmbito da proteção constitucional da respetiva reserva.

Quanto ao âmbito objetivo do direito à reserva sobre a intimidade da vida privada, o Tribunal tem dito — em

consonância com a doutrina acima referida — (*i*) que tal direito inclui, como diferentes manifestações, o *direito à solidão*, o *direito ao anonimato* e o *direito à autodeterminação informativa*; (*ii*) que o direito ao livre desenvolvimento da personalidade, como liberdade comportamental, de livre conformação e expressão da personalidade, é entre nós tratado distintamente do direito à reserva, no sentido de livre controlo da informação sobre aquilo que, em decorrência dessa liberdade de conduta, cada um faz na sua esfera privada; (*iii*) que a fórmula «reserva de intimidade da vida privada» não pode ser interpretada restritivamente, de modo a circunscrever a proteção constitucional à vida *íntima*, pois que tal implicaria deixar de cobrir todas as outras esferas da vida que devem igualmente ser resguardadas do público, como condição de salvaguarda da integridade e dignidade das pessoas; (*iv*) e que o facto de se recusar a equivalência entre «privacidade» e «intimidade» não impede que se não estabeleçam graduações entre diferentes esferas da vida privada, consoante a sua maior ou menor ligação aos atributos constitutivos da personalidade (cf. entre outros, os Acórdãos n.os 306/2003, 368/2002, 355/97, 442/07 e 230/08).

13 — O direito ao desenvolvimento da personalidade, na dimensão de liberdade de ação de um sujeito autónomo dotado de autodeterminação decisória, naturalmente que comporta a *liberdade de comunicar*. Nesta dimensão relacional, do «eu» com o «outro», o objeto de proteção é a *comunicação individual*, isto é, a comunicação que se destina a um recetor individual ou a um círculo de destinatários previamente determinado. A liberdade de comunicar abrange a faculdade de comunicar com segurança e confiança e o domínio e autocontrole sobre a comunicação, enquanto expressão e exteriorização da própria pessoa. Tal liberdade, enquanto refração do direito ao desenvolvimento da personalidade e da tutela da privacidade, mereceu no texto constitucional um recorte material específico, através da autonomização, no artigo 34.º, do *sigilo dos meios de comunicação privada*. Servindo para proteger vários bens jurídico-constitucionais, ele é hoje, como refere Gomes Canotilho, «um dos núcleos essenciais do *direito à autodeterminação comunicativa*, juntamente com a proteção de *dados* pessoais constantes de ficheiros informatizados ou manuais» (cf. «Privatização e Direitos, Liberdades e Garantias. A propósito do sigilo de correspondência no serviço de telecomunicações», in *Estudos de Direitos Fundamentais,* 2.ª ed., p. 162).

Pode falar-se assim de um «direito à autodeterminação comunicativa» que serve para defender vários bens jurídico-constitucionais, entre eles: o direito ao desenvolvimento da personalidade e o direito à reserva da intimidade da vida privada.

Na vertente de defesa da reserva da intimidade da vida privada, o direito à autodeterminação comunicativa protege a esfera pessoal perante as ingerências públicas ou privadas, ou seja, o interesse das pessoas que comunicam em impedir ou em controlar a tomada de conhecimento, a divulgação e circulação do conteúdo e circunstâncias da comunicação. Neste sentido, os interlocutores intervenientes têm *direito a um ato negativo*: à não intervenção de terceiros na comunicação e nas circunstâncias que a acompanham. Trata-se de uma garantia de que devem beneficiar, *prima facie*, todas as comunicações privadas, independentemente de as mesmas dizerem ou não respeito à intimidade dos intervenientes (cf. Lucrecio Rebollo Delgado, «El Secreto de las Comunicaciones: Problemas Actuales», *Revista de Derecho Político*, n.º 48-49, 2000, p. 363).

No entanto, o direito à autodeterminação comunicativa abrange ainda esferas de proteção mais amplas que a da simples reserva da vida privada. É que o progresso tecnológico, ao facilitar a acumulação, conservação, circulação e interconexão de dados referentes às comunicações, aumentou as possibilidades de devassa. Agora é o próprio domínio de atuação do indivíduo que é posto em causa, pois já não tem meios para assegurar a confidencialidade da comunicação. A liberdade de, à distância, trocar com os destinatários livremente escolhidos por cada um, informações, notícias, pensamentos e opiniões está comprometida com as inimagináveis possibilidades da sua afronta pelos avanços tecnológicos. Por isso, é necessário assegurar que a comunicação à distância entre privados se processe como se os mesmos se encontrassem presentes, *i. e.,* que as comunicações entre emissor e recetor, bem como o seu circunstancialismo, se tenham como uma *comunicação fechada*, em que os sujeitos se *autodeterminam* quanto à realização da mesma e esperam, legitimamente, que a comunidade proteja o circunstancialismo daquela pretendida comunicação. Ora, como a interação entre pessoas que se encontram à distância tem de ser feita através da mediação necessária de um terceiro, de um fornecedor de serviços de comunicação, exige-se que esse operador e o Estado regulador também garantam a *integridade* e *confidencialidade* dos sistemas de comunicação.

Neste contexto, o direito à autodeterminação comunicativa assume-se como um direito de liberdade, de liberdade para comunicar, sem receio ou constrangimentos de que a comunicação ou as circunstâncias em que a mesma é realizada possam ser investigadas ou divulgadas. Sem essa confiança, o indivíduo sentir-se-á coartado na liberdade de poder comunicar com quem quiser, quando quiser, pelo tempo que quiser e quantas vezes quiser. Trata-se, pois, de permitir um livre desenvolvimento das relações interpessoais e, ao mesmo tempo, de proteger a confiança que os indivíduos depositam nas suas comunicações privadas e no prestador de serviços das mesmas. Como refere Costa Andrade, «a tutela da inviolabilidade das telecomunicações radica assim na 'específica situação de perigo' decorrente do domínio que o terceiro detém — e enquanto detém — sobre a comunicação (conteúdo e dados). Domínio que lhe assegura a possibilidade fáctica de intromissão arbitrária subtraída ao controlo do(s) comunicador(es). Por ser assim, o regime jurídico do sigilo na segurança e reserva dos sistemas apenas visa proteger a confiança na segurança e reserva dos sistemas (empresas) de telecomunicações.». (cf. Costa Andrade, *ob. cit.,* p. 339). Neste sentido, os comunicadores têm *direito a ações positivas* dos operadores e do Estado que não só assegurem a confidencialidade das comunicações e das circunstâncias em que elas se realizam como também lhes permitam controlar os dados produzidos, guardados e transmitidos que respeitem a comunicações já efetuadas.

E nisto se distingue do *direito à autodeterminação informativa* consagrado no artigo 35.º da CRP, com vista à proteção das pessoas perante o tratamento de dados pessoais informatizados. O objeto de proteção do *direito à autodeterminação comunicativa* reporta-se a *comunicações individuais* efetivamente realizadas ou tentadas e só essas é que estão cobertas pelo sigilo de comunicações. Naquele outro direito protegem-se as *informações pessoais* recolhidas e tratadas por entidades públicas e privadas,

cuja forma de tratamento e divulgação pode propiciar ofensas à privacidade das pessoas a que digam respeito. Como refere Maria Eduarda Gonçalves, neste caso, o problema não está na existência ou na quantidade de dados, mas na qualidade, «entendida esta, em termos amplos, como o conjunto das condições da recolha dos dados, seu tratamento e comunicação, bem como as características desses dados, isto é, a sua exatidão, a sua adequação aos fins prosseguidos» (cf. *Direito da Informação,* Almedina, p. 84). Neste caso, pretende-se impedir que as informações prestadas a um particular ou a uma entidade possam por estes ser divulgadas a outras pessoas ou entidades, ou seja, que a pessoa se torne «simples objeto de informações», face a todos os registos informáticos que vai deixando no seu dia a dia. A proibição de ingerência ou devassa neste domínio implica não apenas a proibição de acesso a terceiros aos dados pessoais mas ainda a proibição de divulgação ou mesmo de interconexão de ficheiros com dados da mesma natureza (cf. Gomes Canotilho e Vital Moreira, *ob. cit.,* p. 554).

De modo que é possível assinalar ao direito à autodeterminação comunicativa uma dupla vertente, enquanto proteção de uma reserva da vida privada e enquanto liberdade de atuação, ou seja, uma conexão entre «segredo das comunicações» e «liberdade de comunicação».

14 — A autodeterminação comunicativa é protegida no artigo 34.º da CRP através da inviolabilidade das comunicações. A «inviolabilidade de princípio» justifica-se, como referem Gomes Canotilho e Vital Moreira, para «limitar na maior medida possível a possibilidade de restrições, sujeitando-se estas a pressupostos bastante vinculados» (cf. *ob. cit.,* vol. I, p. 540). Nessa inviolabilidade inclui-se, no n.º 4 daquele preceito constitucional, a *proibição de ingerência* das autoridades públicas nos meios de comunicação, não só as que estão investidas de *poderes públicos de autoridade* como, mas por maioria de razão, as demais entidades públicas e entidades privadas (n.º 1 do artigo 18.º da CRP).

A garantia de não ingerência tem, porém, um sentido mais vasto que o sigilo de comunicações, podendo assumir um duplo relevo.

Desde logo, ela configura-se como uma garantia de *sentido negativo,* de inviolabilidade, que protege o indivíduo de ingerências do Estado ou de terceiros. Neste contexto assume-se como um direito que garante ao respetivo titular posições jurídicas perante o Estado para defesa de abusos relativos à utilização dos dados em causa. Como correspondência desta garantia, cabe ao Estado um dever de não ingerência*, de não agressão*. Deste direito deriva, como já se referiu, não só a obrigação de princípio de não divulgar o conteúdo das comunicações privadas mas também não aceder às circunstâncias em que as mesmas foram efetuadas.

Por outro lado, a garantia de não ingerência pode, ainda, reclamar um correspondente dever a *ações positivas* por parte do Estado. Desde logo, a obrigação de o Estado adotar os instrumentos jurídicos necessários para manter a comunicação e seu circunstancialismo como «fechados» (nomeadamente, através da aprovação de leis destinadas à proteção dos dados de comunicação). Nesse sentido, o n.º 2 do artigo 26.º da CRP estabelece, precisamente, uma obrigação legiferante, obrigando o legislador a estabelecer garantias contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações. Depois, através da efetivação do referido «direito ao apagamento» ou ao «bloqueio» dos dados de tráfego, que vai ínsito no direito à autodeterminação comunicativa, e no correspondente «direito ao esquecimento». De facto, o direito à autodeterminação comunicativa tem, nos dias de hoje, e face à tendencial perenidade dos registos de dados, de passar pela imposição de limites temporais à conservação dos dados.

15 — É em face da proibição de ingerência das autoridades públicas nas comunicações que o Requerente coloca uma primeira questão: deve o acesso aos dados de tráfego considerar-se uma ingerência nas telecomunicações para os efeitos previstos na norma constitucional?

A resposta passa por averiguar previamente se os chamados «dados de tráfego», na definição já referida, estão abrangidos no conceito de «telecomunicações» ou «demais meios de comunicação» enunciados no n.º 4 do artigo 34.º da CRP. Este preceito manteve a sua redação inalterada até à revisão constitucional de 1997, resultando dos trabalhos preparatórios da mesma que a alteração, com a aditação à referência a «demais meios de comunicação», visou «explicitar dimensões já contidas no artigo 34.º, n.º 4, no sentido de acompanhar a evolução tecnológica» (José Magalhães*, Diário da Assembleia da República,* 2.ª série, de 23 de abril de 1997, p. 2286).

Ora, há um largo consenso na doutrina e na jurisprudência, de resto não se conhece posição contrária, no sentido de se incluir os dados de tráfego no conceito de comunicações constitucionalmente relevante para a proibição de ingerência. Quer dizer: o âmbito de proteção do artigo 34.º, n.º 4, abrange não apenas o conteúdo das telecomunicações mas também os dados de tráfego.

Nesse sentido, Gomes Canotilho e Vital Moreira, em nota ao artigo 34.º da CRP, salientam que «a garantia do sigilo abrange não apenas o conteúdo da correspondência mas o 'tráfego' como tal (espécie, hora, duração, intensidade de utilização)» (*ob. cit.,* p. 544).

Para Costa Andrade, citando jurisprudência alemã, «na medida em que estivermos no âmbito das comunicações, o seu regime e a sua área de tutela abrangem, nos mesmos termos, tanto o *conteúdo* como os *dados ou circunstâncias da comunicação*». Sendo as coisas lineares em relação ao *conteúdo*, hoje não será difícil referenciar a fundamentação e o sentido da inclusão dos *dados da comunicação* sob a mesma área de tutela. Segundo a lição do Tribunal Constitucional Federal (02/03/2006): «também a intromissão nos dados cai na área de tutela do artigo 10.º da Lei Fundamental; o direito fundamental protege também a confidencialidade sobre as circunstâncias do processo de comunicação. O que compreende especialmente o *se*, o *quando*, o *como*, *entre que pessoas* ou *entre que aparelhos* a comunicação teve lugar. De outra forma, a tutela do direito fundamental seria incompleta, uma vez que os dados da comunicação têm um grande contexto expressivo (*Aussagegehalt*). Eles podem, em concreto, permitir conclusões decisivas sobre as ações de comunicação e de movimentação. A frequência, a duração e o momento das ligações dão informação sobre a espécie e intensidade das relações e permitem fazer ilações sobre o conteúdo.» (cf. *ob. cit.,* pp. 340 e 341).

Por sua vez, Germano Marques da Silva e Fernando Sá afirmam que «é possível perceber que a intenção da Constituição é oferecer proteção ao tráfego de informação escrita, desenhada ou falada, entre dois ou mais destinatários definidos» e «essa proteção, especialmente nos modernos meios de comunicação, é ainda constitucional-

mente garantida às circunstâncias em que se realizam as comunicações. Nesses termos, estão também protegidos os dados relativos aos meios de comunicação usados, à hora da sua utilização, à duração da sua utilização, ao local da sua utilização ou à identidade dos seus utilizadores.». (cf. «Anotação ao artigo 34.º», in *Jorge Miranda e Rui Medeiros, ob. cit.,* pp. 772 e 774).

O Tribunal Constitucional também já teve oportunidade de se pronunciar expressamente sobre este aspeto, tendo também equiparado a proteção dos dados de tráfego à proteção constitucionalmente concedida aos dados de conteúdo. Assim, no Acórdão n.º 241/02, em que refere expressamente que «a proibição de ingerência nas telecomunicações, para além de vedar a escuta, interceção ou vigilância de chamadas, abrange, igualmente, os elementos de informação com elas conexionados, designadamente os que no caso foram fornecidos pelos operadores de telecomunicações». A mesma interpretação foi retomada e amplamente desenvolvida no Acórdão n.º 486/2009, em que, reportando-se aos dados de tráfego, se afirmou que «num Estado de Direito democrático, assiste a qualquer cidadão o direito de telefonar quando e para quem quiser com a mesma privacidade que se confere ao conteúdo da sua conversa».

De igual modo, o Conselho Consultivo da Procuradoria da República, nos já referidos Pareceres n.os 16/94, Complementar, de 26/10/1995, e 21/2000, de 16/06/2000, defendeu que «os elementos funcionais, desde logo, os dados de tráfego, na medida em que permitem a identificação ou identificabilidade da comunicação (direção, destinatário, local, hora, duração), integram já elementos suficientemente relevantes da comunicação justificando a proteção do sigilo. São elementos que apenas se geram quando existiu e porque existiu uma determinada transmissão ou comunicação».

No mesmo sentido, o Parecer da Comissão Nacional de Proteção de Dados n.º 29/98, de 16/04/1998, ao concluir que a tutela constitucional do sigilo da correspondência e das telecomunicações «[...] abrange quer o denominado 'tráfego' da comunicação quer o conteúdo desta». Os referidos dados são mesmo considerados particularmente sensíveis, nos termos do artigo 7.º da Lei de Proteção de Dados.

Também a doutrina estrangeira tem defendido amplamente que a privacidade da comunicação ou a autonomia comunicacional abrange não apenas a proibição de interferência, em tempo real, do conteúdo de uma comunicação, como também a impossibilidade do ulterior acesso de terceiros a elementos que revelem as condições factuais em que decorreu uma comunicação (v., neste sentido, Nicolas--González-Cuéllar Serrano*, em* «Garantias constitucionales de la persucución penal en el entorno digital», in *Prueba e Processo Penal,* Tirant lo Blanch, 2008, pp. 171-174).

E semelhante entendimento tem o Tribunal de Justiça da União que, no já referido Acórdão de 08/04/2014, *Digital Rights Ireland Ltd*., processos n.os C-293/12 e C-594/12, que anulou a Diretiva 2004/26/CE, referiu ilustrativamente que, no que toca aos dados de tráfego das comunicações, «a conservação dos dados imposta pela Diretiva 2006/24 constitu[i] uma ingerência particularmente grave nesses direitos», embora não seja «suscetível de afetar o referido conteúdo, tendo em conta que, como resulta do seu artigo 1.º, n.º 2, esta diretiva não permite tomar conhecimento do conteúdo das comunicações eletrónicas, enquanto tal» (*parágrafo 39*). O TJ sublinhou várias vezes a gravidade da ingerência resultante de uma conservação ilimitada de dados de tráfego, pelo facto de os mesmos permitirem «designadamente, saber qual é a pessoa com quem um assinante ou um utilizador registado comunicou, e através de que meio, assim como determinar o tempo da comunicação e o local a partir do qual esta foi efetuada. Além disso, permitem saber com que frequência o assinante ou o utilizador registado comunicam com certas pessoas, durante um determinado período.» (*parágrafo 26*). Mais afirmou: «estes dados, considerados no seu todo, são suscetíveis de permitir tirar conclusões muito precisas sobre a vida privada das pessoas cujos dados foram conservados, como os hábitos da vida quotidiana, os lugares onde se encontram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais e os meios sociais frequentados» (*parágrafo 27*). Assim, conclui, *inter alia*, que «apesar de a Diretiva 2006/24 não autorizar [...] a conservação do conteúdo da comunicação e das informações consultadas através de uma rede de comunicações eletrónicas, não está excluído que a conservação dos dados em causa possa ter incidência na utilização, pelos assinantes ou pelos utilizadores registados, dos meios de comunicação previstos por esta diretiva e, consequentemente, no exercício, por estes últimos, da sua liberdade de expressão, garantida pelo artigo 11.º da Carta» (*considerando 28*).

Já quanto aos dados de base (v. g. número de telefone, endereço eletrónico, contrato de ligação à rede) e aos dados de localização de equipamento, quando não dão suporte a uma concreta comunicação, não são objeto de proteção do direito ao sigilo das comunicações (cf. Acórdão n.º 486/2009). De facto, se o objeto de proteção é uma comunicação individual, então os dados que não pressuponham uma concreta comunicação, que não façam parte do processo de comunicação, ainda que protegidos pela reserva da vida privada — artigo 26.º da CRP — não estão cobertos pela tutela do sigilo das comunicações.

Por tudo isso, também se entende que a área de proteção do sigilo das comunicações consagrada no n.º 4 do artigo 34.º da CRP, compreende tanto o conteúdo da comunicação como os dados de tráfego atinentes ao processo de comunicação. Na verdade, o acesso aos dados de tráfego pode constituir uma ingerência gravosa na vida privada das pessoas, já que se pode aceder a informações relativas a todas as chamadas efetuadas, incluindo as chamadas para as linhas de serviço de emergência/SOS/similares, ao número de chamadas, aos números de telefone chamados, à hora de início e duração de cada chamada e às respetivas unidades de contagem.

Concluímos, pois, respondendo à primeira questão colocada pelo Requerente neste processo, que a proibição de ingerência nas comunicações, constante do artigo 34.º da CRP, abrange os dados de tráfego.

16 — Assente que os dados de tráfego estão na área de tutela do sigilo das comunicações, importa responder à segunda questão do Requerente: pode considerar-se que a autorização prévia e obrigatória da Comissão de Controlo Prévio equivale ao controlo existente no processo criminal?

O artigo 34.º, após estabelecer, no n.º 1, o princípio segundo o qual «o domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis», prescreve, 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*».

Em relação às autoridades públicas, este preceito constitucional exprime duas normas contrapostas no seu sentido deôntico: uma *norma proibitiva* de toda a ingerência na correspondência, telecomunicações e demais meios de comunicação; e uma *norma permissiva* da ingerência nos casos previstos na lei em matéria de processo penal. Entre as duas normas há uma *relação de excecionalidade,* em que a norma proibitiva aparece como geral relativamente à norma permissiva, que exceciona. Com efeito, a norma permissiva autoriza o legislador a criar normas para um setor restrito de casos com uma configuração particular — «em matéria de processo penal» — que consagram uma disciplina oposta à constitucionalmente estabelecida como regime-regra.

O sacrifício do direito à inviolabilidade das comunicações privadas a razões imperiosas de investigação criminal consubstancia uma *restrição* ao conteúdo constitucional daquele direito fundamental, com o âmbito de proteção acima delimitado. O direito à inviolabilidade das comunicações não é pois um direito absoluto, visto que a Constituição autoriza uma intervenção normativa do legislador, para salvaguarda de outros valores constitucionais, nomeadamente de bens jurídicos dotados de dignidade penal (de bens jurídico-penais), ao serviço dos quais se encontra o processo criminal. De facto, o n.º 4 do artigo 34.º da CRP admite restrições a estabelecer por lei com fundamento em exigências de processo criminal relativamente à inviolabilidade de correspondência, telecomunicações e outros meios de comunicação. Trata-se, pois, de um preceito constitucional que contempla uma *previsão constitucional expressa* da restrição de um direito fundamental (sigilo das comunicações), preenchendo o pressuposto material da emanação de leis restritivas a que diretamente se refere ao artigo 18.º, n.º 2, primeira parte, da Lei Fundamental («a lei só pode restringir direitos, liberdades e garantias nos casos expressamente previstos na Constituição»).

Ora, como refere Gomes Canotilho, a autorização de restrição expressa de um direito fundamental «tem como objetivo obrigar o legislador a procurar sempre nas normas constitucionais o *fundamento concreto* para o exercício da sua competência de restrição de direitos, liberdades e garantias», de modo a criar *segurança jurídica* nos cidadãos, que poderão contar com a inexistência de medidas restritivas de direitos fora dos casos expressamente considerados pelas normas constitucionais como sujeitos a reserva de lei restritiva (cf. *Direito Constitucional e Teoria da Constituição*, 5.ª ed., p. 448). Sendo este o sentido das restrições estabelecidas por lei, mediante autorização expressa da constituição, a intervenção normativa abstrata do legislador ordinário só pode ocorrer nos *termos autorizados* pela norma constitucional e nos *casos nela previstos*.

Ora, o tipo de restrições ao direito à inviolabilidade das comunicações que é admitido pelo n.º 4 do artigo 34.º da CRP é muito mais exigente do que as restrições toleradas por outros direitos fundamentais em que se protegem os mesmos bens jurídicos (dignidade da pessoa, desenvolvimento da personalidade, garantia da privacidade, autodeterminação comunicativa). Contrariamente ao que se verifica em alguns desses direitos, em que, através da expressão «nos termos da lei», se atribui uma competência genérica de regulação que pode ser interpretada como incluindo poderes de restrição, a norma permissiva do n.º 4 do artigo 34.º autoriza a restrição do direito à inviolabilidade das comunicações apenas em determinado domínio normativo: «em matéria de processo criminal». Através deste segmento normativo, a autorização constitucional expressa para a restrição do direito à inviolabilidade das comunicações é completada com a discriminação dos *fins e interesses* a prosseguir com a lei restritiva ou com o *critério* que deve balizar a intervenção do legislador ordinário.

Este é, pois, um caso — a par do igualmente estabelecido no artigo 27.º, n.º 3, em que se estabelecem as condições da privação da liberdade — , em que é a própria Constituição que prevê diretamente uma determinada restrição, remetendo para a lei a sua concretização, mas tomando sempre como referencial o *processo criminal*. Noutras situações, a Constituição limita-se a admitir restrições não especificadas, como por exemplo nos artigos 35.º, n.º 4 (proibição de acesso a dados pessoais, salvo nos casos previstos na lei), 47.º, n.º 1 (liberdade de escolha de profissão salvas as restrições legais), 49.º, n.º 1 (direito de sufrágio ressalvadas as incapacidades previstas na lei geral), e 270.º (restrições estabelecidas por lei ao exercício de direitos pelos militares e agentes militarizados).

Enquanto no caso do artigo 34.º, n.º 4, a lei se limita a *declarar* a restrição prevista na Constituição, tendo de se conformar com o condicionalismo que se encontra expressamente recortado no preceito constitucional, nos outros casos, em que não existe uma tal especificação, a lei *cria* a restrição admitida pela Constituição, tendo, no entanto, de sujeitar-se aos requisitos de legitimidade impostos pelo princípio da proporcionalidade, como decorre do artigo 18.º, n.º 2, segunda parte. Tornando-se a todos os títulos claro, neste contexto, que o grau de vinculação do legislador é maior quando a restrição está, desde logo, expressamente prevista na norma constitucional (neste sentido, Gomes Canotilho e Vital Moreira, *ob. cit.*, vol. I, p. 391).

E não é de menor importância a fixação dos *termos da autorização* constitucional para a restrição, já que através deles se conhece também o *âmbito de proteção* da norma constitucional consagradora daquele direito fundamental. É que, como refere Gomes Canotilho, a norma constitucional que consagra um direito sujeito a reserva de lei restritiva, para além de autorizar o legislador a estabelecer limites ao âmbito de proteção constitucionalmente garantido (*norma de autorização de restrição*) é simultaneamente uma norma que reconhece e garante um determinado âmbito de proteção ao direito fundamental (*norma de garantia*) — cf. *ob. cit.,* p. 1260.

De modo que a enunciação constitucional expressa da matéria em que há autorização para uma intervenção legislativa limitadora do âmbito de proteção do direito à inviolabilidade das comunicações constitui também uma garantia de que tais restrições não estão autorizadas noutras matérias e para outras finalidades. O poder de restrição do legislador encontra-se assim vinculado aos pressupostos e fins predeterminados na norma constitucional que autoriza a restrição. Nesse sentido, refere Vieira de Andrade que «o próprio preceito constitucional que autoriza a restrição pode indicar expressamente os fins ou outros pressupostos específicos da restrição. Será o caso, por exemplo, dos artigos 27.º, n.º 3, 34.º, n.º 4, e 47.º, n.º 1, que podem ser considerados de 'reserva qualificada'. Nestas situações, presume-se que o legislador só está autorizado a *restringir* o conteúdo dos direitos *para essas finalidades*, ou seja, para a salvaguarda dos direitos ou valores enunciados, quando muito para outras finalidades que decorram necessariamente ou se possam considerar implicadas nas expressamente referidas.» (cf. *Direitos Fundamentais na Constituição de 1976*, 5.ª ed., p. 281).

17 — Ao definir o campo de incidência da lei restritiva do direito à inviolabilidade das comunicações pela «matéria de processo criminal» a Constituição ponderou e tomou posição (em parte) sobre o conflito entre os bens jurídicos protegidos por aquele direito fundamental e os valores comunitários, especialmente os da segurança, a cuja realização se dirige o processo penal. Não obstante as restrições legais ao direito à inviolabilidade das comunicações que o legislador está autorizado a estabelecer deverem obedecer à ponderação do princípio da proporcionalidade, a *preferência abstrata* pelo valor da segurança em prejuízo da privacidade das comunicações *só pode valer em matéria de processo penal*. É que a não inclusão de outras matérias do âmbito da restrição do direito à inviolabilidade das comunicações não é contrária ao plano ordenador do sistema jurídico-constitucional. Ainda que se pudesse considerar, em abstrato, que há outras matérias em que o valor da segurança sobreleva os valores próprios do direito à inviolabilidade das comunicações, a falta de cobertura normativa da restrição em matérias extraprocessuais não frustra as intenções ordenadoras do atual sistema, porque há razões político-jurídicas que estão na base da abstenção do legislador constitucional.

Que não estamos perante uma «incompletude contrária ao plano normativo» da Constituição é confirmado, de forma implícita, mas clara, pelas opções valorativas tomadas aquando da 4.ª e da 5.ª revisões constitucionais. Nessas revisões foram abertamente tidos em conta imperativos acrescidos de segurança e a necessidade de incrementar medidas contra a criminalidade referida na alínea *c*) do n.º 2 do artigo 4.º do Decreto n.º 426/XII. Esse objetivo levou a alterações que se traduziram em restrições a direitos fundamentais, nesta área, com a consagração de novos equilíbrios normativos entre os valores aqui em confronto.

Assim, pela 4.ª revisão, o artigo 33.º, n.º 3, passou a prever a extradição de cidadãos portugueses, em condições de reciprocidade estabelecidas em convenção internacional, nos casos de terrorismo e de criminalidade internacional organizada, e desde que a ordem jurídica do Estado requisitante consagre garantias de um processo justo e equitativo. Também o n.º 4 do mesmo artigo passou a admitir a extradição por crimes puníveis com a prisão perpétua (ainda que só mediante a garantia de não aplicação ao caso).

O próprio artigo 34.º foi objeto de reponderação, na 5.ª revisão constitucional, passando a admitir-se, no n.º 3, a entrada durante a noite no domicílio das pessoas, com autorização judicial, «em casos de criminalidade especialmente violenta ou altamente organizada, incluindo o terrorismo e o tráfico de pessoas».

O repensamento desta matéria, nas referidas revisões constitucionais, deixou inalterados os termos da norma permissiva de ingerência nas telecomunicações, estabelecida na 2.ª parte do n.º 4 do artigo 34.º, e o seu alcance restrito a «matéria de processo criminal». Apenas se alargou o âmbito da proibição aos «demais meios de comunicação», na revisão de 1997.

Nada autoriza, pois, a admitir uma eventual extensão do âmbito da ressalva final do n.º 4 do artigo 34.º — para a qual, aliás, o intérprete, neste contexto concreto, não dispõe de instrumentos metodológicos adequados.

De facto, a referência ao processo criminal não é apenas uma indicação teleológica, mas também a localização da restrição à proibição de ingerência numa área estruturada normativamente em termos de oferecer garantias bastantes contra intromissões abusivas. Ao autorizar a ingerência das autoridades públicas nos meios de comunicação apenas em *matéria de processo penal*, e não para quaisquer outros efeitos, a Constituição quis garantir que o acesso a esses meios, para salvaguarda dos valores da «justiça» e da «segurança», fosse efetuado através de um instrumento processual que também proteja os direitos fundamentais das pessoas. Porque a ingerência nas comunicações põe em conflito um direito fundamental com outros direitos ou valores comunitários, considerou-se que a restrição daquele direito só seria autorizada para realização dos valores da justiça, da descoberta da verdade material e restabelecimento da paz jurídica comunitária, os valores que ao processo criminal incumbe realizar. Assim, remeteu para o legislador processual penal a tarefa de «concordância prática» dos valores conflituantes na ingerência nas comunicações privadas: por um lado, a tutela do direito à inviolabilidade das comunicações; por outro, a viabilização da justiça penal. Na verdade, como escreve Figueiredo Dias, «o processo penal é um dos lugares por excelência em que tem de encontrar-se a solução do *conflito* entre as exigências comunitárias e a liberdade de realização da personalidade individual» (cf. *Direito Processual Penal*, Coimbra Editora, 1974, p. 59).

Assim, a referência ao *processo criminal*, encontrando-se estreitamente associada à Constituição, onde se detetam normas diretamente atinentes a essa matéria e que condensam os respetivos princípios estruturantes (artigo 32.º) — a ponto de se falar numa *constituição processual criminal* — , tem um sentido hermenêutico inequívoco, não podendo deixar de ser entendido como a «sequência de atos juridicamente preordenados praticados por pessoas legitimamente autorizadas em ordem à decisão sobre a prática de um crime e as suas consequências jurídicas».

Nesse plano, o artigo 34.º, n.º 4, ao delimitar a restrição à matéria de processo penal tem também outras consequências com reflexo no estatuto constitucional do arguido.

Desde logo, a realização da justiça, não sendo um fim único do processo criminal, apenas pode ser conseguida de modo processualmente válido e admissível e, portanto, com o respeito pelos direitos fundamentais das pessoas que no processo se veem envolvidas. O respeito desses direitos conduz, por exemplo, a considerar inadmissíveis certos métodos de provas e a cominar a nulidade de «todas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações» (cf. artigo 32.º, n.º 8, da CRP). A nulidade das provas, com a consequente impossibilidade da sua valoração no processo, quando sejam obtidas por ingerência abusiva nas comunicações, corresponde assim a uma *garantia do processo criminal* e resulta de ter havido acesso à informação fora dos casos em que a própria Constituição consente a restrição ao princípio da inviolabilidade dos meios de comunicação privada.

Por outro lado, a referência ao processo criminal implica que a intervenção restritiva careça de prévia autorização judicial. Sendo o processo criminal uma forma heterocompositiva através da qual se realizam as funções de *jurisdictio* referidas à atuação de pretensões baseadas em normas públicas de direito criminal, exige-se a intervenção de um órgão qualificado para essas funções (cf. artigo 202.º da CRP). Embora se não trate de um caso em que a reserva do juiz ou a reserva de primeira decisão se encontre especialmente individualizada na Constituição (cf. Acórdãos

n.os 4/06 e 426/2005), como sucede em matéria de privação de liberdade (artigos 27.º, n.º 2, e 28.º, n.º 1), entrada no domicílio sem consentimento do titular (artigo 34.º, n.º 2), inibição do poder paternal (artigo 36.º, n.º 6), liberdade de associação (artigo 46.º, n.º 2) e regularidade e validade dos atos do processo eleitoral (artigo 113.º, n.º 7), não pode deixar de reconhecer-se que a reserva absoluta do juiz tende a afirmar-se quando não existe qualquer razão ou fundamento material para a opção por um procedimento não judicial de resolução de litígio (Gomes Canotilho, *ob. cit.,* p. 663). O que é particularmente evidente quando se trate de questões que se reportam ao *núcleo duro da função jurisdicional*, como é o caso das competências exclusivas do juiz de instrução (artigos 268.º e 269.º do Código de Processo Penal), em que releva a prática de atos que afetam direitos, liberdades e garantias das pessoas (cf. Vieira de Andrade, «Reserva do juiz e intervenção ministerial em matéria de fixação da indemnizações por nacionalizações», *Scientia ivridica,* t. XLVII, n.os 274-276, julho/dezembro, 1998, p. 225). Esse é seguramente o caso quando está em causa a interceção, gravação ou registo de comunicações [artigo 269.º, n.º 1, alínea *c*), do CPP].

Estando excluída a possibilidade, em todo este contexto, de efetuar uma interpretação da norma constitucional que consinta o acesso a dados de tráfego, de localização ou outros dados conexos das comunicações no âmbito das atribuições dos serviços de informações, à revelia de qualquer processo penal ou autorização judicial, ainda que tenha em vista a prevenção penal de bens jurídicos muito relevantes [artigos 4.º, n.º 1, alínea *c*), e 78.º, n.º 2, do Decreto], dificilmente se poderá encarar a ideia de uma ampliação do âmbito da restrição contida no artigo 34.º, n.º 4, 2.ª parte, a partir do fim da regulação ou da conexão de sentido da norma. Desde logo, porque a finalidade do preceito, como assinalou o Acórdão do Tribunal Constitucional n.º 241/2002, é a de *delimitar* o âmbito das restrições à garantia da inviolabilidade das comunicações. E, como se deixou exposto, essa delimitação é expressamente assumida pela Constituição como sendo apenas reconduzível às situações enquadradas pelo processo penal. Não há aqui, por isso, uma qualquer lacuna oculta que justifique, contra o seu sentido literal, uma interpretação conforme com a teleologia imanente da norma, já que ela própria tem por objetivo definir o âmbito preciso da restrição, sem que se torne possível estabelecer uma identidade valorativa entre o processo penal e a investigação levada a efeito pelos serviços de informações. Além de que o alargamento do âmbito da norma constitucional, a ser admitida, teria um duplo sentido, implicando não apenas uma ampliação do âmbito aplicativo da restrição ao princípio da não ingerência nas comunicações mas também uma redução da garantia de reserva de juiz, através da remissão do controlo de atos que afetam direitos fundamentais para uma entidade meramente administrativa.

Pode, então, concluir-se que, no caso da proibição de ingerência das autoridades públicas nas comunicações, que o artigo 34.º, n.º 4, primeira parte, consagra como princípio geral, as *exceções* a que se refere o segmento final desse preceito estão condicionadas à *matéria de processo penal*, e sendo a restrição constitucionalmente autorizada apenas nesses termos, não tem cabimento efetuar uma qualquer outra interpretação que permita alargar a restrição a *outros efeitos*, como se a restrição não estivesse especificada no próprio texto constitucional ou se tratasse aí de uma restrição meramente implícita que permitisse atender a outros valores ou bens constitucionalmente reconhecidos.

18 — Este tem sido o entendimento constante, quer da jurisprudência do Tribunal Constitucional, quer da doutrina que se pronunciou sobre o sentido jurídico-normativo do n.º 4 do artigo 34.º da CRP.

A jurisprudência do Tribunal Constitucional tem considerado que a «compressão» da proibição da ingerência nas comunicações só pode ser feita nos termos da lei e em «matéria de processo criminal».

Enquanto critério normativo da solução de um concreto problema jurídico, o n.º 4 do artigo 34.º da CRP foi objeto de interpretação no já referido Acórdão n.º 241/02, em que conheceu da inconstitucionalidade da norma ínsita no artigo 519.º, n.º 3, alínea *b*), do CPC quando interpretada no sentido de que, em processo laboral, podem ser pedidas, por despacho judicial, aos operadores de telecomunicações informações relativas aos dados de tráfego e à faturação detalhada de linha telefónica instalada na morada de uma parte, sem que enferme de nulidade a prova obtida com a utilização dos documentos que veiculam aquelas informações, por infração ao disposto nos artigos 26.º, n.º 1, e 34.º, n.os 1 e 4, da Constituição. Aí se reconheceu que «a garantia da inviolabilidade das telecomunicações não é, na Constituição, absoluta — ela admite a ressalva de 'casos previstos na lei' (n.º 4 do citado artigo 34.º). Simplesmente, a Constituição teve o cuidado de delimitar o âmbito em que esses casos se poderiam inscrever — 'em matéria de processo criminal'.». Sendo esse o critério normativo oferecido pelo preceito constitucional, então, «o âmbito da restrição ao princípio da não ingerência nas telecomunicações está constitucionalmente delimitado, não sendo lícito, a pretexto de concordância com aquele interesse (interesse público da administração da justiça), também constitucionalmente consagrado, ampliar a restrição consentida». Nessa ordem de razão, afirmou-se, expressivamente, que «é certo que se poderia contrapor ao sigilo das telecomunicações [...] o interesse público na administração da justiça, em ordem ao qual se verteu em lei o dever de cooperação das partes e de terceiros para a descoberta da verdade. O certo é que, como se viu, o âmbito da restrição ao princípio da não ingerência nas telecomunicações está constitucionalmente delimitado, não sendo lícito, a pretexto de concordância com aquele interesse, também constitucionalmente consagrado, ampliar a restrição consentida.».

E no Acórdão n.º 198/85, em que se questionou a constitucionalidade do artigo 1216.º do Código de Processo Civil — que prescrevia que toda a correspondência dirigida ao falido era entregue ao administrador — por desconformidade com o n.º 4 do artigo 34.º, na versão originária, o Tribunal entendeu que nessa disposição «apenas se prevê a possibilidade de restrições legais ao sigilo da correspondência 'em matéria de processo criminal', e a restrição ora em causa não tem aí, a todas as luzes, a sua sede — não é, por outras palavras, ditada por um objetivo de investigação e perseguição criminal». E ao comparar a restrição prevista na norma sindicada com o estabelecido nas Leis de Falências italiana e alemã, refere que «em ambos os mencionados ordenamentos a consagração legal da restrição ou restrições em causa depara com menores dificuldades do que entre nós, uma vez que em qualquer deles o respetivo preceito constitucional ressalva, genericamente, as limitações ao direito impostas 'por ato fundamentado da autoridade judiciária, observadas as garantias estabelecidas

pela lei' (Constituição Italiana), ou as limitações impostas 'com base numa lei' (*Grundgesetz*)». Na nossa ordem jurídica, a dificuldade em aceitar a restrição ao sigilo da correspondência existe porque «não é uma fórmula ampla e genérica deste tipo a que se contém no artigo 34.º, n.º 4, da Constituição Portuguesa — mas antes, como se viu, uma fórmula que unicamente prevê restrições (legais) do direito em apreço 'em matéria de processo criminal'».

De igual modo, nos Acórdãos n.os 407/97, 70/2008, 486/2009 e 699/2013 agora em matéria de sigilo de telecomunicações, se considera que a possibilidade de existir ingerência nas telecomunicações só ocorre «no quadro de uma previsão legal atinente ao processo penal (a única constitucionalmente tolerada)»; que «só no domínio do processo penal é que a lei ordinária pode prever restrições à referida garantia contida no artigo 34.º, n.º 4. As necessidades de perseguição penal e de obtenção de provas justificam a compressão do direito individual à comunicação reservada, mas carecem de ser avaliadas pelas autoridades judiciárias em termos de necessidade, adequação e proporcionalidade, de tal modo que violado que seja o princípio da menor intervenção possível e da proporcionalidade, há de a prova assim obtida ser considerada nula (artigos 32.º, n.º 8, da Constituição e 189.º do Código de Processo Penal)»; e que «a proibição de obtenção de meios de prova mediante intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações pode ser afastada, quer pelo acordo do titular dos direitos em causa, quer pelas restrições à inviolabilidade desses direitos expressamente autorizadas pela Constituição. O legislador constitucional prevê expressamente restrições ao sigilo das telecomunicações mas apenas as admite no domínio da lei processual penal».

Assim, o Tribunal Constitucional tem considerado que, para além da permissão de restrições expressamente previstas no n.º 4, referente ao processo criminal, vigora uma proibição absoluta de ingerência das autoridades públicas nos meios de comunicação, incluindo em matéria de dados de tráfego.

E no mesmo sentido se pronunciou o Conselho Consultivo da Procuradoria-Geral da República em quatro Pareceres sobre o sigilo das telecomunicações: (*i*) no *Parecer n.º 92/91*, de 30/3/92, a propósito da questão de saber se a expressão «em matéria de processo criminal», usada no artigo 34.º, n.º 4, da CRP, poderia abranger processos de prevenção criminal, designadamente na área da segurança, concluiu que «a obtenção de prova por meio de escutas telefónicas ou similares só é suscetível de ser judicialmente autorizada a partir do início da fase processual de inquérito», o qual «tem de iniciar-se logo que haja aquisição da notícia da existência de uma infração criminal idónea à formulação de um juízo objetivo de suspeita sobre a sua verificação»; (*ii*) No *Parecer n.º 16/94, de 24/6/94* e *Parecer n.º 16/1994, Complementar*, *de 26/10/1995*, concluiu que «o sigilo das comunicações é tendencialmente absoluto, cedendo apenas nos termos e pelo modo previstos no Código de Processo Penal como meio de aquisição da prova»; (*iv*) e no Parecer n.º 16/2000, de 9/3/2000, pronunciou-se no sentido de que «no âmbito de processos de natureza cível, sendo solicitadas, por parte do juiz da causa, para efeitos de instrução, informações referentes a dados de tráfego e dados de conteúdo, é legítima a recusa, por parte dos operadores de telecomunicações».

Por fim, cabe referir que ao mesmo resultado de interpretação tem chegado a doutrina que se pronunciou sobre o texto e a intenção prático-normativa das normas alojadas no n.º 4 do artigo 34.º da CRP. Gomes Canotilho e Vital Moreira afirmam que do teor desse artigo resulta que nele se «inclui a proibição de ingerência nos meios de comunicação, salvo nos casos previstos na lei (reserva de lei) em matéria de processo penal (e não para outros efeitos)». (cf. *ob. cit.,* p. 543); Cristina Máximo dos Santos refere que o direito ao sigilo das telecomunicações não é absoluto, pois admite exceções previstas na «lei em matéria de processo criminal» «o que vale por dizer que, apenas em processos de natureza penal, se admite a ingerência nas telecomunicações, cabendo à lei ordinária definir os limites em que ela pode ter lugar» (cf. «As novas tecnologias da informação e o sigilo das telecomunicações», *Revista do Ministério Público,* n.º 99, p. 96); Rui Pereira, precisamente a propósito das competências dos Serviços de Informação da República, afirma que «há limites à atividade dos serviços que decorrem da Constituição. Assim, as 'escutas telefónicas' — ou, mais rigorosamente, a ingerência [...] na correspondência, nas telecomunicações e nos demais meios de comunicação... — apenas podem ser levadas a cabo no âmbito do processo penal e carecem sempre se mandado de juiz por se 'prenderem diretamente' com direitos fundamentais» (cf. «Informações e Investigação Criminal», *I Colóquio de Segurança Interna,* Instituto Superior de Ciências Policiais e Segurança Interna, Almedina, p. 161).

19 — Resta, pois, saber se a atividade dos oficiais de informações do SIRP, para efeitos da qual acedem, nos termos da norma em análise, a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, data, hora, duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização, se pode considerar como atividade «em matéria de processo criminal».

Tudo está em saber, a final, se o acesso aos dados de tráfego é um ato que se inclui no âmbito da investigação criminal.

Seguramente que a resposta deve ser negativa.

Na verdade, os fins e interesses que a lei incumbe ao SIRP de prosseguir, os poderes funcionais que confere ao seu pessoal e os procedimentos de atuação e de controlo que estabelece, colocam o acesso aos dados de tráfego fora do âmbito da investigação criminal.

A remissão que o n.º 2 do artigo 78.º do Decreto n.º 426/XII faz para a alínea *c*) do n.º 2 do artigo 4.º, que descreve as atribuições do SIRP, indica a finalidade do acesso aos dados de tráfego: recolha, processamento, exploração e difusão de *informações adequadas a previr* a sabotagem, a espionagem, o terrorismo, a criminalidade altamente organizada de natureza transnacional e a prática de atos que possam alterar ou destruir o Estado de Direito democrático.

Ora, a caracterização dessa concreta atividade como recolha de «informações» para efeitos de «prevenção» dissocia-a, de forma clara e precisa, da atividade própria de investigação criminal. A investigação criminal, di-lo a própria lei — artigo 1.º da Lei n.º 49/2008, de 27 de agosto — «compreende o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo». E mesmo a circunstância de os

dados de tráfego se reconduzirem a crimes tipificados no ordenamento jurídico-penal não permite que se caracterize a «recolha de informação» como um ato de «recolha de provas» ou que a «ação preventiva» configure uma «atividade processual».

Não obstante existir uma relação entre informações e investigação criminal, o legislador teve a preocupação de distinguir, em sentido material e orgânico, as duas atividades. Com efeito, a atividade do SIRP de «produção de informações necessárias à salvaguarda da segurança interna e externa, da independência e interesses nacionais e da unidade e integridade do Estado», prescrita no artigo 2.º do Decreto n.º 426/XII, não inclui o exercício de poderes, atos e atividades, «do âmbito da competência específica dos tribunais, do Ministério Público ou das entidades com funções policiais», conforme se preceitua no n.º 2 do artigo 5.º do mesmo Decreto. Por conseguinte, os serviços de informação não possuem quaisquer atribuições policiais ou de investigação criminal, ou seja, não se destinam a garantir o respeito e cumprimento das leis gerais (v. g. defesa da ordem pública), nem a apurar da autoria da prática de crimes, estando-lhes legalmente vedada tais atividades; nem são órgãos de polícia criminal para efeitos do Código de Processo Penal, nem assumem a qualidade de autoridade de polícia.

Há, pois, uma distinção radical entre informações e investigação criminal, o que impede os oficiais de informação de intervirem no processo penal. As *informações*, no sentido de «elementos de conhecimento sistematizado em quadros interpretativos, através de critérios que sobrepõem a estrutura de sentido à relação causal [...] produzidas através de método próprio e preservadas da atenção e conhecimento de terceiros», nisso se traduzindo os «dois traços distintivos essenciais: — um método próprio; — um regime de segredo» (cf. Arménio Marques Ferreira, «O Sistema de Informações da República Portuguesa», in *Estudos de Direito e Segurança,* Almedina, 2007, p. 69), visam a obtenção de um conhecimento específico necessário à tomada de decisões e não a recolha de prova conducente ao exercício da ação penal. Ainda que a recolha e análise de informações possa ser utilizada na investigação criminal e com vista a medidas de prevenção policiais, não deixa de ser uma atividade autónoma e prévia à investigação criminal.

De facto, iniciando-se o processo penal com a *notitia criminis*, a recolha de informações para esse fim tem de se dirigir a um crime já praticado. De modo que a recolha de dados no âmbito de processo criminal é sempre feita num contexto *previamente delimitado* pelo objeto desse processo, apenas se recolhendo informações no contexto da investigação de um *específico facto* e em relação a *específicos sujeitos* tidos como suspeitos.

Diferente é a configuração da atuação «preventiva» dos serviços de informações, à qual corresponderá um acesso aos dados que pode abranger um universo de pessoas muito mais vasto, precisamente por não estar ainda preordenado à investigação de um facto concreto e delimitado. As funções de recolha e tratamento de informações a levar a cabo pelo SIRP, porque preventivas, não se orientam para uma atividade investigatória de crimes praticados ou em execução. Não são atos de polícia judiciária, destinada à investigação criminal.

É evidente que uma atuação investigatória processualizada e publicizada, na forma de *inquérito preliminar* ou de *instrução,* não só salvaguarda a liberdade e segurança no decurso do processo como dá garantia de que a prova para ele canalizada foi obtida com respeito pelos direitos fundamentais. A mesma conclusão não se pode extrair de uma *ação de prevenção* não processualizada ou mesmo não suficientemente formalizada, coberta pelo segredo de Estado, que decorre na total ausência de instrumentos defensivos que comportem um mínimo de dialética processual. Os procedimentos preventivos dessa natureza, desvinculados da dependência funcional a uma autoridade judiciária, não fazem parte da investigação criminal. A Lei Fundamental enquadra essas ações no direito constitucional da polícia — artigo 272.º —, não como atividade auxiliar da realização da justiça mas apenas como «medidas de polícia» de caráter preventivo. A atividade relativa à produção de informações pelo SIRP destinadas a previr os crimes contra a segurança do Estado, soberania nacional e realização do Estado de Direito, pode ser abrangida por esse preceito (cf. Jorge Miranda e Rui Medeiros, *ob. cit.,* pp. 663 e 664), mas, porque não se dirige à descoberta da autoria de um crime, não reveste a natureza de investigação criminal. As ações de prevenção do SIRP são, pois, *procedimentos administrativos* que, devendo respeitar os direitos, liberdades e garantias (artigo 5.º do Decreto n.º 426/XII), não obedecem aos princípios jurídico-constitucionais conformadores do processo penal, proclamados no artigo 32.º da CRP.

20 — E não é a intervenção da *Comissão de Controlo Prévio* que tem a virtualidade de judicializar o acesso aos dados de tráfego. A titularidade do processo penal é atribuída às *autoridades judiciárias* competentes — Ministério Público, juiz de instrução criminal e juiz de julgamento [cf. alínea *b*) do artigo 1.º do CPP] e aquela Comissão tem a natureza de *órgão administrativo* não inserido jurídico normativamente na organização judicial, pese embora a qualidade dos seus membros. De facto, do ponto de vista formal ou orgânico, não exerce a *função judicial* e, do ponto de vista material, não exerce a *função jurisdicional*. Em questões do foro criminal é sempre inadmissível qualquer procedimento administrativo prévio, por mor das «exigências» do *ius puniendi*: exclusividade pelos tribunais e exclusividade processual (cf. artigos 202.º e 32.º da CRP). Ou seja, cumpre aos juízes e tribunais declarar o crime e determinar a pena proporcional aplicável, e tal atividade deve ocorrer no âmbito de um processo penal válido e com todas as garantias constitucionalmente estabelecidas.

Ora, é precisamente a falta de intervenção de uma entidade judicial, exigida pelo artigo 32.º, n.º 4, da CRP no que se refere à intervenção nos direitos e liberdades das pessoas, que demonstra não se poder configurar a atuação de acesso aos dados de comunicações privadas por parte dos oficiais dos serviços de informação como integrando um «processo criminal». É certo que, nos termos do artigo 35.º do Decreto n.º 426/XII, a Comissão de Controlo Prévio é composta por três magistrados judiciais, designados pelo Conselho Superior da Magistratura, de entre juízes conselheiros do Supremo Tribunal de Justiça, com pelo menos três anos de serviço nessa qualidade. No entanto, e independentemente da sua concreta composição, a Comissão de Controlo Prévio configura um *órgão administrativo* e neste ponto é irrelevante saber se é composta por magistrados judiciais, já que os mesmos atuam, não na veste de entidade judicial, mas como membros da referida comissão administrativa. De facto, não é específica atividade profissional dos membros que compõem um determinado órgão

que muda a natureza do mesmo, transformando-o de órgão administrativo em órgão judicial.

Nem o sistema de autorização prévia dada pela referida Comissão para acesso e manutenção dos dados de tráfego se poderia equiparar ao controlo existente num processo penal. De facto, este último, no que toca ao acesso aos presentes dados, assegura garantias não só no que respeita ao acesso mas ainda no que toca ao tratamento, manutenção e destruição ou cancelamento dos mesmos, definindo inclusivamente prazos máximos perentórios para o efeito. Neste contexto, vigoram as garantias do Código de Processo Penal e da já mencionada Lei n.º 32/2008 que, depois de especificar, no artigo 2.º, n.º 1, alínea *f*), quais as autoridades competentes para acederem aos dados de tráfego das comunicações (no qual não consta qualquer serviço de informações), estabelece várias garantias no que toca ao tratamento e conservação de todos esses dados, sendo nota comum a todo o acesso, tratamento, conservação e extinção a intervenção de um juiz (assim, artigos 7.º e 9.º e artigo 11.º, que estabelece sobre destruição de dados). Todavia, esta intensidade de controlo não é levada a cabo pela referida Comissão de Controlo Prévio, que se limita a conceder um «visto» prévio de autorização, após o que deixa de ter qualquer intervenção durante as atividades de acesso aos dados em causa.

21 — Aliás, independentemente da questão da reserva de juiz em processo penal, a falta das mencionadas garantias verifica-se ainda no que toca à *atuação* da referida Comissão de Controlo Prévio. De facto, da lei não resulta com suficiente determinação quais os *casos* ou *circunstâncias* em que a referida Comissão pode conceder a autorização de acesso aos dados, nem se estabelece com clareza quais as garantias dos visados no que toca à *duração* da autorização de acesso ou à *eliminação* dos dados.

Ora, uma atividade de acesso aos dados de tráfego, levada a cabo sem conhecimento dos visados, exige regras claras e determinadas que permitam saber até onde pode ir a ingerência, para que haja a necessária segurança jurídica no que toca às restrições possíveis aos seus direitos. De facto, onde a atividade e poderes são exercidos em segredo, maior é o risco de arbitrariedade, já que os indivíduos não têm conhecimento nem controlam a atividade de ingerência em concreto.

A esse propósito, o Tribunal Europeu dos Direitos do Homem já afirmou que um processo de acesso a dados, porque não sujeito ao escrutínio dos indivíduos visados, tem de ser compensado por uma lei suficientemente tuteladora dos direitos fundamentais (Acórdão de 06/06/2006, *Segerstedt-Wiberg e outros c. Suécia*, queixa n.º 62332/2000); que essa lei deve empregar termos suficientemente claros para possibilitar a todos os cidadãos terem conhecimento das circunstâncias e dos requisitos que permitem ao poder público fazer uso de uma medida secreta que lesa o direito à vida privada pessoal e familiar e à correspondência (Acórdão de 02/08/1984, *Malone c. Reino Unido*, queixa n.º 8691/79); que seria contrária às exigências do artigo 8.º, n.º 2, da CEDH se a ingerência nas telecomunicações fosse conferida aos poderes públicos através de um poder amplo e discricionário, e que são necessárias regras claras e detalhadas, especialmente devido ao facto de a tecnologia disponível se tornar cada vez mais sofisticada, a fim de garantir uma proteção adequada contra ingerências arbitrárias (Acórdão de 16/02/2000, *Amann c. Suíça* 95, queixa n.º 27798/95); e nos casos *Valenzuela c. Espanha* (Acórdão de 30/07/1998, queixa n.º 27671/95) e *Prado Bugallo c. Espanha* (Acórdão de 18/02/2003, queixa n.º 58496/00), chegou à mesma conclusão, afirmando que a lei que permitia a ingerência nas comunicações não era suficientemente clara e precisa, não mencionando a natureza das infrações que podem dar lugar às mesmas, a fixação de um limite de duração da medida, as condições de acesso aos dados e a eliminação dos mesmos.

E a jurisprudência constitucional estrangeira orienta-se no mesmo sentido. O Tribunal Constitucional espanhol afirmou já, por diversas vezes, que a ingerência nas comunicações telefónicas só pode considerar-se constitucionalmente legítima quando esteja prevista na lei com *suficiente grau de precisão* (Decisão n.º 49/99, de 5 de abril, Decisão n.º 184/2003, de 23 de outubro); e o Tribunal Constitucional alemão, em relação a uma lei que não regulava como deveriam os dados ser guardados nem oferecia garantia de uma efetiva supervisão, decidiu que, no âmbito da realização de uma base de dados partilhada entre o serviço de inteligência e vários serviços de segurança, com o objetivo de combater o terrorismo, a partilha ou transferência de informação estava sujeita a requisitos constitucionais muito exigentes, dos quais se destacava a sua detalhada configuração legal (Decisão de 24/04/2013, 1.º Senado).

Desta jurisprudência decorrem, pois, várias exigências para uma norma que, como a presente, permita o acesso a dados de tráfego das comunicações de indivíduos sem o seu consentimento ou conhecimento. Em primeiro lugar, a lei deve empregar *termos suficientemente claros* para possibilitar a todos os cidadãos terem conhecimento das circunstâncias e dos requisitos que permitem ao poder público aceder aos dados em causa, sendo que os requisitos para o efeito devem ser claramente determinados; deve ainda fazer menção, com precisão, dos *casos específicos* em que o acesso deve ter lugar, prever a fixação de um *limite de duração* da medida, e das regras e prazos para eliminação dos dados de tráfego. Só assim se poderá falar de uma ingerência determinável e que garanta segurança jurídica aos interessados.

22 — Mas, se assim é, há que reconhecer que, para além da impossibilidade de compatibilização com a norma do n.º 4 do artigo 34.º da CRP, a norma do n.º 2 do artigo 78.º do Decreto n.º 426/XII não contém *densidade suficiente* para, num domínio de lei restritiva, possibilitar a fiscalização da legalidade e a defesa dos direitos e interesses dos cidadãos. Com efeito, a norma não satisfaz suficientemente, como contrapartida do acesso aos dados de tráfego, as exigências de determinabilidade que são garantidas em matéria de processo criminal, devolvendo para a esfera administrativa ponderações que deveriam constar da lei.

Desde logo, e quanto aos *pressupostos* da concessão da autorização de acesso aos dados, a lei estabelece que o acesso aos dados de tráfego de comunicações tem lugar *nos casos* previstos na alínea *c*) do n.º 2 do artigo 4.º, que respeitam à *prevenção* de sabotagem, espionagem, terrorismo e sua proliferação, a criminalidade altamente organizada de natureza transnacional e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido. Mas a parte final da norma não oferece suficiente segurança jurídica aos potenciais lesados, já que resulta indeterminado o que podem constituir «atos que, pela sua natureza, possam alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido». Assim, não se pode considerar que a lei tenha determinado de forma suficientemente precisa

os casos em que a ingerência possa ter lugar. Trata-se, aliás, de uma verdadeira *indeterminabilidade*, que pode ser facilmente manipulável para permitir um acesso arbitrário aos dados de tráfego das comunicações.

Depois, porque delimita *as condições* em que o acesso a dados de tráfego pode ter lugar por parte dos oficiais de informações do SIRP da seguinte forma: «sempre que sejam necessários, adequados e proporcionais, numa sociedade democrática, para o cumprimento das atribuições legais dos serviços de informações». Ora, a referência às exigências de necessidade, adequação e proporcionalidade em sentido estrito, quando reportada à atuação dos oficiais de informações em matéria de dados e informações, não representa mais do que um afloramento de um parâmetro de juridicidade da Administração, tal como se encontra genericamente consagrado no artigo 266.º, n.º 2, da Constituição, e é, nesse plano, inteiramente redundante na medida em que se trata de um princípio material conformador de toda e qualquer atividade administrativa.

E, sendo assim, a alusão ao princípio da proporcionalidade nos sobreditos termos nada esclarece quanto às condições específicas em que, no âmbito das atribuições dos serviços de informações, pode haver lugar ao acesso a dados conexos com as comunicações.

Note-se que, em contrapartida, a Lei n.º 32/2008, que não se aplica aos sistemas de informação, estabelece requisitos muito mais precisos para o acesso à informação em contexto de processo penal, ao prever, no artigo 9.º, n.º 1, que «a transmissão dos dados referentes às categorias previstas no artigo 4.º só pode ser autorizada [...] 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 no âmbito da investigação, deteção e repressão de crimes graves». Assim, no artigo 78.º do Decreto, para além de os *casos* que permitem o acesso aos dados de tráfego não resultarem suficientemente determinados, o mesmo se pode dizer das *condições* de acesso, já que dele não resulta quais os critérios a que se deve atender para aferir se a ingerência estadual, num determinado caso, é «necessária, adequada e proporcional, numa sociedade democrática».

Por outro lado, e ainda quanto às situações de facto cuja ocorrência depende a possibilidade legal de intervenção da Comissão de Controlo Prévio, a norma objeto de fiscalização, em conjugação com a alínea *c*) do n.º 2 do artigo 37.º do Decreto, não impede que se autorize a recolha e análise de informação sem referência a alvos concretos. Muito pelo contrário, ele deixa espaço para que o acesso a dados seja feito de forma bastante alargada de modo a detetar padrões de conduta que possam reconduzir os cidadãos a potenciais suspeitos de crime. Muito diversas são as garantias atualmente previstas no contexto do processo penal, em que a Lei n.º 32/2008 estabelece, no artigo 9.º, n.º 3, que só pode ser autorizada a transmissão de dados relativos ao suspeito ou arguido, a pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido, ou a vítima de crime, mediante o respetivo consentimento, efetivo ou presumido. Assim, a lei sobre transmissão de dados atualmente em vigor em matéria criminal exige uma determinabilidade dos dados acessíveis que não tem qualquer correspondência com as latas menções constantes do Decreto. E isto porque a utilização de um meio invasivo nos direitos fundamentais que aqui estão em causa dependerá sempre da verificação de uma suspeita substanciada segundo limiares de plausibilidade ou de probabilidade.

23 — Acresce, por fim, que a norma do n.º 2 do artigo 78.º, no contexto jurídico-sistemático em que está inserida, não torna claro e explícito todo o *procedimento de acesso*, a *duração do acesso* e a *eliminação* dos dados de tráfego recolhidos.

De facto, daquela norma, nem de qualquer outra do Decreto, resulta c*omo é feito o acesso aos dados*. Mais uma vez se impõe o contraponto com a Lei n.º 32/2008, que determina, no n.º 3 do artigo 7.º, como é feita a transmissão de dados por parte das operadoras no contexto do processo penal: «processa-se mediante comunicação eletrónica, nos termos das condições técnicas e de segurança fixadas em portaria conjunta dos membros do Governo responsáveis pelas áreas da administração interna, da justiça e das comunicações, que devem observar um grau de codificação e proteção o mais elevado possível, de acordo com o estado da técnica ao momento da transmissão, incluindo métodos de codificação, encriptação ou outros adequados». Ora, o Decreto n.º 426/XII nada menciona no que toca à forma de comunicação dos dados, nem remete esta matéria para qualquer outra regulamentação.

E quanto ao tempo durante o qual é permitido o acesso aos dados, verifica-se a mesma falta de segurança jurídica. Nos termos do artigo 37.º, n.º 2, alínea *d*), do Decreto, o prazo de acesso não pode exceder três meses, mas pode ser estendido, mediante autorização expressa. Porém, a lei não contém qualquer limite para tal prorrogação, nem estabelece em que condições pode ser autorizada a referida prorrogação. A lei prevê assim, a partir do momento em que a Comissão de Controlo Prévio dá a sua autorização, uma possibilidade de acesso aos dados de tráfego sem qualquer limite máximo de tempo. Assim, tal como decidiu o TEDH no caso *Valenzuela c. Espanha*, acima referido, a falta de menção de prazo específico de duração da medida gera incerteza para os destinatários da mesma, pelo que não se pode considerar, também por aqui, que a lei cumpra a exigência de determinabilidade.

Idêntica incerteza pode apontar-se no que respeita à *eliminação dos dados* — que corresponderia, aliás, a uma exigência do direito à autodeterminação comunicativa, na vertente do «direito ao esquecimento». No Decreto n.º 426/XII não se especifica qualquer prazo para a manutenção ou eliminação obrigatória dos dados. De resto, são escassas e incertas as possibilidades previstas referentes à eliminação dos dados. O artigo 37.º, n.º 8, prevê a possibilidade de a Comissão de Controlo Prévio, em coletivo, participar à Comissão de Fiscalização «os elementos conducentes à destruição imediata desses dados ou informações». Todavia, sem a previsão legal de um acompanhamento constante por essa Comissão, fica por saber como chega ao seu conhecimento a existência de dados que devem ser eliminados. Por seu turno, o Secretário-Geral tem poderes para ordenar a destruição imediata de todos os dados e informações recolhidos mediante a autorização prevista no presente artigo, «sempre que não tenham relação com o objeto ou finalidades da mesma» (artigo 37.º, n.º 7). Assim, na prática, a fiscalização da manutenção de dados é apenas levada a cabo pela Comissão de Fiscalização do SIRP, que, em regra, exerce a sua atividade fiscalizadora dos centros de dados *por amostragem* (artigo 30.º, n.º 1). A única norma que se refere a um «dever» de eliminação de dados consta do artigo 30.º, n.º 3, de acordo com a qual a referida Comissão de Fiscalização «deve ordenar o cancelamento

ou retificação de dados recolhidos que envolvam violação dos direitos, liberdades e garantias consignados na Constituição e na lei». Não se estipula, porém, em que condições ou em que prazos tem lugar uma fiscalização conducente a esta avaliação e correspondente destruição dos dados. No mais, qualquer possibilidade de eliminação ou destruição de dados estará sempre dependente do conhecimento e pedido dos visados, nos termos do artigo 32.º Ora, a falta de prazos perentórios de eliminação de dados, ou de procedimentos periódicos obrigatórios destinados a averiguar a necessidade de manutenção de todos os dados existentes, bem como de clara determinação do momento ou condições em que a manutenção dos dados deixa de ser necessária, também não oferece suficiente segurança à defesa dos direitos e interesses dos cidadãos.

24 — De todo o exposto resulta, assim, que, independentemente da natureza específica do órgão «Comissão de Controlo Prévio», a atuação do mesmo não se afigura equiparável ao controlo jurisdicional existente em processo penal em matéria de direitos fundamentais. De facto, este último, no que toca à ingerência nas comunicações, assegura garantias não só no que respeita ao acesso mas ainda no que toca ao tratamento, manutenção e destruição ou cancelamento dos dados, definindo inclusivamente prazos máximos perentórios para o efeito. Neste contexto, vigoram as garantias do Código de Processo Penal e da Lei n.º 32/2008, que estabelece várias garantias no que toca ao tratamento e conservação de todos esses dados, sendo nota comum a todo o acesso, tratamento, conservação e extinção a intervenção de um juiz (cf. artigos 7.º, 9.º e 11.º). Esta intensidade de controlo não é levada a cabo pela referida Comissão de Controlo Prévio, que se limita a conceder um «visto» prévio de autorização, após o que não exerce qualquer acompanhamento durante as atividades de acesso aos dados em causa. Neste ponto se vê, pois, também que a institucionalização do controlo prévio mencionado em nada se pode considerar equiparável ao oferecido em matéria de processo penal.

Enfim, importa reconhecer que a ingerência nos dados de comunicação não tem, no presente contexto, lugar num procedimento que dê garantias e faculdades de proteção de alcance assimilável àquelas que conformam constitucionalmente o processo criminal. Assim, as razões que justificaram a exceção expressamente mencionada no n.º 4 do artigo 34.º da CRP, que se prendiam, precisamente, com as específicas garantias existentes em processo criminal, não se verificam no presente caso.

Por conseguinte, também a resposta à segunda questão que foi colocada pelo Requerente neste processo é seguramente negativa: a Comissão Prévia de Controlo é um órgão administrativo que não tem poderes equivalentes a uma intervenção em processo criminal.

III — *Decisão*. — Pelo exposto, ao abrigo do artigo 278.º da Constituição da República, o Tribunal decide pronunciar-se pela inconstitucionalidade da norma do n.º 2 do artigo 78.º do Decreto n.º 426/XII da Assembleia da República que «Aprova o Regime Jurídico do Sistema de Informações da República Portuguesa», por violação do n.º 4 do artigo 34.º da CRP.

Lisboa, 27 de agosto de 2015. — *Lino Rodrigues Ribeiro — Fernando Vaz Ventura — Carlos Fernandes Cadilha — Ana Guerra Martins — Maria Lúcia Amaral* (com declaração) — *Teles Pereira* (votei vencido conforme declaração junta) — *Joaquim de Sousa Ribeiro.*

Declaração de voto

Votei a decisão. Não subscrevo, no entanto, os fundamentos que a sustentaram e que foram sufragados pela maioria.

1 — O juízo de inconstitucionalidade que o Tribunal faz, no presente caso, decorre de uma operação de interpretação constitucional que conduz ao seguinte resultado: em Portugal, diz-se, a CRP *proíbe* em qualquer circunstância que os Serviços de Informação da República acedam aos dados de tráfego das telecomunicações privadas, uma vez que o direito fundamental à inviolabilidade destas últimas só pode ser restringido através da lei em matéria de processo criminal. De acordo, portanto, com esta interpretação, *extra delictum* — fora de um processo [criminal] já iniciado contra alguém em tribunal e para além das suas garantias — as autoridades públicas portuguesas não estarão pura e simplesmente autorizadas a intercetar dados de tráfego telecomunicacional, quaisquer que sejam os fundamentos constitucionais que sustentem a necessidade da interceção ou qualquer que seja *o valor comunitário* pela mesma prosseguido.

A razão de ser desta interpretação reside na redação literal do n.º 4 do artigo 34.º da CRP, particularmente no seu inciso final. Por causa deste inciso, deve entender-se (diz ainda o Tribunal) que, ocorrendo *in casu* uma «tensão» ou «colisão» entre dois valores constitucionais de primeiríssima grandeza — a liberdade individual, por um lado, expressa no direito à inviolabilidade das telecomunicações, e, por outro, a segurança e preservação da própria ordem constitucional, expressa na necessidade de prevenir a ocorrência de atos que contra ela atentem —, a resposta à questão de saber em que *termos* é que essa «tensão» ou «colisão» deve ser constitucionalmente resolvida não é tarefa que caiba ao intérprete empreender, uma vez que foi o próprio legislador constituinte que conferiu para ela uma solução clara. E essa é a da «reserva absoluta» do processo criminal, porque assim o determina a parte final do n.º 4 do artigo 34.º da CRP. Nestes termos, e a menos que haja uma revisão constitucional contendo para tanto uma explícita autorização, os Serviços de Informações da República, que se situam claramente fora do âmbito do poder judicial e que atuam por outros meios que não os próprios de um processo que corra em juízo, não podem, em caso algum, intercetar os chamados *dados de tráfego.*

Dissenti desta interpretação. A meu ver, na sua base está um entendimento do que seja o limite previsto no n.º 2 do artigo 18.º da CRP («[a] lei só pode restringir os direitos, liberdades e garantias *nos casos expressamente previstos na Constituição*») de tal modo estreito que não serve para resolver questões em que, como no presente caso, estejam em causa problemas difíceis de «colisão» entre diferentes direitos fundamentais (o direito à liberdade e o direito à segurança), ou — vistas as coisas de uma perspetiva objetiva e não apenas subjetiva — entre diferentes valores constitucionais dotados ambos da mais intensa carga axiológica: o valor da liberdade, por um lado, e o valor da defesa da ordem constitucional democrática, por outro.

2 — Na verdade, e subjacente ao entendimento que foi adotado — segundo o qual os Serviços de Informações da República se situam claramente *fora* da autorização constitucional que é dada ao legislador para restringir o direito à inviolabilidade das telecomunicações — está a convicção segundo a qual a remissão que é feita para a lei restritiva, quer a que consta do n.º 4 do artigo 34.º da CRP quer a que conste de qualquer outro preceito da lei

fundamental, é sempre uma «exceção» a uma «norma» ou «regra». De acordo com este entendimento, a «norma» ou a «regra» é o direito fundamental em si mesmo considerado; e a «exceção», a autorização constitucional para o restringir. E como, em termos lógicos, a exceção a uma «regra» se apresenta sempre como um *quid* fechado que não admite «extensões», assim também as «exceções» aos direitos fundamentais, resultantes das autorizações constitucionais para os restringir, nunca admitiriam outras para além daquelas que o legislador constituinte expressamente enunciou. Nestes termos, e voltando à autorização constitucional para restringir o direito à inviolabilidade das telecomunicações, constante do n.º 4 do artigo 34.º da CRP. Como tal autorização constitui uma «exceção», e a «exceção» só comporta a «matéria de processo criminal», encontra-se vedado — na lógica do Tribunal — qualquer processo interpretativo que procure indagar da razão de ser dessa mesma «exceção», a fim de saber se nela se poderá ou não incluir outra «matéria» que, não sendo a expressamente prevista, apresente no entanto com esta última afinidades *valorativas,* constitucionalmente relevantes.

3 — Creio, no entanto, que não é deste modo que se deve entender o conceito constitucional de «autorização para restringir [um direito fundamental]». Penso que quando a Constituição *remete* para a lei, indicando a possibilidade legal de limitação de um certo direito para um certo fim, não está a prever nenhuma «exceção» a nenhuma «regra» ou «norma». A complexidade da ordenação constitucional dos direitos fundamentais, e da sua relação com a lei, não se deixa reduzir a tão simples termos. Quando a Constituição remete para a lei, indicando a finalidade de uma restrição a um direito, o que está a fazer é coisa diversa: está a antecipar a possibilidade de ocorrência futura de conflitos entre o direito que consagra e outros «interesses» ou «valores» constitucionalmente protegidos, devolvendo ao legislador ordinário a tarefa necessária de resolução acertada desse conflito. No caso, em que se autorizou o legislador a restringir a inviolabilidade do segredo das telecomunicações «em matéria de processo criminal», previu-se a possibilidade de ocorrência futura de um conflito entre tal inviolabilidade, expressão da liberdade das pessoas, e a necessidade de preservação de valores comunitários fundamentais, expressos, nos termos da Constituição, por leis penais incriminadoras, aplicadas por intermédio das normas pertinentes de processo criminal. Além disso, e porque a incriminação de comportamentos e a sua concretização pelas normas de processo significam também elas próprias, como bem se sabe, restrições à liberdade (do destinatário das incriminações), a autorização constitucional expressa para restringir a inviolabilidade do sigilo das telecomunicações em matéria de processo criminal significa também a necessidade, constitucionalmente reconhecida, de fazer concordar a liberdade de uns (os titulares do direito à inviolabilidade das telecomunicações) com a liberdade de outros (os titulares dos direitos que a CRP confere a quem é arguido em processo criminal).

4 — A existência de Serviços de Informações da República — cujos fundamentos constitucionais o Tribunal pura e simplesmente não aborda —, numa ordem, como a nossa, de Estado de direito democrático, justifica-se pela necessidade de salvaguardar bens jurídicos, coletivos e individuais, que ocupam na axiologia constitucional um lugar não menor que os bens tutelados por normas penais incriminadoras. Todavia, da aplicação das normas que enformem o sistema de organização dos serviços da informações, ou da definição das suas competências, não decorrem — pela natureza mesma desses serviços — uma ameaça lesiva da liberdade individual que seja, pela sua intensidade, equiparável àquela que emerge, inevitavelmente, da aplicação das normas de processo criminal. Assim, e havendo afinidade valorativa ou teleológica entre as finalidades prosseguidas pelos serviços de informação e as normas penais incriminadoras — e decorrendo da aplicação das primeiras uma potencialidade de agressão da liberdade individual em todo o caso menor do que aquela que ocorre com a mera adjetivação das segundas — poder-se-ia concluir, se tivesse sido outra a posição conceptual e metódica de que se partisse, que a autorização constitucional para restringir a inviolabilidade das telecomunicações em «matérias de processo criminal» se estenderia, *por maioria de razão,* aos Serviços de Informações da República. Impedir a extensão por razões meramente textuais, ultrapassáveis pelo acrescento de algumas palavras à parte final do n.º 4 do artigo 34.º feito em processo de revisão constitucional, não me parece convincente: creio que os caminhos de uma hermenêutica constitucional adequada não passam pelo método estrito de uma «textualidade» como esta, que ergue em objeto de «interpretação» preceitos [e incisos desses preceitos] isoladamente tomados, sem consideração pelo lugar que ocupam no sistema axiológico da Constituição. Impedir a extensão por razões *valorativas* — que, por isso mesmo, permaneceriam para além de uma decisão parlamentar tomada pela maioria qualificada a que se refere o n.º 1 do artigo 286.º da CRP — implicaria demonstrar que só a *função jurisdicional do Estado* estaria apta para resolver em concreto o conflito entre a liberdade e a segurança que a necessidade de interceção de dados de tráfego das telecomunicações implica. Ora, a meu ver, essa demonstração não pode ser feita. Não vejo como possa retirar-se do sistema constitucional, no seu conjunto tomado, a proibição da existência de meios administrativos de *defesa da Constituição,* destinados a garantir a convivência adequada entre liberdade individual e segurança coletiva [e também individual], e por isso mesmo, capazes de ser abrangidos pela autorização constitucional constante da parte final do n.º 4 do artigo 34.º da CRP.

5 — Dito isto, não restam dúvidas que a interceção, por parte das autoridades públicas, dos dados de tráfego das telecomunicações, constitui por si mesma uma restrição grave do direito fundamental que o artigo 34.º consagra, com repercussões várias na limitação de outras facetas da liberdade individual, constitucionalmente consagradas. Como aliás o revela a jurisprudência supranacional que o Acórdão refere, a simples obrigatoriedade de conservação, por parte dos operadores privados de telecomunicações, desses mesmos dados durante um certo período de tempo — obrigatoriedade essa que se justifica para que as autoridades públicas àqueles possam aceder — já prefigura de *per se* uma lesão intensa na privacidade, e logo, na liberdade individual, que pode ser desde logo agredida por terceiros, ou por entidades privadas. Estando por isso o Estado obrigado a impedir essa agressão por parte de terceiros — através da emissão de normas suficientemente protetoras da liberdade individual — mal se compreenderia que, no que toca ao acesso dos seus próprios órgãos e agentes a esses mesmos dados, se não munisse de um sistema de regulação tão ou mais exigente do que aquele que é aplicado nas relações entre privados.

A regulação, por lei, dos Serviços de Informações da República, a incluir no sistema de competências desses

mesmos serviços a possibilidade de interceção dos dados de tráfego de telecomunicações, teria assim de, pelo menos, tornar tão claras e precisas quanto possível as circunstâncias em que o acesso a esses dados seria legítimo, de modo a não deixar à administração a liberdade de ponderar — sem quaisquer limites legais — da necessidade da interceção. Esta é uma exigência que decorre, desde logo da primeira frase do n.º 2 do artigo 18.º da CRP, uma vez ser a reserva de lei, que aí se consagra, não apenas *formal* mas também *material*. A intervenção agressiva da administração na esfera da liberdade dos privados não pode deixar de ser balizada por certos critérios a *definir por lei,* de modo a que seja a lei a distinguir, com um mínimo de precisão, a intervenção administrativa legítima da ilegítima. Depois, e ainda nos termos do n.º 2 do artigo 18.º da CRP, tal intervenção não poderia deixar de ser proporcionada, limitando-se ao necessário para «salvaguardar outros direitos ou interesses constitucionalmente protegidos». Por isso mesmo, a lei reguladora do sistema dos Serviços de Informações da República, a incluir na competência dos seus órgãos ou agentes a possibilidade de interceção dos dados de tráfego das telecomunicações, ter-se-ia de munir de um sistema interno de controlo quanto ao cumprimento dos limites legais dessas interceções que fosse, ele também, protetor da ameaça da liberdade que a referida interceção sempre representa.

6 — A meu ver, a norma no caso impugnada, e que atribuía, precisamente, a agentes dos Serviços de Informações da República a competência para a interceção dos dados de tráfego das telecomunicações, não cumpria estas exigências, que decorrem do disposto no n.º 2 do artigo 18.º da CRP.

Desde logo, e como se diz no Acórdão, a norma impugnada não definia com a precisão necessária os limites da intervenção administrativa na liberdade individual. A exigência de reserva de lei, na sua dimensão material, não se encontrava portanto (em meu entendimento) neste caso cumprida. Dizer, como se dizia no n.º 2 do artigo 78.º do Decreto da Assembleia, que tal intervenção seria legítima quando implicasse a adoção de meios «necessários, adequados e proporcionais, numa sociedade democrática, para o cumprimento das atribuições legais dos serviços de informação», equivale praticamente a dizer que *toda a ponderação quanto à proporcionalidade da intervenção* [e, portanto, quanto à legitimidade da mesma] seria por inteiro devolvida à administração. Nenhum critério minimamente preciso ou determinado, de distinção da intervenção lícita da ilícita, era pela lei fixado. Por outro lado, dizer-se — como se diz ainda na norma impugnada — que tal intervenção só seria possível, «para efeitos do disposto na alínea *c*) do n.º 2 do artigo 4.º» [que determinava deverem os serviços de informações «desenvolver atividades de recolha, processamento, exploração e difusão de informações [...] [a]dequadas a prevenir a sabotagem, a espionagem, o terrorismo e a sua proliferação, a criminalidade altamente organizada de natureza transnacional e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito democrático constitucionalmente estabelecido»], significava, pela amplitude e indeterminação da habilitação que era conferida à administração, que a intervenção desta última seria legítima numa tão vasta plêiade de circunstâncias que se tornaria praticamente impossível delimitar os fatores da sua não admissibilidade.

Perante este dado, o facto de, ainda de acordo com o n.º 2 do artigo 78.º do decreto parlamentar, os «oficiais de informações do SIS e do SIED [só poderem] aceder a dados de tráfego [...] mediante a autorização prévia e obrigatória da Comissão de Controlo Prévio» não preencheria por si só a necessidade de controlo e fiscalização interna da intervenção administrativa. Perante o silêncio da lei quanto aos limites da legalidade dessa intervenção, nenhuma garantia efetiva podia ser dada aos cidadãos de que a simples autorização prévia por parte da Comissão constituiria em si mesmo um procedimento *eficiente* de controlo da atuação administrativa, que prevenisse ou evitasse intromissões abusivas nas liberdades individuais. Assim, também por este motivo se não teria cumprido no caso a exigência decorrente do n.º 2 do artigo 18.º

A meu ver, o juízo de inconstitucionalidade deveria ter-se fundado apenas nestas razões, aliás retomadas, a final [pontos 21 e seguintes], no texto do próprio Acórdão. — *Maria Lúcia Amaral.*

Declaração de voto

Votei vencido.

Entendo, conforme memorando que apresentei como relator original, que o n.º 2 do artigo 78.º do Decreto n.º 426/XII, no específico quadro interpretativo traçado nesse memorando, é conforme à Constituição. É esse quadro interpretativo que pretendo deixar explicitado neste voto, servindo-me de partes significativas do memorando. É esta a explicação para a extensão do presente voto.

1 — Conforme se indica no Acórdão — e constitui pressuposto do pronunciamento do Tribunal —, o objeto do pedido de fiscalização preventiva restringe-se ao trecho do n.º 2 do artigo 78.º do Decreto n.º 426/XII que permite o acesso aos oficiais de informações do SIS e do SIED, em determinadas condições, a «dados de tráfego» e demais dados conexos com equipamentos de telecomunicações. Embora o requerimento de fiscalização indique todo o n.º 2, percebe-se do restante contexto expositivo ser esse tipo de dados (não a informação bancária e fiscal) que é visto pelo Requerente como problemático do ponto de vista da conformidade constitucional.

2 — Interessa a este respeito o disposto no n.º 4 do artigo 34.º da Constituição, norma integrada no título respeitante a «Direitos, liberdades e garantias» (especificamente no capítulo que integra os «Direitos, liberdades e garantias pessoais»), e que estabelece o seguinte, numa redação que vem (a do n.º 4) da Revisão Constitucional de 1997:

«Artigo 34.º

Inviolabilidade do domicílio e da correspondência

1 — O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis.

2 — A entrada no domicílio dos cidadãos contra a sua vontade só pode ser ordenada pela autoridade judicial competente, nos casos e segundo as formas previstos na lei.

3 — Ninguém pode entrar durante a noite no domicílio de qualquer pessoa sem o seu consentimento, salvo em situação de flagrante delito ou mediante autorização judicial em casos de criminalidade especialmente violenta ou altamente organizada, incluindo o terrorismo e o tráfico de pessoas, de armas e de estupefacientes, nos termos previstos na lei.

4 — 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.» (ênfase acrescentado).

O texto deste segmento anterior à 4.ª Revisão Constitucional (à Lei Constitucional n.º 1/97, de 20 de setembro) vinha da versão inicial da Constituição, estabelecendo o seguinte:

> «4 — É proibida toda a ingerência das autoridades públicas na correspondência e nas telecomunicações, salvos os casos previstos na lei em matéria de processo criminal.»

Consistiu esta alteração de 1997, pois, e sem qualquer indício — sublinhamo-lo desde já — de se ter visado algo mais do que o acesso pelas autoridades ao próprio conteúdo da comunicação, na integração no texto constitucional, em paralelo à correspondência em sentido clássico (o correio em suporte físico: as cartas, as encomendas postais e o telégrafo) e às telecomunicações existentes (basicamente o telefone, eventualmente já o fax e a telecópia), que correspondiam aos meios de comunicação clássicos pensados como a realidade existente em 1976, de outros meios equivalentes, os «demais meios de comunicação», abrindo a previsão do artigo a uma evolução, já fortemente pressentida em 1997, para novas realidades técnicas comunicacionais entre as pessoas. Estas, todavia, mantiveram no texto constitucional (no artigo 34.º, n.º 4) o sentido essencial que, então (em 1997), lhes era atribuído: fundamentalmente o correspondente ao conteúdo da própria comunicação (os *dados de conteúdo*, numa terminologia que posteriormente se tornou usual), não tanto, então em 1997, com um sentido, que possamos considerar claro, de abarcar outros dados respeitantes à comunicação, concretamente o que no futuro viria a ser qualificado como *dados de tráfego*, enquanto elementos que nada aportassem quanto ao conteúdo, em si mesmo, do ato comunicacional. A doutrina propendia, então (continuamos a referir o momento histórico da revisão de 1997), a associar a ideia de ingerência nas telecomunicações, essencialmente, à interceção das palavras trocadas entre os intervenientes. Com efeito, era então comum a referenciação «da danosidade social das escutas telefónicas» ao «direito à palavra» (Manuel da Costa Andrade, *Sobre as Proibições de Prova em Processo Penal*, Coimbra, 1992, p. 275; deve o trecho aqui citado ser situado no exato contexto em que foi escrito, em 1992, bem antes da evolução que viria a culminar com a introdução pela Lei n.º 48/2007, de 29 de agosto, do atual n.º 2 do artigo 189.º do CPP).

O que aqui se pretende sublinhar, sem menosprezar o significado do elemento evolutivo que a questão dos *dados de tráfego* assumiu posteriormente, é, tão-somente, a circunstância de o n.º 4 do artigo 34.º da CRP não se ter formado num quadro em que a questão do acesso aos dados circunstanciais da comunicação se colocasse exatamente com o mesmo sentido do próprio acesso ao conteúdo da comunicação, e já então a questão do acesso das autoridades aos *dados de tráfego* havia sido equacionada, por exemplo, na jurisprudência do Tribunal Europeu dos Direitos do Homem, no Acórdão *Malone v. Reino Unido*, de 1984, a respeito do trecho do artigo 8.º, n.º 2, da *Convenção* que exige que a ingerência das autoridades esteja «prevista na lei» (foi esse o exato sentido da decisão *Malone*, cf. os respetivos pontos 66 a 68, e, posteriormente, em 1990, da decisão *Huvig e Kruslin c. França*, cf. Louis-Edmond Pettiti, Emmanuel Decaux, Pierre-Henri Imbert, *La Convention Européenne des Droits de L'Homme. Commentaire article par article*, 2.ª ed., Paris, 1999, pp. 314/315). Ou seja, o que aqui se pretende afirmar é, tão-só, que o texto constitucional, não se tendo cristalizado numa fase (inicial) de «indiferença valorativa» pelo que hoje chamamos *dados de tráfego*, não assimilou logo para estes um grau de proteção absolutamente idêntico ao dos *dados de conteúdo*.

Adiante voltaremos a esta questão, a respeito da apreciação de precedentes na jurisprudência deste Tribunal que entendemos dever convocar à discussão da viabilidade constitucional do artigo 78.º, n.º 2, do Decreto n.º 426/XII. Por ora, interessa-nos — e isso é claro no trecho final do artigo 34.º, n.º 4, da CRP — que a exceção à proibição de ingerência das autoridades públicas nas telecomunicações é estabelecida sob *reserva de lei* («salvos os casos previstos na lei») e é referida a «matéria de processo criminal».

3 — Pelo preenchimento do primeiro destes elementos, a *reserva de lei*, vale aqui a clareza da opção do legislador originário e exclusivo nesta matéria, a Assembleia da República [cf. o artigo 164.º, alínea *q*), da CRP], envolvendo o Diploma aprovado uma manifestação inequívoca e particularmente expressiva — facto que o Requerente não deixou de sublinhar no artigo 4.º do pedido de fiscalização — do propósito de conceder aos Serviços de Informações integrados no SIRP, mediante condições bem definidas, que incluem um mecanismo dedicado de controlo prévio condicionante, de acesso aos *dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização*.

Interessa sublinhar esta incidência, além de tudo o mais, enquanto preenchimento expressivo de uma condição identificada, no quadro dos Estados de direito, relativamente a leis que envolvam elementos restritivos de direitos fundamentais, e especificamente quanto à consideração dos meios de atuação dos Serviços de Informações. Referimo-nos ao chamado «princípio da afirmação clara» pelo legislador (*clear statemant principle*), expressão cunhada por Cass Sunstein, referindo-se, como caso paradigmático, a uma decisão do Supremo Tribunal de Israel, de 6 de setembro de 1999 [*Association for Civil Rights in Israel v. The General Security Service (1999). Supreme Court of Israel: Judgement Concerning the Legality of the General Security Service's Interrogation Methods, 38, I. L. M. 1471 (1999)*], afirmando a absoluta ilegitimidade do estabelecimento, pelo próprio serviço de informações, de meios ou métodos de atuação, sem um expresso mandato legal, *maxime*, na ausência de uma clara e inequívoca decisão a esse respeito por parte do legislador (do Parlamento), excluindo que qualquer opção neste domínio seja definida, «com base numa construção legal vaga e ambígua», criada *ad hoc* no seio do próprio serviço de informações, arvorando-se este uma faculdade de fixar métodos de atuação e de avançar num qualquer vazio legal. Comentando este pronunciamento do Supremo Tribunal de Israel, refere Cass Sunstein:

> «[...]
> Podemos tomar esta decisão judicial enquanto afirmação de um princípio geral, segundo o qual o poder legislativo deve autorizar, explicitamente, medidas controversas que apresentem um potencial restritivo de direitos fundamentais [*explicitly authorize disputed infringments on civil liberty*]. A razão para o estabelecimento desta salvaguarda assume um sentido garantístico, contra o estabelecimento de restrições inadequadamente ponderadas nas suas consequências, reforçando

a salvaguarda política consistente na existência de um acordo formado no seio de um órgão deliberativo de estrutura plural, enquanto pré-condição mínima para a adoção de medidas restritivas de direitos. Constitui um risco especial neste domínio que a polarização, no seio de um grupo específico dentro da Administração, conduza a opções que não tenham sido sujeitas a um debate suficientemente alargado a todas as perspetivas. Contrariamente, um processo de deliberação no seio do Parlamento [*Deliberation within the legislative branch*] corresponde a uma mais ampla garantia de que as opções restritivas de direitos sejam efetivamente defensáveis. Um Parlamento, precisamente em função da amplitude e diversidade da sua composição, dá maiores garantias de consideração dos pontos de vista dos onerados com a restrição [*is more likely to contain people who will speak for those who are burdened*] e, por isso mesmo, um processo legislativo ocorrido no seu seio potencia uma mais adequada proteção da realidade que Hayek identifica com o Estado de direito. Neste sentido, a exigência de uma opção legislativa clara [*a clear legislative statement*] assegura a existência de níveis diversificados de controlo [*checks and balances*] na proteção dos direitos individuais.

[...]» (*Laws of Fear. Beyond the Precautionary Principle*, Cambridge, Nova York, 2005, pp. 212/213).

4 — Assente que a aprovação do Diploma (do Decreto n.º 426/XII), integrando a norma aqui questionada, consubstancia — e esta afirmação tem algo de tautológico — a própria *reserva de lei*, numa expressão clara e inequívoca, interessa agora caracterizar a atividade dos Serviços de Informações, enquanto elemento central da discussão em torno da referenciação, no n.º 4 do artigo 34.º da CRP, do *processo criminal*, como espaço de tolerabilidade da *ingerência das autoridades públicas nas telecomunicações e demais meios de comunicação*. Trata-se aqui de referenciar essa atividade (a dos Serviços de Informações) no plano constitucional e de procurar a articulação desta atividade com o plano dos valores substanciais intuídos no trecho final desse n.º 4. Com efeito, a existência dessa articulação propiciará um modelo interpretativo apto a sustentar — interpretativamente — que a referência ao *processo criminal* não afasta, em termos absolutos, da lógica de viabilização de uma ingerência reportada aos *dados de tráfego*, a atividade dos serviços de informações.

5 — A Constituição da República Portuguesa não trata em qualquer norma — queremos dizer que não trata direta e explicitamente — da atividade dos Serviços de Informações, atividade que referenciaremos aqui, olhando à essência teleológica base de um Diploma contendo o Regime Jurídico do SIRP (a Lei n.º 30/84, de 5 de setembro, e o Decreto n.º 426/XII), como *função de produção de informações*. Todavia, através de um argumento de pendor orgânico, referido à alocação da competência legislativa exclusiva nesta matéria ao Parlamento {referimo-nos ao artigo 164.º, alínea *q*), da Constituição: [*é*] *da exclusiva competência da Assembleia da República legislar sobre* [...] *q*) [*r*]*egime do sistema de informações da República e do segredo de Estado* [...]}, podemos intuir, através da integração dessa competência na reserva absoluta da Assembleia, a consideração da organização funcional, atribuições legais e meios de atuação dos Serviços de Informações — dos Serviços integrantes do SIRP — como matéria pretendida sujeitar aos requisitos específicos que justificam uma tal opção atributiva de competência, a saber: «[...] o sentido e alcance da reserva absoluta de lei parlamentar [*significa*], sobretudo: (*a*) que o processo de criação legislativa é público, desde a apresentação do projeto ou da proposta de lei na AR; (*b*) que o procedimento legislativo está sujeito ao contraditório político, com intervenção das minorias; (*c*) que todas e cada uma das normas são formalmente produto da vontade da assembleia representativa.» (J. J. Gomes Canotilho, Vital Moreira, *CRP. Constituição da República Portuguesa Anotada,* 4.ª ed., Coimbra, 2010, p. 309).

Esta reserva absoluta foi introduzida na revisão constitucional de 1997, traduzindo-se na migração da anterior reserva relativa [antiga alínea *r*) do artigo 168.º] para a atual reserva absoluta. A origem desta opção é caracterizada por um participante nesse processo de revisão, como «[inculcando] nitidamente que a reserva não se confina à aprovação de bases gerais ou de estatuto (geral) dos serviços. A solução aprovada acarreta, pois, notória diminuição dos poderes que o Governo vinha exercendo [durante os anos 80] neste domínio sensível, podendo contribuir para atenuar a opacidade e secretismo que têm caracterizado o processo de instalação dos serviços de informações (e reforçar o controlo democrático das suas atividades)» (José Magalhães, *Dicionário da Revisão Constitucional*, Mem Martins, 1989, p. 57). Note-se que, adicionalmente à intencionalidade que, em si mesma, a alocação desta reserva já inculca, existe um elemento significativo, exterior ao texto constitucional, de referenciação de todo o Sistema de Informações, na vertente do seu controlo externo, ao Parlamento. É esse o sentido da existência, desde a conceção inicial do SIRP, do *Conselho de Fiscalização do Sistema de Informações da República Portuguesa* [artigo 7.º, alínea *a*), da Lei n.º 30/84, designado agora, no Decreto n.º 426/XII — artigos 3.º, n.º 3, alínea *a*), e 20.º, alínea *a*) —, *Conselho de Fiscalização do SIRP*], eleito pela Assembleia da República (artigos 8.º a 13.º da Lei n.º 30/84, artigo 21.º do Decreto n.º 426/XII).

6 — A discussão no plano constitucional — no quadro de uma democracia constitucional — da atividade dos Serviços de Informações convoca ao debate, necessariamente, os valores *Segurança* e *Democracia*, colocados em paralelo, assumindo a existência de uma tensão existencial permanente entre a adoção de políticas públicas promotoras de segurança e os valores democráticos — os valores próprios de um Estado de direito democrático —, concretamente aqueles que se expressam no exercício de direitos fundamentais. Trata-se neste domínio, essencialmente, de responder a um desafio: o desafio da perspetivação da Segurança, no sentido decorrente do artigo 27.º, n.º 1, da CRP («[t]odos têm direito à liberdade e à segurança»), enquanto obrigação prestacional do Estado aos cidadãos, numa relação de tensão entre valores constitucionais. E, com efeito, todos reconheceremos que a prestação de Segurança pelo Estado suscita frequentemente questões complexas de compatibilização (mesmo de tensão existencial) entre direitos, apresentando-se como um domínio de eleição na atuação do princípio da proporcionalidade, com o sentido que o nosso texto constitucional confere a este: «[a] lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos e interesses constitucionalmente protegidos» (artigo 18.º, n.º 2, da Constituição).

Simplificando, diremos que a compressão que uma determinada política pública, promotora do valor segurança,

possa induzir numa posição jusfundamental justificar-se-á — só se justificará — se essa compressão for efetivamente referida à promoção desse valor constitucional, sendo necessária à implementação dele e, entre as opções possíveis, representar o mínimo de compressão necessário à salvaguarda desse valor. É este, fundamentalmente, «metido numa casca de noz», o sentido do princípio da proporcionalidade e a aplicação deste aos valores segurança e liberdade, colocando frequentemente problemas delicados, não convoca um modelo analítico distinto do que subjaz ao artigo 18.º, n.º 2, da Constituição, concretizado nas chamadas «quatro regras da proporcionalidade»: *prossecução de um fim legítimo*, *adequação* a esse fim, *necessidade* e proporcionalidade em sentido estrito, em que se determina, comparando diretamente as situações em confronto, se a restrição representa um ganho líquido relativamente à sua não adoção. Utilizámos neste trecho expositivo, na caracterização do princípio da proporcionalidade, a «desdobragem» do mesmo em «quatro componentes», no sentido referido por Matthias Klatt e Moritz Meister (*The Constitutional Structure of Proportionality*, Oxford, 2012, pp. 8/9) e por Ahron Barak (*Proportionality. Constitutional Rights and Their Limitations*, Cambridge, 2012, pp. 131/132). A jurisprudência deste Tribunal, concretamente no Acórdão n.º 187/2001, ao qual adiante recorreremos desenvolvidamente, analisa o princípio da proporcionalidade em três subprincípios: adequação, necessidade ou exigibilidade e proporcionalidade em sentido estrito. Não expressamos aqui algo de substancialmente distinto desta visão ao isolar, como ponto de partida da aferição de proporcionalidade, a necessária prossecução de um fim constitucionalmente legítimo, sendo certo que este elemento é intuído — sempre o foi — pela jurisprudência deste Tribunal, como questão prévia condicionante da restrição, cujo reflexo encontramos no artigo 18.º, n.º 2, no trecho «[...] nos casos expressamente previstos na Constituição [...]».

Reconhece-se que no seio desta equação — prestação de segurança pelo Estado, defesa da liberdade — a atuação dos Serviços de Informações constitui uma área sensível — até particularmente sensível —, justificando-se o tratamento destes como um caso especial. Esta sensibilidade é explicada por Jennifer E. Sims e Burton Gerber, aludindo ao dilema que se coloca aos decisores políticos nas opções referidas à estruturação dos Serviços de Informações: «[...] os melhores sistemas de informação [*intelligence systems*] envolvem segredo de Estado a exploração do engano e a atuação clandestina; contudo, esses sistemas, quando centrados dentro do país para fazer face a ameaças a interesses vitais nacionais vindas do exterior, podem colocar em risco elementos fundamentais da democracia que, paradoxalmente, devem proteger [...]. Este risco sublinha a menor importância que, para esconjurar este perigo, a estrutura organizacional tem, comparativamente às políticas, práticas e liderança implementadas nesses serviços» (*Transforming US Intelligence*, Washington, 2005, p. XI da Introdução).

Vale, a respeito da promoção da segurança como valor constitucional, o entendimento da Constituição, do espaço vivencial por ela desenhado, como envolvendo uma proteção ativa do modelo democrático que expressa, funcionando o texto constitucional como «contrato social» contendo cláusulas, explícitas e implícitas, de autodefesa, através das quais se constrói o conteúdo de uma função de «proteção da Constituição» (fórmula que a Constituição alemã expressamente inclui no seu texto — *Verfassungsschutz*), que legítima, além da tutela penal propriamente dita, o que se pode designar como «proteção administrativa da Constituição». Trata-se aqui do que a Doutrina constitucional germânica identifica como «[...] institutos e faculdades para a defesa da ordem fundamental livre e democrática [...]», englobando a atividade dos serviços de informações, ou seja: «[...] a recolha e tratamento de informações [...] em âmbitos que antecedem as ameaças concretas para os bens jurídicos protegidos. Tal recolha e avaliação abarca [...] a vigilância de pessoas e organizações suspeitas de atividades contrárias à Constituição» (Erhard Denninger, «Stretbare Demokratie und Schutz der Verfassung», in *Benda, Maihofer, Vogel, Hesse, Heyde, Handbuch des Verfassungs Rechts*, 2.ª ed., Berlim, 1994, p. 699). Corresponde esta forma especial de proteção, a atividade que a concretiza, ao domínio primordial de atuação dos Serviços de Informações, corresponde, enfim, à função de produção de informações.

Assim, podemos caracterizar a intencionalidade desse conteúdo funcional (a tal atividade de proteção da Constituição, não de proteção ou de defesa do Estado aparelho de poder) como um sistema estruturado em vista do desencadear de mecanismos de *alerta prévio*, uma função sequencialmente referida ainda a um momento anterior ao da entrada em jogo — *rectius*, da adjetivação — da tutela penal, mas que, nem por isso, deixa de estar ligada aos valores específicos (aos tipos) abarcados pela lei penal, e de poder mesmo vir a entroncar na adjetivação penal. É que, num Estado de direito democrático, fora de um quadro de referenciação aos valores subjacentes à tutela penal — fora dos mínimos éticos e dos valores jurídico-constitucionalmente reconhecidos em que esta assenta (v. Jorge de Figueiredo Dias, *Direito Penal*, Parte Geral, t. I, 2.ª ed., Coimbra, 2007, p. 120, § 25) — não existe qualquer intervenção legítima de proteção do espaço constitucional. Pelo contrário, existirá um uso abusivo e ilegítimo dessa função protetiva. Defender-se-á algo, eventualmente defender-se-á o poder (algum poder circunstancial), mas isso nada tem de ver com a proteção de uma «ordem fundamental livre e democrática». E é esta que legitima — e só ela legitima — a tarefa de «proteção da Constituição». Esta — esta atividade exercida num espaço de legitimidade constitucional — situar-se-á, pois, na antecâmara da tutela penal, numa fase ainda larvar desta, e atuará onde os respetivos valores, mesmo que em termos difusos e ainda com um significado ambíguo, já estejam demonstravelmente presentes, já tenham, enfim, sido colocados nalgum tipo de insegurança existencial minimamente concretizada e individualizada. E será este *mínimo de concretização* e de *individualização* de uma ameaça que também poderíamos caracterizar através da ideia de risco, reportada aos valores elencados no n.º 2 do artigo 4.º do Decreto n.º 426/XII (todos eles reportáveis, por sua vez, à tutela penal), que os Serviços de Informações sujeitarão à apreciação da *Comissão de Controlo Prévio*, na lógica de funcionamento do n.º 2 do artigo 78.º do mesmo Decreto, recaindo sobre eles (sobre os Serviços de Informação) o ónus de demonstrar os pressupostos mencionados na norma.

Assim, numa espécie de síntese conclusiva, diremos que **a atividade de proteção da Constituição incidirá sobre condutas individuais ou coletivas que contenham uma potencialidade, não negligenciável, de menoscabo, mesmo que embrionário, dos valores próprios de uma «ordem fundamental livre e democrática», quando esse desvalor seja reportável ao elenco do n.º 2 do artigo 4.º do Decreto n.º 426/XII e potencie, ou torne ra-**

cionalmente expectável, uma evolução que, em última análise, nos conduza a condutas penalmente típicas, referenciáveis aos valores estruturantes dessa «ordem fundamental livre e democrática» — em particular o terrorismo (ao qual se refere a Lei n.º 52/2003, de 22 de agosto), a espionagem e outros dos crimes contra o Estado, fundamentalmente os elencados no título V do Código Penal, constituindo estes exemplos paradigmáticos que justificam essa intervenção precoce correspondem ao espaço de referência da defesa da Constituição.

7 — A *função de produção de informações* — a atividade dos serviços de informações — no quadro institucional dos organismos do Estado dedicados a essa tarefa (que são, no nosso caso, os organismos integrantes do SIRP) traduz-se na incumbência funcional de «[...] assegurar, através dos serviços de informações, no estreito respeito da Constituição e da lei, a produção de informações necessárias à salvaguarda da segurança interna e externa, da independência e interesses nacionais e da unidade e integridade do Estado» (artigo 2.º do Decreto n.º 426/XII). Esta tarefa recai, no quadro do SIRP, sobre dois Serviços: o *Serviço de Informações de Segurança* (artigo 56.º do Decreto n.º 426/XII), que é um serviço dedicado à produção de informações de segurança interna, e o *Serviço de Informações Estratégicas de Defesa* (artigo 57.º do mesmo Decreto), que é um serviço de informações reportado à vertente externa (exterior ao território nacional) da segurança do Estado Português e da projeção externa dos seus interesses.

Tratam-se estas de caracterizações cuja essência decorre da atribuição funcional, com âmbitos distintos (a segurança externa e a segurança interna), da tarefa de produção de informações. Atividade correspondente — e as definições legais pressupõem e acomodam-se a esta ideia — à procura de um conhecimento sistematizado, qualitativamente superior, projetado no futuro, no sentido em que se exprime através da formulação de previsões, visando a eliminação ou a redução da incerteza, num quadro de competição ou de conflito, com o sentido de habilitar o destinatário do produto assim criado na tomada de decisões. A informação — as *informações* com este sentido — não se reduz à procura de meras notícias mais ou menos contextualizadas, que expressam, quanto muito, a matéria-prima (a informação em bruto) a partir da qual se produzem, após processamento, as *informações* funcionalmente atribuídas aos Serviços de Informações.

A atividade de produção de informações, no sentido aqui relevante, expressa-se, assim — e seguimos aqui um texto de Arménio Marques Ferreira, «O Sistema de Informações da República Portuguesa», em *Estudos de Direito e Segurança*, Coimbra, 2007, p. 69 —, em elementos sistematizados em quadros interpretativos, através de critérios que sobrepõem a estrutura de sentido à relação causal (projetam o significado de uma realidade complexa em si mesma), que são produzidas através de uma ferramenta metodológica específica, de um método próprio [habitualmente referido como o *ciclo de produção de informações*: (*i*) *orientação da pesquisa*, (*ii*) *pesquisa*, (*iii*) *análise*, (*iv*) *difusão da informação*], método este que se reproduz funcionalmente dentro de um serviço de informações, na divisão entre áreas de pesquisa e áreas de análise, elementos esses que são preservados do conhecimento de terceiros através de procedimentos protetivos próprios, correspondentes, na sua vertente normativa, à ideia de *segredo de Estado*.

Trata-se, pois, quando falamos da produção de informações, de caracterizar um tipo especial de conhecimento — um conhecimento interpretativo qualificado — e de o referir, na sua origem, a estruturas organizacionais, os Serviços de Informações, assentes numa metodologia de trabalho própria, dedicados à produção desse tipo de conhecimento. Nas palavras de Robert Gates, as informações lidariam primordialmente com segredos: os segredos, porque passíveis de ser descobertos, situar-se-iam num plano de cognoscibilidade direta correspondente ao que é «claro» — ao que se torna claro quando é descoberto, aliás. Depois viriam os *mistérios*, situando-se estes numa zona de ambiguidade intrínseca que nunca fornece respostas claras. A tarefa da *análise* seria solucionar, por via dos segredos descobertos, os mistérios que ensombram o processo de tomada de decisão, eliminando ou diminuindo substancialmente o fator incerteza (adaptámos aqui a caracterização por Robert Gates da atividade de *análise*, in *Intelligence Requirements for the 1990's: Collection, Analysis, Counterintelligence, and Covert Action*, ed. Roy Godson, Washington, 1989, p. 115).

Assim, constitui a essência da *função de produção de informações* — da função de «inteligência» (o vocábulo apropriado à designação das *informações* que teimosamente se recusa a entrar no nosso léxico) — a «[...] recolha e tratamento da informação, sendo que a análise, recorrendo a todo o tipo de fontes, traduz uma componente específica dessa atividade, tal como a ação encoberta [*covert action*]». Todavia, «[...] a característica comum e principal desta atividade reside no seu caráter sensível, por questões de propriedade e de legalidade, mas principalmente por razões de vulnerabilidade das suas fontes e métodos à adoção de contramedidas [...]. Daqui decorre o caráter secreto da atividade de informações: o secretismo constitui a imagem de marca das informações, a base da sua relação com o governo (com o destinatário da informação) e a sua própria autoimagem» (Michael Herman, *Intelligence Services in The Information Age*, Londres, 2002, pp. 3/4).

Como conclusão diremos, enfim, que estas diversas definições projetam a matriz militar milenar das *informações* [que remonta à *A Arte da Guerra* de Sun Tzu (*Sunzi*), possivelmente escrita no século VI antes da era comum] e poderiam, sem perda de rigor, ser reduzidas à caracterização que Richard Posner nos dá de *intelligence* dizendo que «[o] objetivo da 'produção de informações' [*the goal of intelligence*] é o conhecimento das intenções e das capacidades de inimigos potenciais» (*Preventing Surprise Attacks. Intelligence Reform in the Wake of 9/11*, Nova York, Oxford, 2005, p. 99).

8 — O elemento central na previsão da norma objeto, o que é questionado na sua conformidade constitucional pelo Requerente, refere-se à natureza dos dados relativos às telecomunicações facultados aos oficiais de informações, mediante autorização da Comissão de Controlo Prévio. Tratam-se de *dados de tráfego — de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização*. São estes elementos que a exposição de motivos que acompanhava a proposta de lei do Governo que esteve na origem do Decreto n.º 426/XII (cf. o artigo 3.º do pedido) qualificava, não com total rigor, como correspondendo a

metadados, enquanto conceito intuído como apropriado aos *dados de tráfego*.

Todavia, o emprego desta expressão — metadados — no contexto que aqui nos interessa é suscetível de criar equívocos. Com efeito, na ciência da computação, corresponde o conceito de *metadados*, usualmente definidos como «dados sobre dados» {«[*m*]*etadata is simply data about data* [...]», Jembaa Cole, «*When invisible electronic ink leaves red faces: tactical, legal and ethical consequences of the failure to remove metadata*», disponível em: https://digital.law.washington.edu/}, à separação, dentro de uma determinada realidade significativa, entre um núcleo que qualificaríamos de central, correspondente à própria realidade, e elementos periféricos, laterais, a ela ligados por alguma relação ou ponto de contacto, os quais, não contendo essa realidade em si mesma, expressam algum tipo de contexto circundante da mesma, relacionado mas separado dela. É assim que os *metadados* são referidos, na ciência da computação, como «[...] informação estatística não visível respeitante a um determinado documento, gerada por um programa de *software* [...]» (Jembaa Cole, «*When invisible electronic ink leaves red faces*…», cit.). A utilidade destes elementos refere-se especialmente à gestão de bases ou de grandes bancos de dados (armazéns de dados, *data warehouse*), no sentido em que permitem parametrizar determinados elementos — nomes, números, relações lógicas redutíveis a um predicado verbal — e, através destes, procurar conexões relevantes (procurar informação útil) dentro de uma base de dados, evitando a necessidade de realizar uma procura através da «localização física», documental, dessas conexões (como paradigmaticamente ocorre numa procura com ficheiros em suporte de papel).

Ora, os *dados de tráfego* aqui em causa são (contêm) informação em si mesmos, permitem o estabelecimento de conexões entre pessoas e situações, tomando como ponto de partida a existência pretérita de uma determinada comunicação, esgotando-se o seu sentido numa extrapolação analítica realizada com base na existência dessa comunicação e das relações que ela indica, não com base no conteúdo da própria comunicação. Tal circunstância introduz, desde logo, o elemento central — por vezes objeto de confusão numa discussão superficial — da caracterização dos *dados de tráfego*, qualificados como *metadados*, referidos, como aqui sucede, às telecomunicações, distinguindo (separando) estes do próprio conteúdo da comunicação (a mensagem em si mesma). É com este sentido, num debate que envolve frequentemente a ponderação do significado do acesso das autoridades públicas aos chamados *metadados* (se entendidos como *dados de tráfego*), que se contrapõe, quando — como aqui sucede — está em causa, tão-somente, o acesso a estes, o sentido de uma «análise do tráfego contra a análise do conteúdo» («*traffic versus content analysis*»), reconduzindo a uma dimensão mais atenuada o potencial de compressão de direitos, mesmo de afetação da autodeterminação informacional, envolvido por um acesso exclusivo aos *metadados* (cf. Amitai Etzioni, *Privacy in a Cyber Age. Policy and Practice*, Nova York, 2015, pp. 132/133). Esse acesso não deixa, todavia, de consubstanciar uma intromissão na privacidade e, por isso mesmo, não dispensa o seu tratamento como tal: como intromissão numa dimensão específica do direito à privacidade.

Existe, porém, uma diferença relativamente aos dados de conteúdo (ao que faculte um efetivo acesso ao conteúdo da comunicação), diferença que é facilmente percetível no seu significado, ponderando um exemplo prático, que reputo de sugestivo, referido pelo Autor antes citado, a propósito da recolha de *dados de tráfego* {«[os] registos telefónicos que mostram quem chamou e para que números, o momento em que a chamada foi feita e a sua duração — e nada mais [...]», *ob. cit.,* p. 133}: «[i]sto é equivalente à cópia de um envelope contendo um endereço, por contraposição a ler efetivamente a correspondência nele contida — uma prática que, de facto, é levada a cabo regularmente, em massa, pelo U. S. Postal Service. Com efeito, o USPS 'fotografa o exterior de cada objeto postal que é processado nos Estados Unidos' e conserva este registo fotográfico por um período de tempo indeterminado» (*ibidem*; a abonação, no texto de Amitai Etzioni, desta afirmação é a seguinte: «Ron Nixon, 'U. S. Postal Service Logging All Mail for Law Enforcement'», *The New York Times,* July 3, 2013, http://www.nytimes.com/2013/07/04/us/monitoring-of--snail-mail.html?pagewanted=all, n. 86, p. 223).

É ainda relevante sublinhar o contexto da aquisição deste tipo de informação (dos ditos *metadados*). Pode tratar-se (*i*) de uma aquisição de informação em larga escala, por transferência integral, para alguma autoridade pública, dos registos existentes num operador, ou pode tratar-se (*ii*) de uma transferência individualizada, realizada (autorizada e controlada) caso a caso, com base numa suspeita concreta e individualizada. É relevante a distinção porque colocam as duas situações problemas muito distintos. Notamos que à primeira situação correspondem os programas de recolha de dados, pela NSA — *National Security Agency*, à escala global, vindos a público em 2013 (no âmbito do chamado caso Snowden), basicamente o programa «*Bulk Collection of Telephone Metadata*», referido à recolha e conservação, pela NSA, dos registos de comunicações telefónicas efetuadas e recebidas nos Estados Unidos, o programa «*PRISM*», dedicado à recolha, igualmente pela NSA, de comunicações eletrónicas de determinados fornecedores de serviços *online*, caso da *Google* e do *Facebook*, este programa dirigido, fundamentalmente a «não-americanos» e o programa «*TEMPORA*», mantido pelo *Government Communications Headquarters* (GCHQ) do Reino Unido (cf., quanto à caracterização dos dois primeiros Programas, Amitai Etzioni, *Privacy in a Cyber Age*…, cit., pp. 123/125, e quanto ao programa «*TEMPORA», «A simple guide to GCHQ's internet surveilance programme Tempora*», in *Wired.co.UK*, http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora101). E notamos que a segunda situação — a obtenção de *dados de tráfego* caso a caso —, desde logo pela sua escala, dimensão individualizada e especificamente motivada por factos concretos, controlados exteriormente ao interessado na aquisição da informação, não contém o perigo da verdadeira «pesca de arrastão» à escala global, que conduziu o Tribunal de Justiça da União Europeia, no Caso *Digital Rights Ireland, Ltd* (C-293/12), Acórdão de 8 de abril de 2014, a considerar inválida a «Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, 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, e que altera a Diretiva 2002/58/CE».

Estava em causa nesta situação, com efeito, a conservação pelos operadores, obrigatoriamente, de dados de tráfego por um período mínimo de seis meses e máximo de dois anos, a qual, incidindo sobre todas as comunicações, indiferenciadamente à escala global europeia, comportava

uma ingerência, não substanciada em indícios concretos e atendíveis, «nos direitos fundamentais de quase toda a população europeia» (v. os pontos 56 e 58 do Acórdão). Ora, este fator de perigo desaparece (no específico sentido em que o Tribunal de Justiça o enunciou) quando o que ocorre é, tão-somente, a prestação de uma informação pelo operador de telecomunicações, em suporte de papel, quanto às chamadas realizadas por um determinado número e à localização espacial dessas chamadas (do equipamento com o qual foram realizadas) por referência a uma antena que distribuiu o sinal. Mais ainda, quando essa informação só é obtida em situações individualizadas, baseadas na existência de indícios consistentes, necessariamente referidos a pressupostos específicos exigentes, controlados caso a caso por uma entidade independente, cuja atuação visa, precisamente, limitar o acesso aos dados e a sua utilização ao estritamente necessário para se alcançar o objetivo prosseguido num espaço de legitimidade legal e constitucional.

Serve isto para deixar clara a absoluta falta de paralelismo de situações de recolha de dados abstratos em massa com a situação suscitada nesta fiscalização preventiva, desde logo pela incomensurável diferença de escala envolvida, que induz perigos totalmente distintos. Com efeito, trata-se aqui — e só disso se trata — dos dados individualizados de um caso concreto (que têm de pressupor a existência de um «caso concreto» no serviço de informações que a eles pretende aceder), quando nessas outras situações se tratava da transferência em bloco de grandes massas de dados, desligados de casos concretos, no intuito de, algures no futuro, serem estes dados confrontados com hipotéticos casos concretos. Aqui, no particular contexto do tipo de *dados de tráfego* relativos a telecomunicações, previstos no n.º 2 do artigo 78.º do Decreto n.º 426/XII, além da dimensão individualizada destes, sempre sujeita a um controlo prévio condicionante assente em pressupostos de base restritiva, verificamos que a ulterior conservação pelos Serviços de Informações dos dados cumulativamente gerados pelos acessos autorizados no passado, os dados acumulados ao longo do tempo, sempre será controlada pela *Comissão de Fiscalização de Dados do SIRP* (o órgão de fiscalização externo com origem na Magistratura do Ministério Público, prevista nos artigos 29.º a 34.º do Decreto n.º 426/XII), com a efetiva possibilidade de cancelamento do que seja indevidamente conservado ou incluído nos centros de dados dos dois Serviços. Existe, pois, na lógica de funcionamento do sistema — na lógica de funcionamento do SIRP — uma salvaguarda de controlo externo das potencialidades desvaliosas da concentração de grandes massas de informação referida a pessoas.

9 — Posicionado o sentido da regra contida no artigo 34.º, n.º 4, *in fine* da CRP, explicitado o sentido da função de produção de informações, inserida na arquitetura fundamental das estruturas dedicadas a essa função, os Serviços de Informações, e caracterizados os dados em causa na previsão legal sujeita à presente fiscalização, interessa centrar esta indagação na procura de resposta às duas questões colocadas no ponto 7.º do requerimento de apreciação da conformidade com a Constituição da norma constante do n.º 2 do artigo 78.º do Decreto n.º 426/XII. São elas: *i*) *deve o acesso aos metadados considerar-se uma ingerência nas telecomunicações para os efeitos previstos na norma constitucional?; e ii*) *pode considerar-se que a autorização prévia e obrigatória da Comissão de Controlo Prévio equivale ao controlo existente no processo criminal?*

9.1 — A resposta à primeira pergunta implica que se caracterizem os *dados de tráfego* em causa no n.º 2 do artigo 78.º do Decreto, por referência a alguns precedentes colhidos na jurisprudência deste Tribunal. A tal propósito, o Tribunal Constitucional acolheu, desde o Acórdão n.º 241/2002, uma classificação tripartida (louvando-se, então, nos Pareceres do Conselho Consultivo da Procuradoria-Geral da República n.os 16/94, votado em 24/06/94, na base de dados da DGSI, 16/94 — complementar, votado em 2/05/1996, in *Pareceres*, vol. VI, pp. 535 a 573, e 21/2000, de 16/06/2000, no *Diário da República,* 2.ª série, de 28/08/2000) dos dados resultantes do serviço de telecomunicações. Ali se distinguiram:

> «[...]
> [O]s 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 (por exemplo, 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** [...].
> [...]»

Tal classificação tripartida foi retomada pelo Tribunal — assinalando que se mantinha, então, «consensual» — no Acórdão n.º 486/2009. Também o Conselho Consultivo da Procuradoria-Geral da República continuou a fazer uso dela (v. g., no Parecer de 07/05/2009, disponível na base de dados da DGSI), já com apoio suplementar na Lei n.º 41/2004, de 18 de agosto, que, no seu artigo 2.º, n.º 1, alínea *d*), define os dados de tráfego como «quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma». Os tribunais superiores também acolheram a dita classificação (cf. os Acórdãos do Supremo Tribunal de Justiça de 03/03/2010, proferido no processo n.º 886/07.8PSLSB.L1.S1, do Tribunal da Relação do Porto de 11/02/2015, proferido no processo n.º 2063/14.2JAPRT-A.P1, de 10/09/2014, proferido no processo n.º 1953/00.4JAPRT-B.P1, e de 09/05/2012, proferido no processo n.º 311/08.7JFLSB.P2, do Tribunal da Relação de Lisboa de 20/06/2013, proferido no processo n.º 1746/05.2TJLSB.L1-8, e de 18/01/2011, proferido no processo n.º 3142/09.3PBFUN-A.L1-5, e do Tribunal da Relação de Coimbra de 03/10/2012, proferido no processo n.º 84/11.6JAGRD-A.C1, todos pesquisáveis na base de dados da DGSI).

Ora, rememorando aqui o texto da norma objeto, o n.º 2 do artigo 78.º do Decreto n.º 426/XII, observamos prever este que: «[o]s oficiais de informações do SIS e do SIED podem, para efeitos do disposto na alínea *c*) do n.º 2 do artigo 4.º, e no seu exclusivo âmbito, aceder a informação bancária, a informação fiscal, a dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou **para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização**, sempre que sejam necessários, adequados e proporcionais, numa sociedade democrática, para cumprimento das atribuições legais dos serviços de informações, mediante a autorização prévia e obrigatória da Comissão de Controlo Prévio, na sequência de pedido devidamente fundamentado» (ênfase acrescentado

aqui). Tratam-se, inequivocamente, de *dados de tráfego*, na referida classificação, não só pelo rótulo formal que o legislador lhes atribui, mas — decididamente — pela natureza da informação em causa, descrita por referência à dinâmica exterior, envolvente, de uma concreta comunicação (a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, o equipamento de telecomunicações e a sua localização).

9.2 — Note-se que a proteção do sigilo das comunicações pela Constituição não se limita aos *dados de conteúdo*, abrangendo igualmente os *dados de tráfego*. Nesse sentido, J. J. Gomes Canotilho e Vital Moreira, em nota ao artigo 34.º da CRP, salientam que «[a] garantia do sigilo abrange não apenas o conteúdo da correspondência, mas o 'tráfego' como tal (espécie, hora, duração, intensidade de utilização)» (*CRP. Constituição da República Portuguesa Anotada,* vol. I, 4.ª ed., Coimbra, 2007, p. 544). Por sua vez, Jorge Miranda e Rui Medeiros afirmam que «[...] é possível perceber que a intenção da Constituição é oferecer proteção ao tráfego de informação escrita, desenhada ou falada, entre dois ou mais destinatários definidos [...]» e «[...] essa proteção, especialmente nos modernos meios de comunicação, é ainda constitucionalmente garantida às circunstâncias em que se realizam as comunicações. Nesses termos, estão também protegidos os dados relativos aos meios de comunicação usados, à hora da sua utilização, à duração da sua utilização, ao local da sua utilização ou à identidade dos seus utilizadores» (*Constituição da República Portuguesa Anotada,* t. I, 2.ª ed., Coimbra, 2010, pp. 772 e 774).

Este Tribunal também aproximou a proteção dos *dados de tráfego* à concedida aos *dados de conteúdo*. Sobre a matéria, tomou posição no já citado Acórdão n.º 486/2009:

> «[...]
> O sigilo das telecomunicações, garantido nos termos do artigo 34.º, n.º 1, da Constituição, abrange não só o conteúdo das comunicações mas também o tráfego como tal [...]. 'O que está em causa é assegurar o livre desenvolvimento da personalidade de cada um através da troca à distância, de informações, notícias, pensamentos e opiniões, à margem da devassa da publicidade' (Costa Andrade, em 'Bruscamente no verão passado...', ano 137.º, n.º 3951, julho-agosto 2008, p. 339). A privacidade da comunicação, como corolário da reserva da intimidade da vida privada, abrange não apenas a proibição de interferência, em tempo real, de uma chamada telefónica, como também a impossibilidade do ulterior acesso de terceiros a elementos que revelem as condições factuais em que decorreu uma comunicação (v., neste sentido, Nicolas Gonzales-Cuellar Serrano, em 'Garantías constitucionales de la persucución penal en el entorno digital', in *Prueba e Processo Penal (Análisis especial de la prueba prohibida en el sistema español e en el derecho comparado*), pp. 171-174, da edição de 2008, da *Tirant lo Blanch*). Efetivamente, num Estado de Direito democrático, assiste a qualquer cidadão o direito de telefonar quando e para quem quiser com a mesma privacidade que se confere ao conteúdo da sua conversa.
> [...]»

Todavia, a aproximação da proteção dos *dados de tráfego* àquela que se concede aos *dados de conteúdo* não esconde uma evidência que se impõe intuitivamente: é diversa a afetação da reserva da intimidade da vida privada na recolha ou interceção de *dados de base*, de *dados de tráfego* ou de *dados de conteúdo*. Nesta classificação/enumeração sequencial esconde-se uma inegável progressão de intensidade.

As apontadas diferenças não são, claro está, irrelevantes para a consideração, no presente contexto, das duas situações.

Desde logo, permitem colocar a proteção dos *dados de base* num plano inteiramente distinto dos outros dois. Como se assinalou no Acórdão n.º 486/2009:

> «[...]
> O mesmo raciocínio [*sobre os dados de tráfego*] não vale para os elementos ou dados de base, já que, conforme assinala Costa Andrade, 'a pertinência dos dados à categoria e ao regime das telecomunicações pressupõe, em qualquer caso, a sua vinculação a uma concreta e efetiva comunicação — ao menos tentada/falhada — entre pessoas' [...]. Na verdade, por exemplo, a mera identificação do titular de um número de telefone fixo ou móvel, mesmo quando confidencial, surge com uma autonomia e com uma instrumentalidade relativamente às eventuais comunicações e, por isso mesmo, não pertence ao sigilo das telecomunicações, nem beneficia das garantias concedidas ao conteúdo das comunicações e aos elementos de tráfego gerados pelas comunicações propriamente ditas (v., neste sentido, Costa Andrade, em 'Comentário Conimbricense do Código Penal', Parte Especial, t. III, pp. 797-798, da edição de 2001, da Coimbra Editora). A mesma falta de tutela constitucional no plano do sigilo das telecomunicações valerá para os dados de localização celular que não pressuponham qualquer ato de comunicação, bastando para o efeito que o telemóvel esteja em posição de *stand by,* isto é, ligado e apto para receber chamadas (v., neste sentido, Costa Andrade, em 'Bruscamente no verão passado..., ano 137.º, n.º 3951, julho-agosto 2008, p. 341).
> [...]»

Daí que os tribunais superiores da jurisdição comum tenham vindo a conferir um tratamento diverso, no sentido de uma menor proteção — *rectius*, uma menos acentuada intangibilidade —, aos *dados de base*, colocando-os no plano das demais informações sujeitas a segredo profissional, nos termos do artigo 135.º do CPP (cf. os Acórdãos do Tribunal da Relação de Lisboa de 19/06/2014, proferido no processo n.º 1695/09.5PJLSB.L1-9, de 20/06/2013, proferido no processo n.º 1746/05.2TJLSB.L1-8, e de 18/01/2011, proferido no processo n.º 3142/09.3PBFUN-A.L1-5, todos disponíveis na base de dados da DGSI).

As apontadas diferenças não esgotam a sua relevância na distinção entre os *dados de base* e os demais dados decorrentes do serviço de telecomunicações. Elas estendem-se à distinção entre os *dados de tráfego* e os *dados de conteúdo*. Sendo verdade que, como atrás se concluiu, a Constituição aproxima estes no sentido de ambos encontrarem acolhimento no artigo 34.º da CRP, mas tal não significa que lhes imponha, necessariamente, um tratamento rigorosamente idêntico. Tal nota distintiva não passou despercebida — e constitui um elemento importante a reter — ao Tribunal Constitucional no Acórdão n.º 486/2009, embora ali não tenha sido desenvolvida, por não interferir com a decisão. Com efeito, observou-se neste aresto:

> «[...]
> Aqui chegados, importa, portanto, concluir que os dados da faturação detalhada e os dados da localização

celular que fornecem a posição geográfica do equipamento móvel com base em atos de comunicação, na medida em que são tratados para permitir a transmissão das comunicações, são dados de tráfego respeitantes às telecomunicações e, portanto, encontram-se abrangidos pela proteção constitucional conferida ao sigilo das telecomunicações. **Outra coisa será o diferente grau de ofensa que o acesso a estes dados reveste para os direitos e liberdades protegidos pelo sigilo das telecomunicações, relativamente às 'escutas telefónicas', quer pela menor informação que revelam, quer pelo facto de não se tratar de um método oculto de obtenção de prova, o que tem suscitado a interrogação sobre se esse acesso deve estar sujeito aos mesmíssimos pressupostos** (v., Mouraz Lopes, em 'Escutas telefónicas: Seis teses e uma conclusão', na *Revista do Ministério Público,* ano 26.º, n.º 104, p. 143).

[...]» (ênfase acrescentado).

Também no Acórdão do Supremo Tribunal de Justiça de 29/04/2010, proferido no processo n.º 128/05.0JDLSB-A.S1 (disponível na base de dados da DGSI), a propósito da identidade de questões apreciadas, tendo em vista aferir a viabilidade de um recurso extraordinário, se assinalou, designadamente, o seguinte:

«[...]

Vê-se assim que, à partida, os factos são diferentes desde logo quanto aos meios de prova que estão em causa. Localização de telefone celular e registo de dados de tráfego no acórdão recorrido, e escutas telefónicas no acórdão fundamento. Ora, o grau de intromissão na privacidade da pessoa alvo destas medidas é muito diverso, como bem diferente é o contributo que as medidas aqui contrapostas podem dar, como prova indiciária.

[...]»

A principal razão pela qual terá de ser diferente o tratamento final a conceder aos *dados de tráfego*, face aos *dados de conteúdo*, é fácil de compreender: sabendo que as restrições legais permitidas pelo artigo 34.º da CRP estão sempre sujeitas ao princípio da proporcionalidade (neste sentido, cf. Jorge Miranda e Rui Medeiros, *Constituição da República Portuguesa Anotada,* cit., t. I, p. 774), é por demais evidente que qualquer ponderação de proporcionalidade tem, necessariamente, de considerar, em um dos pratos da balança, a intensidade da lesão, e que, consequentemente, quanto menor a lesão, maior é o leque de atividades que podem ser consideradas legitimadas pela aferição de proporcionalidade.

Esta diferença é importante, designadamente, para compreender que, como melhor se analisará adiante, as posições deste Tribunal sobre a proporcionalidade das restrições de direitos a propósito das escutas telefónicas (dos *dados de conteúdo*), designadamente nos Acórdãos n.os 426/05 e 4/06, não são imediata e automaticamente transponíveis, por ser relevante a falta de uma total identidade de razão, para a recolha individualizada, *caso a caso* — e é o que aqui está em causa —, de *dados de tráfego*.

10 — Aqui chegados, importa enfrentar o obstáculo da letra do n.º 4 do artigo 34.º da CRP, ao referir-se à «matéria de processo criminal», reconduzido à seguinte questão: a norma constitucional impede o acesso a dados de tráfego pelos serviços de informações, por não se tratar, ali, de um processo criminal?

Já articulámos neste texto a atividade de produção de informações — por referência à ideia de *defesa administrativa da Constituição* — com a atividade de adjetivação penal, referenciando àquela um sentido e intencionalidade preambulares desta (da adjetivação penal), estabelecendo, pois, uma articulação temática entre as duas atividades, em termos que nos permitirão, agora, dar sentido e enfrentar as consequências de uma relação de complementaridade, na respetiva referenciação à área temática de intervenção dos Serviços de Informações. Estamos em crer, aliás, ser essa referenciação que dá sentido, no quadro de um Estado de direito democrático, à função de produção de informações na área da segurança interna.

Assim — e formulamos aqui, tão-somente, um ponto de partida argumentativo —, parece a letra do preceito (o artigo 34.º, n.º 4, da CRP), à superfície, ser clara no sentido de restringir a possibilidade de acesso aos dados de comunicações — incluindo, pois, como se deixou afirmado, os *dados de tráfego* — ao âmbito do processo criminal, *tout court*.

No entanto, tendo presente que a letra da lei — de qualquer lei, obviamente também a lei constitucional, que é, paradigmaticamente, uma lei interpretativamente aberta — é o primeiro passo na complexa tarefa de a interpretar, mas não simultaneamente o derradeiro passo nesse sentido (artigo 9.º, n.º 1, do Código Civil), poderá então o seu sentido literal sofrer ajustamentos reclamados por outras considerações (sistemáticas, desde logo, sem perder de vista a concreta realidade social que reclama a aplicação da norma). Recorrendo às palavras de Karl Engisch (*Introdução ao Pensamento Jurídico*, tradução de J. Batista Machado, 10.ª ed., Lisboa, 2008, pp. 336 e ss.), diríamos: «[q]ue se passa aqui? Se se considera claro o 'teor verbal' como um limite absoluto da interpretação, já não se trata aqui certamente de interpretação — nem sequer de uma interpretação frouxamente vinculada, enquanto se entenda que esta pressupõe um teor verbal ambíguo (plurissignificativo) e se afasta do sentido vocabular mais imediato e aparente, na direção de um mais distante. Mas as coisas já se apresentam de outra forma se entendermos os conceitos de interpretação 'restritiva' e 'extensiva' no sentido de que, através destes modos de interpretação, se faz vingar a genuína vontade ou a verdadeira valoração de interesses do legislador. Sendo assim, então talvez pudéssemos falar [...] de uma interpretação teleológica restritiva [...]». Trata-se de uma «[...] espécie de 'retificação da lei', que guarda fidelidade à posição tomada pelo legislador, ao seu querer, ao escopo que persegue, e apenas quebra os limites do sentido literal [...]», distinguindo-se da «[...] insurreição contra o legislador por amor da transcendente ideia de Direito» (Autor e *ob. cit.,* p. 338). No fundo, trata-se de afirmar uma «obediência pensante», na célebre e feliz expressão de Heck.

Temos, assim, de questionar se, atento o quadro já traçado de evolução normativa e de contexto histórico do artigo 34.º da CRP, ao lado do qual colocaremos a sede constitucional conferida à função de produção de informações (aos Serviços de Informações), a fidelidade ao sentido querido pelo legislador constitucional, atualizado por referência à realidade social de 2015, reclama ou não um ajustamento — uma redução — da proibição literal contida no n.º 4 daquele artigo. No caso, precisamente, uma *redução teleológica*, procurando responder a uma lacuna oculta: «[qualificamos] de lacuna 'oculta' o caso em que uma regra legal, contra o seu sentido literal, mas de acordo com a teleologia imanente à lei, precisa de uma restrição que não está contida no texto legal. A integração de uma tal

lacuna efetua-se acrescentando a restrição que é requerida em conformidade com o sentido. Visto que com isso a regra contida na lei, concebida demasiado amplamente segundo o seu sentido literal, se reconduz e é reduzida ao âmbito de aplicação que lhe corresponde segundo o fim da regulação ou a conexão de sentido da lei, falamos de uma 'redução teleológica'» (Karl Larenz, *Metodologia da Ciência do Direito*, tradução portuguesa da 6.ª edição alemã por José Lamego, 5.ª ed., Lisboa, 2009, pp. 555/556), sendo que «[...] a analogia, a resolução com base num princípio achado pela via da generalização de uma regra e a redução teleológica representam uma correção do, em parte demasiado estrito, em parte demasiado amplo, teor literal da lei, conforme à *ratio legis* e à teleologia própria da lei; representam, por conseguinte, um 'desenvolvimento do Direito imanente à lei'. De vez em quando, uma tal correção do teor literal da lei ocorre ainda de outro modo. Os casos em que o teor literal demasiado estrito é ampliado, sem que por isso se trate de uma analogia, podem denominar-se [...] de casos de 'extensão teleológica'. A seu lado hão de colocar-se aqueles casos em que o teor literal, em si contraditório, de uma disposição é retificado pela jurisprudência de acordo com o seu escopo» (Autor e *ob. cit.,* p. 564).

A resposta à questão em análise não prescinde de algumas observações.

10.1 — A primeira prende-se com o que poderíamos chamar de *geografia sistemática* dos Serviços dedicados à função de produção de informações e do processo criminal. Tratam-se de dois sistemas — de duas áreas da atividade do Estado — que, face ao que vai dito supra não podem, com propriedade, dizer-se enraizados em diferentes lugares, realidades e funções, respondendo a preocupações radicalmente — e sublinhamos o advérbio: *radicalmente* — diversas, no mais amplo e complexo sistema de segurança e justiça.

Na verdade, se o SIRP tem como finalidade assegurar, através dos dois Serviços de Informações que o integram, no estreito respeito da Constituição e da lei, a produção de informações necessárias à salvaguarda da segurança interna e externa, da independência e interesses nacionais e da unidade e integridade do Estado (artigo 2.º do Decreto n.º 426/XII) e se desenvolve atividades de recolha, processamento, exploração e difusão de informações necessárias à salvaguarda da independência nacional, dos interesses nacionais e da segurança interna e externa do Estado Português, informações que contribuam para garantir as condições de segurança dos cidadãos, bem como o pleno funcionamento das instituições democráticas, no respeito pela legalidade, informações adequadas a prevenir a sabotagem, a espionagem, o terrorismo, e sua proliferação, a criminalidade altamente organizada de natureza transnacional e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido (artigo 44.º, n.º 2, do Decreto n.º 426/XII), sendo isto assim, dizíamos, forçoso é concluir, desde logo, que se posiciona, a atividade de produção de informações, no âmbito da tutela preventiva de bens jurídicos protegidos pelo Direito Penal, no sentido de referenciáveis a ele, bens estes instrumentalmente servidos pelo direito processual penal.

Não é isto o mesmo — é forçoso, desde já, dizê-lo — que fazer coincidir a sua atividade (a produção de informações) com a que se desenvolve no processo penal. O que aqui se afirma é uma relação de complementaridade, são conexões, não uma identidade, tanto mais que ao pessoal do SIRP é vedado exercer poderes, praticar atos ou desenvolver atividades do âmbito ou da competência específica dos tribunais, do Ministério Público ou das entidades com funções policiais (artigo 5.º, n.º 2, do Decreto n.º 426/XII).

Neste conspecto, salienta-se que o SIS é o *único* organismo incumbido da produção de informações que contribuam para a salvaguarda da segurança interna, do acompanhamento de fenómenos e da deteção de ameaças nos domínios da sabotagem, da espionagem, do terrorismo, e sua proliferação, do crime organizado transnacional e da prevenção da prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de Direito constitucionalmente estabelecido (artigo 56.º, n.º 1, do Decreto n.º 426/XII) e o SIED é o *único* organismo incumbido da produção de informações que contribuam para a salvaguarda da independência nacional, dos interesses nacionais e da segurança externa do Estado Português (artigo 57.º do Decreto n.º 426/XII). E, neste sentido, os *oficiais de informações* atuam, entre outros, no domínio da prevenção do terrorismo, da espionagem, da sabotagem e da criminalidade altamente organizada (artigo 74.º, n.º 1, do Decreto n.º 426/XII).

A atividade do SIRP é objeto, como já dissemos, de fiscalização externa especializada (*i*) do Conselho de Fiscalização do SIRP, composto por três cidadãos de reconhecida idoneidade, eleitos Assembleia da República; (*ii*) da Comissão de Fiscalização de Dados do SIRP, composta por *três magistrados do Ministério Público nomeados pelo Procurador-Geral da República*, com sede na Procuradoria-Geral da República; e, agora, (*iii*) da Comissão de Controlo Prévio, composta por *três magistrados judiciais, designados pelo Conselho Superior da Magistratura*, de entre juízes conselheiros do Supremo Tribunal de Justiça, com, pelo menos, três anos de serviço nessa qualidade (artigos 20., 21.º, 29.º e 35.º do Decreto n.º 426/XII).

A esta primeira nota — diríamos *estática* — acresce a mais importante *imagem dinâmica* dos serviços de informações, visto que a sua atividade passa, em boa medida, por reunir informações destinadas a *prevenir a ocorrência de factos previstos e punidos na lei penal*, designadamente em matéria de criminalidade *grave* e *altamente organizada*, informações essas que, para além de se destinarem aos decisores políticos competentes, são também destinadas — quando a matéria diga respeito à respetiva área de atuação — às entidades competentes de investigação criminal.

10.2 — Em face do exposto no ponto antecedente, a questão da *redução teleológica* pode agora ser equacionada através de duas opções interpretativas colocadas em alternativa: (*i*) aceitamos que o sentido literal do n.º 4 do artigo 34.º da CRP é completo e integralmente fiel à vontade do legislador, ainda que no confronto da recolha de *dados de tráfego* pelos serviços de informações, seja porque o legislador constitucional pensou nesta hipótese, seja porque, se a tivesse pensado, não a teria ressalvado e, nesse caso, a mencionada interferência nas comunicações não é permitida pela CRP; ou (*ii*) interpretamos o n.º 4 do artigo 34.º da CRP, através de uma *redução teleológica*, no sentido de que a recolha dos dados de tráfego no âmbito da atividade dos serviços de informações, por esta ser *conexa* com a (e logicamente antecedente à) do processo criminal, é permitida pela CRP.

Perante as mencionadas opções — alternativas —, afastamos a primeira, porquanto implicaria aceitar que o legislador constitucional quis (ou quereria) um corte de uma

peça essencial de um sistema complexo que pressupõe o trânsito de informações do SIRP para o âmbito do processo penal, quando necessário em função do tipo de informação em causa. De entre as informações que podem ser recolhidas, a respeitante aos dados de tráfego é essencial, designadamente para o estabelecimento de conexões entre pessoas (eventualmente, futuros suspeitos e, sendo caso disso, arguidos em processo penal). Essencial também para assegurar a boa construção e funcionamento do sistema de prevenção e investigação criminal. Em suma, negar a apontada redução teleológica é afirmar que o legislador constitucional preferiu (ou preferiria) não afetar o direito à reserva da intimidade da vida privada um pouco mais a montante do sistema processual penal (apesar de tudo, em termos não tão drásticos quanto aqueles que tal afetação pode atingir na investigação criminal), assim privando tal sistema de parte das informações centralmente relevantes para o seu bom funcionamento.

Por outro lado, o bem fundado da segunda opção, no sentido da apontada *redução teleológica*, revela-se não só *a contrario* pelas razões constantes do parágrafo antecedente como também afirmativamente por uma compatibilização mais harmoniosa entre os interesses da reserva da intimidade da vida privada — aqui mais direcionados ao *direito à autodeterminação informativa* (artigo 35.º da CRP) —, do bom funcionamento do sistema de prevenção criminal, na articulação deste com o processo criminal, e da defesa da ordem constitucional, sendo certo que a «inviolabilidade de princípio», contida no artigo 34.º da CRP deve entender-se limitada, como justamente apontam Jorge Miranda e Rui Medeiros, «[...] pela própria Constituição no seu todo, em especial pelo equilíbrio entre os diferentes direitos fundamentais, *maxime* o direito à vida ou à integridade física. Constata-se, desta forma, que o recorte do conceito de inviolabilidade utilizado no artigo 34.º deve ser aferido à luz de uma leitura sistemática da Constituição, e não através de uma leitura atomística do referido preceito» (*ob. cit.,* pp. 757/758).

11 — Tomada posição no sentido da admissibilidade, face ao disposto no artigo 34.º, n.º 4, da CRP, do acesso a dados de tráfego pelos Serviços de Informações, não se alcança ainda a resposta final sobre a conformidade à Lei Fundamental do artigo 78.º, n.º 2, do Decreto n.º 426/XII. Isto porque a citada norma não tolera toda e qualquer restrição do direito à reserva da intimidade da vida privada, mas apenas as que obedeçam «à ponderação do princípio da proporcionalidade» (Jorge Miranda e Rui Medeiros, *ob. cit.,* p. 774).

11.1 — É extensa, profunda e consistente a jurisprudência do Tribunal Constitucional sobre o princípio da proporcionalidade, *na vertente de proibição de excesso*, aqui relevante. Escreveu-se, sobre a matéria, no Acórdão n.º 187/2001:

> «[...]
> Embora tenha havido tentativas de ancorar o princípio de proporcionalidade em raízes mais antigas — ligadas, quer à *iustitia vindicativa,* quer à *iustitia distributiva* —, a ideia de subordinar o exercício do poder a uma exigência de proporcionalidade recebe acolhimento jurídico claro apenas a partir do iluminismo, no domínio penal e do direito administrativo de polícia, com a vinculação da administração a uma exigência de necessidade, transitando a partir daí para o direito constitucional.
>
> A ideia de proporcionalidade *lato sensu* representa, hoje, uma importante limitação ao exercício do poder público, servindo a garantia dos direitos e liberdades individuais (a aplicação às limitações a direitos fundamentais, enquanto 'limite da limitação' remonta, na verdade, pelo menos a Herbert Krüger, 'Die Einschränkung von Grundrechten nach dem Grundgesetz', *Deutsche Verwaltungsblätter,* 1950, pp. 628 e ss).
>
> [...]
>
> Também o Tribunal Constitucional português tem reconhecido e aplicado, em várias decisões, o princípio da proporcionalidade, aferindo frequentemente perante ele, quer normas penais incriminatórias — por exemplo, nos Acórdãos n.os 634/93 (inconstitucionalidade da punição como desertor daquele que, sendo tripulante de um navio e sem motivo justificado, o deixe partir para o mar sem embarcar, quando tal tripulante não desempenhe funções diretamente relacionadas com a manutenção, segurança e equipagem do mesmo navio), 274/98 (não inconstitucionalidade de norma que pune o não acatamento de ordem de demolição), publicados nos *ATC,* respetivamente vol. 26.º, pp. 205 e ss., e vol. 39.º, pp. 585 e ss. —, quer normas de outro tipo, que previam encargos ou limitações a direitos fundamentais — *v. g.,* os Acórdãos n.os 451/95 (inconstitucionalidade de norma que estabelece a impenhorabilidade total de bens anteriormente penhorados pelas repartições de finanças em execuções fiscais), 1182/96 (inconstitucionalidade de normas sobre custas nos tribunais tributários), 758/95 (inconstitucionalidade de norma que impede a participação pessoal, na assembleia geral dos bancos, e em certas condições, de acionistas que não disponham de 1/300 da soma dos votos possíveis), 176/2000 e 202/2000 (perda dos instrumentos do crime) e 484/00 (não inconstitucionalidade de norma que prevê o indeferimento tácito do pedido de legalização de obras), publicados respetivamente nos *ATC,* respetivamente, vol. 31.º, pp. 129 e ss., vol. 35.º, pp. 431 e ss., vol. 32.º, pp. 803 e ss., e *Diário da República,* 2.ª série, de 27 e 11 de outubro de 2000 e de 4 de janeiro de 2001).
>
> Relativamente às restrições a direitos, liberdades e garantias, a exigência de proporcionalidade resulta do artigo 18.º, n.º 2, da Constituição da República. Mas o princípio da proporcionalidade, enquanto princípio geral de limitação do poder público, pode ancorar-se no princípio geral do Estado de Direito. Impõem-se, na realidade, limites resultantes da avaliação da relação entre os fins e as medidas públicas, devendo o Estado-legislador e o Estado-administrador adequar a sua projetada ação aos fins pretendidos, e não configurar as medidas que tomam como desnecessária ou excessivamente restritivas.
>
> [...]»

A nossa Jurisprudência constitucional desdobra o princípio da proporcionalidade em três subprincípios. Continuando a citar o Acórdão n.º 187/2001:

> «[...]
> O princípio da proporcionalidade, em sentido lato, pode, além disso, desdobrar-se analiticamente em três exigências da relação entre as medidas e os fins prosseguidos: **a adequação** das medidas aos fins; **a necessidade ou exigibilidade** das medidas e a **proporcionalidade em sentido estrito**, ou 'justa medida'. Como se escreveu no citado Acórdão n.º 634/93, invocando a doutrina:
>
> 'o princípio da proporcionalidade desdobra-se em três subprincípios: princípio da adequação (as medidas

restritivas de direitos, liberdades e garantias devem revelar-se como um meio para a prossecução dos fins visados, com salvaguarda de outros direitos ou bens constitucionalmente protegidos); princípio da exigibilidade (essas medidas restritivas têm de ser exigidas para alcançar os fins em vista, por o legislador não dispor de outros meios menos restritivos para alcançar o mesmo desiderato); princípio da justa medida, ou proporcionalidade em sentido estrito (não poderão adotar-se medidas excessivas, desproporcionadas para alcançar os fins pretendidos).'

Pode dizer-se que a verificação da adequação se configura como a primeira (se a medida não for adequada, será logo violadora do princípio da proporcionalidade). Retomando o que se escreveu no referido Acórdão n.º 1182/96:

'Num primeiro momento perguntar-se-á se a medida legislativa em causa [...] é apropriada à prossecução do fim a ela subjacente.'

Num segundo momento, há que questionar a possibilidade de adoção de medidas menos intrusivas com os mesmos efeitos na prossecução do fim visado.

Como se disse no citado aresto:

''Seguidamente haverá que perguntar se essa opção, nos seus exatos termos, significou a 'menor desvantagem possível' para a posição jusfundamental decorrente do direito [de propriedade]. Aqui, equacionando-se se o legislador 'poderia ter adotado outro meio igualmente eficaz e menos desvantajoso para os cidadãos' [Gomes Canotilho, *Direito Constitucional,* 6.ª ed., Coimbra, 1993, pp. 382-383].''

É, porém, certo que medidas que sejam de considerar necessárias ou exigíveis não podem deixar de ser também adequadas (embora o inverso não seja verdadeiro). Assim, na prática, a verificação da necessidade ou exigibilidade resolve logo também a da adequação.

A verificação da necessidade ou exigibilidade pode envolver, por outro lado, uma avaliação *in concreto* da relação empírica entre as medidas e os seus previsíveis efeitos, à luz dos fins prosseguidos, para apurar a previsível maior ou menor consecução dos objetivos pretendidos, perante as alternativas disponíveis.

Por último, retira-se ainda do princípio de proporcionalidade um último critério, designado como proporcionalidade em sentido estrito ou critério de justa medida.

''Haverá, então, que pensar em termos de 'proporcionalidade em sentido restrito', questionando-se 'se o resultado obtido [...] é proporcional à carga coativa' que comporta'' (*ibidem*).

Trata-se, pois, de exigir que a intervenção, nos seus efeitos restritivos ou lesivos, se encontre numa relação 'calibrada' — de justa medida — com os fins prosseguidos, o que exige uma ponderação, graduação e correspondência dos efeitos e das medidas possíveis.

[...]»

Por fim, importa considerar os limites do controlo a realizar pelo Tribunal sobre o referido princípio, no âmbito da atividade legislativa, e continuamos a citar o Acórdão n.º 187/2001:

«[...]

Não pode contestar-se que o princípio da proporcionalidade, mesmo que originariamente relevante sobretudo no domínio do controlo da atividade administrativa, se aplica igualmente ao legislador. Dir-se-á mesmo — como o comprova a própria jurisprudência deste Tribunal — que o princípio da proporcionalidade cobra no controlo da atividade do legislador um dos seus significados mais importantes. Isto não tolhe, porém, que as exigências decorrentes do princípio se configurem de forma diversa para a atividade administrativa e legislativa — que, portanto, o princípio, e a sua prática aplicação jurisdicional, tenham um alcance diverso para o Estado-Administrador e para o Estado-Legislador.

Assim, enquanto a administração está vinculada à prossecução de finalidades estabelecidas, o legislador pode determinar, dentro do quadro constitucional, a finalidade visada com uma determinada medida. Por outro lado, é sabido que a determinação da relação entre uma determinada medida, ou as suas alternativas, e o grau de consecução de um determinado objetivo envolve, por vezes, avaliações complexas, no próprio plano empírico (social e económico). É de tal avaliação complexa que pode, porém, depender a resposta à questão de saber se uma medida é adequada a determinada finalidade. E também a ponderação suposta pela exigibilidade ou necessidade pode não dispensar essa avaliação.

Ora, não pode deixar de reconhecer-se ao legislador — diversamente da administração —, legitimado para tomar as medidas em questão e determinar as suas finalidades, uma 'prerrogativa de avaliação', como que um 'crédito de confiança', na apreciação, por vezes difícil e complexa, das relações empíricas entre o estado que é criado através de uma determinada medida e aquele que dela resulta e que considera correspondente, em maior ou menor medida, à consecução dos objetivos visados com a medida (que, como se disse, dentro dos quadros constitucionais, ele próprio também pode definir). Tal prerrogativa da competência do legislador na definição dos objetivos e nessa avaliação (com o referido 'crédito de confiança' — falando de um 'Vertrauensvorsprung', v. *Bodo Pieroth/Bernhard Schlink, Grundrechte. Staatsrecht II,* 14.ª ed., Heidelberg, 1998, n.os 282 e 287) afigura-se importante sobretudo em casos duvidosos, ou em que a relação medida-objetivo é social ou economicamente complexa, e a objetividade dos juízos que se podem fazer (ou suas hipotéticas alternativas) difícil de estabelecer.

Significa isto, pois, que, em casos destes, em princípio o Tribunal não deve substituir uma sua avaliação da relação, social e economicamente complexa, entre o teor e os efeitos das medidas, à que é efetuada pelo legislador, e que as controvérsias geradoras de dúvida sobre tal relação não devem, salvo erro manifesto de apreciação — como é, designadamente (mas não só), o caso de as medidas não serem sequer compatíveis com a finalidade prosseguida —, ser resolvidas contra a posição do legislador.

Contra isto não vale, evidentemente, o argumento de que, perante o caso concreto, e à luz do princípio da proporcionalidade, ou existe violação — e a decisão deve ser de inconstitucionalidade — ou não existe — e

a norma é constitucionalmente conforme. Tal objeção, segundo a qual apenas poderia existir 'uma resposta certa' do legislador, conduz a eliminar a liberdade de conformação legislativa, por lhe escapar o essencial: a própria averiguação jurisdicional da existência de uma inconstitucionalidade, por violação do princípio da proporcionalidade por uma determinada norma, depende justamente de se poder detetar um erro manifesto de apreciação da relação entre a medida e seus efeitos, pois aquém desse erro deve deixar-se na competência do legislador a avaliação de tal relação, social e economicamente complexa.

A diferenciação, nestes termos, da vinculação do legislador e da administração é, aliás, salientada na doutrina nacional e estrangeira (v., para esta, por todos, a obra por último citada) e acolhida na jurisprudência. Assim, escreveu-se recentemente no Acórdão n.º 484/00, citando doutrina nacional:

'O princípio do excesso [ou princípio da proporcionalidade] aplica-se a todas as espécies de atos dos poderes públicos. Vincula o legislador, a administração e a jurisdição. Observar-se-á apenas que o controlo judicial baseado no princípio da proporcionalidade não tem extensão e intensidade semelhantes consoante se trate de atos legislativos, de atos da administração ou de atos de jurisdição. Ao legislador (e, eventualmente, a certas entidades com competência regulamentar) é reconhecido um considerável espaço de conformação (liberdade de conformação) na ponderação dos bens quando edita uma nova regulação. Esta liberdade de conformação tem especial relevância ao discutir-se os requisitos da adequação dos meios e da proporcionalidade em sentido restrito. Isto justifica que perante o espaço de conformação do legislador, os tribunais se limitem a examinar se a regulação legislativa é manifestamente inadequada.' (assim, Gomes Canotilho, *Direito constitucional e teoria da constituição,* Coimbra, 1998, p. 264).

Ora, estando em causa a constitucionalidade de uma norma, é apenas a intervenção do legislador que tem de ser aferida — com os limites assinalados.

E tal posição é também a seguida por outras jurisdições que aplicam o princípio da proporcionalidade à atividade legislativa — v., a título ilustrativo, os Acórdãos do Tribunal de Justiça das Comunidades Europeias de 13 de novembro de 1990 (processo C-331/98, *Coletânea de Jurisprudência do Tribunal de Justiça,* 1990, p. I-4203), 12 de novembro de 1996 (processo C-84/94, caso 'tempo de trabalho', in *Coletânea cit.,* 1996, p. I-5755) e 13 de maio de 1997 (caso 'garantia de depósitos', processo C-233/94, na *Colect. cit.,* 1997, pp. I-2405), lendo-se no último destes arestos que, quando a situação é economicamente complexa, ao julgar a conformidade com o princípio da proporcionalidade, 'o Tribunal não pode substituir a apreciação do legislador comunitário pela sua própria apreciação. De resto, só pode censurar a opção normativa do legislador se esta for manifestamente errada ou se os inconvenientes daí resultantes para certos agentes económicos forem desproporcionados em relação às vantagens que apresenta.'.

[...]»

11.2 — Testando a norma do artigo 78.º, n.º 2, do Decreto n.º 426/XII face ao referido princípio, a primeira nota que se colhe — para além da legitimidade de princípio (***fim legítimo***) de uma intervenção legislativa consistente na alocação de meios de atuação aos Serviços de Informações, protagonistas de uma função do Estado que a Constituição expressamente refere — para além disto, dizíamos, colhe-se a ideia de uma manifesta **adequação** da medida legislativa à prossecução do fim a que se destina (obtenção de informações relevantes para a atividade dos Serviços integrados no SIRP). A obtenção de «dados de tráfego, de localização ou outros dados conexos das comunicações, necessários para identificar o assinante ou utilizador ou para encontrar e identificar a fonte, o destino, a data, a hora, a duração e o tipo de comunicação, bem como para identificar o equipamento de telecomunicações ou a sua localização» é manifestamente adequada — no contexto da atuação dos serviços de informações — ao funcionamento do ciclo de produção de informações, permitindo, designadamente, estabelecer a (essencial) conexão entre pessoas e lugares que aqueles Serviços tenham por carecidos de análise. Sublinhar-se-á aqui, relativamente ao fenómeno terrorista contemporâneo, enquanto ameaça bem presente nas sociedades dos nossos dias, o desenvolvimento deste em rede, através de conexões (contactos) entre pessoas em pontos geográficos afastados, em termos que tornam intuitiva, como matéria-prima informacional, a deteção e relacionação desses contactos.

A ***necessidade ou exigibilidade***, por sua vez, traduzida na impossibilidade de adoção de medidas menos intrusivas com os mesmos efeitos na prossecução do fim visado, também deve ter-se aqui por estabelecida, uma vez que aos Serviços de Informações será, hoje mais ainda do que até agora, imprescindível a recolha dos identificados *dados de tráfego*, precisamente para estabelecimento das apontadas conexões entre informações dispersas, em vista da formação de um quadro informacional coerente. Trata-se, basicamente, de propiciar acesso a elementos determinantes para a alimentação e regular constituição e funcionamento do *ciclo de produção de informações*. E é este um resultado que não poderia obter-se por via menos intrusiva, certamente inalcançável através dos vagos e imprecisos *dados de base*. Os instrumentos resultantes daquele n.º 2 traduzem, assim, a já assinalada «menor desvantagem possível» no (necessário) sacrifício de algo na esfera pessoal de reserva de intimidade, entendida como direito à autodeterminação informativa.

11.3 — É mais complexa, no entanto — desde já se adianta —, a verificação da **proporcionalidade em sentido estrito**. Para concluir no sentido da «justa medida» da solução legislativa, importa considerar: (*i*) a espécie de informação obtida; (*ii*) a escala da informação; (*iii*) o funcionamento das comissões de fiscalização; e, face ao quadro precedente, concluindo, (*iv*) o sentido das exigências de proporcionalidade.

A *espécie de informação* obtida é, como já se referiu, pela sua natureza, limitada (*dados de tráfego*) e, pese embora afete uma projeção da reserva da intimidade da vida privada, não afeta esse tipo de informação, longe disso, essa intimidade projetiva, com uma intensidade igual ou mesmo equivalente à afetada pela informação resultante dos próprios *dados de conteúdo*, que permanecem — é essa a opção do legislador português — inacessíveis aos Serviços de Informações.

Mais importante para apurar o sentido da proporcionalidade é, todavia, o que designamos pela *escala da informação*. Como já referimos, atualmente, o debate internacional sobre a privacidade das comunicações tem como principais alvos sistemas muito complexos, alguns deles já referidos

neste texto. Em tais casos, trata-se da recolha sistemática de informações, realizada em massa, com ténue ou sem qualquer circunscrição de pessoas, tempo e lugares, sem uma prévia verificação da utilidade concreta da grande maioria da informação recolhida, tendo em vista o seu tratamento posterior e assentando na expectativa da sua utilidade futura, para estabelecimento de conexões entre pessoas que venham a ser suspeitas de ameaçar ou de lesar os interesses do Estado. Tal recolha de informações é, na sua escala, absolutamente dissociada do que se prevê no artigo 78.º, n.º 2, do Decreto n.º 426/XII: tão-só, um acesso pontual, delimitado por circunstâncias concretas, que tem de ser previamente solicitado a uma comissão independente, alegando e justificando a necessidade, adequação e proporcionalidade do acesso, por referência às atribuições legais dos Serviços de Informações.

Por outro lado, como já se assinalou, a atividade do SIRP é fiscalizada por *três comissões independentes*, sendo que a sua atuação garante — especificamente a da *Comissão de Fiscalização de Dados do SIRP* — o apagamento dos dados que não interessam à atividade dos serviços, por serem ou terem deixado de ser úteis. Ademais — e é este um ponto de particular importância —, centrando a nossa atenção na *Comissão de Controlo Prévio*, à qual cabe *em exclusivo* autorizar o acesso aos *dados de tráfego*, é visível o esforço do legislador em encontrar um justo equilíbrio dos interesses em jogo. Tratando-se de uma comissão administrativa, não de um tribunal, a sua composição por magistrados judiciais visa importar para aquela Comissão uma particular cultura profissional de isenção, imparcialidade, independência e o saber, apurado pela longa experiência profissional, da aplicação do direito à luz dos princípios fundamentais do sistema jurídico, incluindo o da proporcionalidade. Aliás, é precisamente no n.º 2 do artigo 78.º do Decreto n.º 426/XII que repousa a chave do respeito pela proporcionalidade em cada concreta autorização a conceder, pois ali se prevê a aplicação do princípio, em cada adjetivação de pedidos de acesso formulados pelos Serviços de Informações.

Acresce que, considerando o momento de atuação do SIRP, o legislador terá sentido grande dificuldade, ou mesmo encontrado barreira intransponível, na construção de um controlo jurisdicional (isto é, propriamente, por um *tribunal*), num momento em que *não existe e poderá não vir a existir* processo judicial. E a solução que encontrou — que copia soluções existentes em diversos países da União Europeia, caso da Alemanha e do Reino Unido (cf. Carlos Ruiz Miguel, «Problemas Actuales del Derecho de los Servicios de Inteligência», in *Anuario de Derecho Constitucional Y Parlamentário*, ano 2003, n.º 15, p. 166) —, a solução encontrada, dizíamos, num compromisso possível com os interesses em jogo, consistiu na criação de uma comissão administrativa (mas de feição parajudicial) que, na maior medida possível, replicasse o sentido profundo do controlo que, na sua dimensão mais literal, o n.º 4 do artigo 34.º entrega aos tribunais. Precisamente a respeito da natureza de uma entidade de controlo do acesso aos *dados de tráfego*, salienta-se que o Acórdão, já referido neste texto, do Tribunal de Justiça no Caso *Digital Rights Ireland, Ltd* (C-293/12), decisão de 8 de abril de 2014 — que invalidou a Diretiva 2006/24/CE, 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 — este Acórdão, dizíamos, tomou posição expressa no sentido do controlo prévio não ter que assumir, necessariamente, natureza jurisdicional, apontando a necessidade de «[...] um controlo prévio efetuado por um órgão jurisdicional **ou por uma entidade administrativa independente cuja decisão vise limitar o acesso aos dados e a sua utilização ao estritamente necessário para se alcançar o objetivo prosseguido e ocorra na sequência de um pedido fundamentado** destas autoridades, apresentado no âmbito de **procedimentos de prevenção**, de deteção ou de uma ação penal [...]» (trecho do ponto 62 do Acórdão; destaque acrescentado), condições que o Decreto ora em apreciação, ao prever a *Comissão de Controlo Prévio* (e ao estabelecer os termos da respetiva atuação) assegura.

Por fim, não se esquecendo a profundidade com que o Tribunal tem entendido a necessidade de controlo da informação resultante da interceção de comunicações, não se pode deixar de notar que nem todas as exigências implicadas na realização de escutas (cf., designadamente, os Acórdãos do Tribunal n.os 426/2005 e 4/2006) fazem sentido quando apenas estão em causa os dados de tráfego. Ali, importa atentar no *conteúdo* das informações, para o mais rapidamente possível aferir da sua relevância, eliminando rapidamente o resultado lesivo (isto é, destruindo as escutas) na parte inútil, precisamente por respeito ao princípio da proporcionalidade, momentos e necessidades que não se reproduzem quando apenas estão em causa dados de tráfego.

Tudo visto e sopesado, afigura-se que a solução encontrada pelo legislador implica, usando o critério do Acórdão n.º 187/2001, efeitos restritivos ou lesivos que se apresentam, todavia, numa relação «calibrada» — de justa medida — com os fins prosseguidos, ponderando aqueles efeitos face às medidas possíveis, tudo à luz do reconhecimento e outorga ao legislador do «crédito de confiança» que lhe é devido.

12 — Aqui chegado, retomando as questões/dúvidas formuladas pelo Requerente no artigo 7.º do pedido de fiscalização, responder-lhes-ia nos seguintes termos: (1) à primeira questão — *deve o acesso aos metadados considerar-se uma ingerência nas telecomunicações para os efeitos previstos na norma constitucional?* — responderia que o acesso aos *dados de tráfego* pelos *oficiais de informações* do SIRP, nos termos do artigo 78.º, n.º 2, do Decreto n.º 426/XII, constitui uma ingerência nas telecomunicações, sendo esta, todavia, permitida pela norma do n.º 4 do artigo 34.º da CRP, interpretada, através de uma *redução teleológica*, por forma a incluir a atividade dos Serviços de Informações, ao lado da atividade de investigação criminal, na exceção à proibição de princípio ali consagrada; (2) à segunda questão — *pode considerar-se que a autorização prévia e obrigatória da Comissão de Controlo Prévio equivale ao controlo existente no processo criminal?* — responderia que a referida autorização da *Comissão de Controlo Prévio* representa um mecanismo de controlo concreto da necessidade, adequação e proporcionalidade da interceção de dados, que a Constituição impõe, e assume, no particular contexto da atuação do SIRP, um papel equivalente, por proximidade axiológica, ao do juiz no processo penal, o qual, nos concretos termos constantes do Decreto n.º 426/XII, entendo não contrariar as exigências da Lei Fundamental.

13 — São estas, no essencial, as razões que me conduzem a afirmar, contra o entendimento que fez vencimento, a conformidade constitucional da norma do n.º 2 do artigo 78.º do Decreto n.º 426/XII da Assembleia da República. — *José António Teles Pereira.*