MESTRADO EM DIREITO E SEGURANÇA

Dissertação de Mestrado

Do Acesso aos Dados de Telecomunicações e Internet pelos Serviços de Informações Portugueses

Autor: Tiago Miguel Martins Silva

Orientador: Professor Doutor José Fontes

Lisboa, 15 de setembro de 2018

MESTRADO EM DIREITO E SEGURANÇA

Dissertação de Mestrado

Do Acesso aos Dados de Telecomunicações e Internet pelos Serviços de Informações Portugueses

Autor: Tiago Miguel Martins Silva

Orientador: Professor Doutor José Fontes

Lisboa, 15 de setembro de 2018

"Filhos do Caos e da Noite, o erro e a dúvida são o nosso pão de cada dia, e parece que os apreciamos, visto que oramos para o pedir. Estamos […] onde já estavam os gregos, salvo que a complicação dos nossos fenómenos sociais faz que forçosamente observemos muito menos bem, e a nossa indisciplina mental que necessariamente raciocinemos muito pior. O espírito humano tem uma ânsia natural de conhecer; revela-o a criança insistentemente, e a criança – ser absurdo, sentimental e desamparado – é o tipo exato (perfeito) da humanidade".

(Fernando Pessoa - *O Outro Império*, s.d.)

"Amat Victoria Curam"

(Catullus, 1aC)

DECLARAÇÃO DE COMPROMISSO DE ANTIPLÁGIO

Declaro por minha honra que o trabalho que apresento é original e que todas as minhas citações estão devidamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Lisboa, 15 de setembro de 2018

_____

Tiago Silva

AGRADECIMENTOS

A concretização deste trabalho não seria possível sem o apoio incondicional do meu orientador, Professor Doutor José Fontes, a quem agradeço toda a atenção, disponibilidade e motivação. Demonstro o meu reconhecimento por me incentivar em prosseguir com este estudo, mesmo antes de ser meu orientador.

Um agradecimento especial ao Professor Doutor Jorge Bacelar Gouveia pela criação e direção do mestrado em Direito e Segurança, onde reúne um quadro Docente de excelência com o qual foi um prazer aprender.

Aos meus Pais, ao meu Irmão e à Patrícia, pelo carinho e amor com que me acompanham nesta e noutras jornadas da minha vida.

MODO DE CITAR E OUTROS ESCLARECIMENTOS

1. A presente dissertação foi redigida conforme as regras do novo acordo ortográfico.
2. As monografias são citadas com a referência ao autor, título, edição, local de publicação, editora, ano, página(s) e ISBN. No corpo da dissertação é feita referência ao autor, ano e página consultada.
3. As partes ou volumes e contribuições em monografias são citadas por referência ao(s) autor(es), título da parte ou do volume, título livro, autor(es) do livro, volume e/ou número, edição, local de edição, editora, ano, ISBN e página(s).
4. Nas obras ou artigos consultados na Internet é feita referência ao(s) autor(es), título do artigo, data da publicação, hiperligação de obtenção e respetiva data de consulta.
5. Optamos por não traduzir as transcrições de obras em língua estrangeira, não correndo o risco de perder a essência das palavras utilizadas pelo autor.

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

AA. VV. – Autores vários

Ac. – Acórdão

al. – Alínea

AR – Assembleia da República

Art./Art.os – Artigo/Artigos

CDFUE – Carta dos Direitos Fundamentais da União Europeia

CE – Conselho da Europa

cf. – Conforme

CFDSIRP – Comissão de Fiscalização de Dados do Sistema de Informações da República Portuguesa

CFSIRP – Conselho de Fiscalização do Sistema de Informações da República Portuguesa

CISMIL – Centro de Informações e Segurança Militares

CNCTR - *Comission Nationale de Controle des Techniques de Renseignement*

CNPD – Comissão Nacional de Proteção de Dados

CRP – Constituição da República Portuguesa

i.e. – Isto é

LOSIRP – Lei da Orgânica do Sistema de Informações da República Portuguesa – Lei n.º 9/2007, de 19 de fevereiro

LQSIRP – Lei-Quadro do Sistema de Informações da República Portuguesa – Lei n.º 30/84, de 5 de setembro

n.º/ n.os – Número / Números

ONU – Organização das Nações Unidas

op. Cit. – Obra já citada anteriormente do mesmo autor

OTAN – Organização do Tratado do Atlântico Norte

p. ex. – Por exemplo

p./pp. – Página/Páginas

para. – Parágrafo

SAPDOC – Sistema de Acesso ou Pedido de Dados aos Prestadores de Serviços de Comunicações Eletrónicas

SIED – Serviço de Informações Estratégicas de Defesa

SIEDM – Serviço de Informações Estratégicas de Defesa e Militares

SIM – Serviço de Informações Militares

SIRP – Sistema de Informações da República Portuguesa

SIS – Serviço de Informações e Segurança

ss. – Seguintes

STJ – Supremo Tribunal de Justiça

TC - Tribunal Constitucional

TEDH - Tribunal Europeu dos Direitos do Homem

TFUE – Tratado de Funcionamento da União Europeia

TJUE - Tribunal de Justiça da União Europeia

TUE – Tratado da União Europeia

UE – União Europeia

v. – Verificar

DECLARAÇÃO DE CONFORMIDADE DO NÚMERO DE CARACTERES

Declaro que o corpo da dissertação, incluindo espaços e notas, apresenta um total de 311.928 caracteres.

Declaro ainda que do Resumo constam 2.073 caracteres e do *Abstract* constam 1.938 caracteres, incluindo espaços.

Pelo que cumpre com o consignado no n.º 4 do artigo 7.º do Regulamento do Segundo Ciclo de Estudos conducente ao Grau de Mestre em Direito e Segurança (Regulamento n.º 402/2016, publicado no Diário da República, 2.ª série – n.º 80-26 de abril de 2016), na medida em que a dissertação de mestrado não pode exceder os 350.000 caracteres de texto.

Lisboa, 15 de setembro de 2018

_____

Tiago Silva

RESUMO

O Sistema de Informações da República Portuguesa (SIRP) é um órgão inserido na Administração Pública, sendo constituído pelo Serviço de Informações Estratégicas de Defesa (SIED) e pelo Serviço Informações de Segurança (SIS). Estes Serviços de Informações estão incumbidos da produção de informações necessárias à prevenção das ameaças à segurança interna e externa do Estado Português, entre outras tarefas. Até à criação recente da Lei Orgânica n.º 4/2017, de 25 de agosto, o acesso aos dados de telecomunicações e Internet constituía um meio de atuação vedado aos Serviços de Informações portugueses, num Mundo interconectado em que uma ameaça ao Estado democrático pode surgir tanto no seu interior como a partir do exterior.

A busca de paridade com a maioria dos serviços congéneres na utilização deste meio técnico para a produção de informações relevantes à defesa e segurança do Estado, de forma a garantir uma cooperação fluente e atendendo à sua importância na prossecução das adstritas competências do SIS e do SIED, devem ser acompanhadas de mecanismos de controlo e fiscalização que permitam salvaguardar equilibradamente os direitos, liberdades e garantias envolvidas.

Nesta dissertação discorremos sobre o progresso legislativo alcançado pela possibilidade dada aos Serviços de Informações Portugueses de acederem aos dados de telecomunicações e Internet na prossecução da sua honrosa missão, analisando igualmente o impacto do Acórdão n.º 403/2015 do Tribunal Constitucional. Visamos apresentar a significação dos dados em análise e a sua pertinência na prossecução da atividade do SIRP, bem como discorrer brevemente acerca das disposições legais comparativas com este meio de produção de informações ao dispor serviços de informações estrangeiros. Discorremos ainda sobre a evolução histórica do SIRP e os seus princípios regentes de atuação num contexto de liberdade e segurança. Por último, para além de verificarmos os mecanismos de fiscalização e controlo do SIRP, indagamos acerca da pertinência da adequação deste meio às finalidades a que se propõe.

PALAVRAS-CHAVE: Sistema de Informações da República Portuguesa | Produção de Informações | Dados de Telecomunicações e Internet | Segurança | Fiscalização

ABSTRACT

The Information System of the Portuguese Republic (SIRP) is inserted in public administration, being composed by Strategic Information Service of Defence (SIED) and the Security Information Service (SIS). These Intelligence Services are responsible for producing information necessary that may assist in prevent threats to the internal and external security of the Portuguese State, among other tasks. Until the recent creation of Organic Law 4/2017, of 25th August, access to telecommunications and Internet data was a prohibited means of operation of the Portuguese Intelligence Services, in an interconnected World in which a threat to the democratic State may arise both within as from the outside.

The search for parity with most of the similar services in the use of this technical resource for intelligence relevant to the defence and security of the State, guaranteeing a fluent cooperation, as well as its magnitude in the pursuit of the associated roles, must be accompanied by strict control and oversight mechanisms willing to balance rights, freedoms and guarantees involved.

In this dissertation we discuss the legislative progress achieved by the Portuguese Intelligence Services to access telecommunications and Internet data in the pursuit of their honourable mission, also analysing the impact of Judgement No. 403/2015 of the Constitutional Court. We aim to present the significance of the data under analysis and their relevance in the pursuit of the SIRP activity, as well as to briefly discuss the legal provisions related to this intelligence resource by foreign intelligence services. We also discuss the historical evolution of the SIRP and its governing principles of action in a freedom and security context. In addition to verifying the mechanisms of oversight and control of the SIRP, we inquire about the pertinence of the suitability of this legislative progress for the intended of purposes that it applies.

KEY WORDS: Information System of the Portuguese Republic | Intelligence | Telecommunications and Internet Data | Security | Oversight

INTRODUÇÃO

No âmbito do Mestrado em Direito e Segurança da Faculdade de Direito da Universidade Nova de Lisboa foi possível aprofundar uma visão multidimensional e ampla da Segurança, nas suas diferentes inserções e perspetivas. Consideramos de especial interesse a matéria lecionada na disciplina de "Produção de Informações". A partir desta unidade curricular abordou-se, principalmente, a teoria da produção de informações, bem como as normas, princípios e limites que regem a atuação dos Serviços de Informações.

Entendemos que continua a ser uma área pouco estudada academicamente e que carece de um maior envolvimento da sociedade civil, muito devido à necessidade de incrementar uma cultura de informações - principalmente, num país onde as repercussões de um período ditatorial se fazem sentir nesta matéria.

Os Serviços de Informações estão incumbidos de assegurar, no estrito respeito da Constituição e da lei, a produção de informações (ou *intelligence*, de acordo com a terminologia anglo-saxónica) necessárias à preservação da segurança interna e externa, bem como à independência e interesses nacionais e à unidade e integridade do Estado (Art. 2.º da Lei n.º 30/84, de 5 de setembro). O SIRP é um órgão da administração pública[1] que tem uma missão crucial no Estado de Direito democrático, já que os seus serviços previnem e detetam ações que podem colocar em perigo a segurança e o bem-estar do Estado em que nos relacionamos.

Por considerarmos uma matéria pertinente e recentemente discutida, optámos por discorrer sobre a Lei Orgânica n.º 4/2017, de 25 de agosto, que aprova e regula o procedimento especial do acesso a dados de telecomunicações e Internet (previamente armazenados por prestadores de serviços de comunicações eletrónicas) pelos Oficiais de informações do Serviço de Informações de Segurança (SIS) e do Serviço de Informações Estratégicas de Defesa (SIED).

[1] Segundo ALICE FEITEIRA (2015, p. 14), "À semelhança de outros domínios, a administração pública de segurança destina-se a prestar um serviço público. Este serviço é enquadrado na administração pública geral e prossegue as finalidades de segurança individual e colectiva, com um fim exclusivamente público".

Na abordagem deste progresso legislativo, não podemos deixar de percorrer os meandros até à sua criação, mormente o Acórdão do Tribunal Constitucional (TC) n.º 403/2015[2].

Procuramos, assim, fomentar uma reflexão crítica acerca da aplicação do instrumento de acesso aos dados de telecomunicações e Internet, retratando a sua significância na *arena* de atuação dos Serviços de Informações portugueses, no papel do SIS e do SIED. Desta forma, abordaremos os desígnios Segurança e Liberdade num Estado democrático, partindo do princípio que nos relacionamos num mundo em constante mudança, em que as decisões que tomamos hoje poderão ter um forte impacto no nosso futuro.

Não pretendemos neste estudo realizar uma análise histórica profunda das Informações em Portugal, pois não é este o escopo do estudo. Assim, retratamos uma análise atualista dos Serviços de Informações, tendo assente aquilo que são os mecanismos legais e normas instituídas que orientam o seu funcionamento.

Como questões de partida à investigação, cumpre-nos formular as seguintes: A Sociedade em Rede requer novas formas de combate às ameaças? Representa este meio de atuação do SIS e do SIED uma resposta política às inquietações sentidas pelos cidadãos? São realmente estas informações necessárias à prossecução das atribuições do SIRP? A ampliação dos meios de atuação dos Serviços de Informações significa um maior risco de cometimento de ilegalidades ou atuações arbitrárias, abusivas e incontroladas? Será escassa a transparência nesta atuação? Existe necessidade de reforçar e mobilizar a sociedade civil para alargar o debate público à atividade operada pelo SIRP, sobretudo relacionado com a importância da manutenção de um contexto securitário?

A partir deste estudo pretendemos responder, sobretudo, se existe a necessidade de os Serviços de Informações serem dotados desta ferramenta de produção de informações, na perspetiva de dever do Estado nas suas funções enquanto prestador de Segurança.

[2] Processo n.º 773/15.

Neste estudo, apresentamos uma perspetiva jurídica, onde são tidos em conta aspetos sociológicos que se consideram fundamentais para torná-lo mais completo. Integramos referências bibliográficas do panorama nacional que, apesar de escassas, permanecem atuais na sua essência e são fundamentais no estudo desta área da Segurança. Apresentamos fontes de direito no plano interno, internacional e da União Europeia, fazendo destaque a jurisprudência de relevo. Recorremos igualmente a bibliografia estrangeira, como artigos de diversos especialistas na área de *intelligence* e segurança, expondo assim diferentes perspetivas sobre as questões suscitadas no decurso da investigação.

No que concerne à estrutura capitular, optamos por organizar a apresentação do estudo da seguinte forma:

- No primeiro capítulo, começamos por introduzir, necessariamente, os Direitos Fundamentais mais pertinentes na "sociedade em rede" em que nos relacionamos, para partirmos para a apresentação de diferentes definições de dados de telecomunicações e explanar as potencialidades da sua utilização na produção de informações.

- No segundo capítulo, apresentamos uma breve referência a ordenamentos jurídicos estrangeiros em matéria de *intelligence*, mais concretamente no que concerne ao acesso aos dados de telecomunicações por serviços congéneres. Assim, aludimos à legislação que vigora no Reino Unido, França e Alemanha.

- Referenciamos a atividade do SIRP no seu plano orgânico e normativo, no capítulo III. Nesta seção, discorreremos, ainda que não extensivamente, pois não é este o objetivo da dissertação, sobre a evolução histórica do quadro jurídico-normativo e os princípios regentes da atuação dos Serviços de Informações em Portugal.

- Finalmente, abordamos o núcleo deste trabalho, centrando-nos no avanço metodológico de *intelligence* proporcionado pelo acesso pontual aos dados de telecomunicações e Internet. No capítulo IV aglutinamos inevitavelmente o Capítulo I com o Capítulo III, o que faz dele o mais extenso desta dissertação. Começamos por

indagar a atuação dos Serviços enquanto parte integrante na equação Liberdade e Segurança no plano do combate às ameaças ao Estado democrático. Assim, discorremos sobre a proteção de dados e o sigilo das telecomunicações, referindo o Ac. do Tribunal Constitucional n.º 403/2015, a importância da Fiscalização do SIRP no papel das entidades responsáveis, bem como o controlo judicial e a autorização prévia de acesso aos dados de tráfego prevista na Lei Orgânica n.º 4/2017, de 25 de agosto. Para encerrar esta secção, refletimos criticamente sobre a adequação deste meio às finalidades a que se propõe, ou seja, aferir se existe uma ponderação factual entre o acesso aos dados de telecomunicações e Internet e as necessidades sentidas na prossecução das missões do SIS e do SIED.

Entendemos que existe uma multiplicidade de riscos associados à utilização das tecnologias da comunicação à disposição do público em geral, da mesma forma que devemos considerar as ameaças à nossa segurança num determinado contexto espácio-temporal. Cada vez mais, as ameaças a que estamos sujeitos levam-nos a tomar decisões num curto espaço de tempo, conforme presenciamos nos recentes atentados terroristas, sentidos particularmente na Europa[3] - pelo que não podemos deixar de considerar a especial importância que os Serviços de Informações desempenham na manutenção do espaço securitário que partilhamos.

Pretendemos chegar à conclusão que competirá ao Estado proporcionar um contexto de segurança, onde os princípios de ação e objetivos das entidades competentes nesta matéria se rejam por um elevado grau direcionamento e certeza das finalidades a que se predispõem, permanecendo ao mesmo tempo conscientes do não comprometimento de direitos fundamentais dos cidadãos que neste contexto se

[3] Numa breve retrospetiva recente, assistimos a uma série de atentados terroristas perpetrados em solo Europeu. A 13 de novembro, em Paris um ataque coordenado que provocou a morte de 130 pessoas, onde maioria dos perpetradores eram de nacionalidade francesa ou belga, com ligações prévias a atividades de cariz terrorista; a 22 de março de 2016, com três ataques bombistas em Bruxelas, no aeroporto e no metro de Maalbeek, que provocaram a morte de 32 pessoas; a 14 de julho de 2016, quando um camião conduzido por um tunisino radicalizado com residência francesa atropelou uma multidão, em Nice e 19 de dezembro, quando pelo mesmo método de ataque, um camião entrou por um mercado de Natal em Berlim, matando 13 cidadãos; Londres, 22 de março de 2017, quando um carro atropelou 4 pessoas na ponte de Westminster que terminou com o esfaqueamento de um polícia; a 7 de abril do mesmo ano, quando um camião atropelou pedestres em Estocolmo, matando 5 pessoas; em Manchester, quando uma bomba explode em pleno concerto, a 22 de maio de 2017; os esfaqueamentos no *Borough Market*, a 3 de junho de 2017; mais tarde, a 17 de agosto de 2017 nas ruas de Barcelona, por meio de atropelamento resulta a morte de 14 pessoas.

relacionam. Desta forma, propomo-nos aferir se pela vigência de mecanismos de controlo e fiscalização do SIRP é viável limitar possíveis lesões aos bens jurídicos fundamentais que a Constituição pretende salvaguardar. Assim, procuramos demonstrar que ameaças como o terrorismo[4], espionagem e criminalidade altamente organizada[5] devem ser combatidas de forma sigilosa e com discrição, através da identificação atempada de fenómenos e tipologias de atuação, onde assume especial importância uma forte cooperação internacional - premissas que entendemos estarem ao alcance do SIRP, por via da consideração do responsável e equilibrado incremento das suas capacidades.

Por esta via, desejamos que este trabalho se torne num contributo da promoção do debate crítico, académico e social necessário acerca da atuação do SIRP, designadamente, no que concerne ao esclarecimento das suas missões e à clarificação dos meios de atuação à sua disposição no plano da sua constante atualização face às ameaças a que estamos sujeitos.

[4] Importa referir que o Relatório Anual de Segurança Interna (RASI, p. 70) referente a 2017 alertou para o facto de o terrorismo representar uma ameaça de classificação "moderada" para Portugal. O Relatório aponta que "não existe imunidade no que ao terrorismo diz respeito", já que "o nosso país enfrenta riscos potenciais semelhantes àqueles que impendem, atualmente, sobre o conjunto de países europeus". Contudo, realça que existe "a possibilidade do recurso ao território nacional como plataforma de trânsito ou apoio logístico para o recrutamento de jihadistas".

[5] Conforme informa JOSÉ MANUEL ANES (2010, p. 25), "a criminalidade organizada é certamente a mais nefasta das formas de crime e a que mais prejudica a sociedade em geral. A criminalidade, entendida como o conjunto dos crimes – ações humanas previstas e punidas por legislação penal – praticados num determinado espaço e período de tempo, à semelhança de outros fenómenos sociopolíticos, tem demonstrado seguir essas transformações".

I. OS DADOS DE TELECOMUNICAÇÕES E INTERNET

1. A Sociedade Interconectada e os Direitos Fundamentais

Na obra "Sociedade de Risco Mundial*",* ULRICH BECK (2015, p. 84) aborda a globalização do perigo do terrorismo, na medida em que este se manifesta maioritariamente como "globalização da expetativa de possíveis atentados terroristas em quase todos os lugares do mundo em qualquer momento", advertindo que, "esta expetativa possui consequências profundas para o direito, os militares, a liberdade, o quotidiano das pessoas, a estabilidade da ordem política em todo o mundo, uma vez que desfaz as garantias de segurança das instituições básicas dos Estados-nação"[6].

O fenómeno da globalização assume assim um importante papel no surgimento de atores internacionais, maioritariamente não estatais que, pela sua forma de atuar, promoveram uma alteração dos parâmetros de intervenção e resposta das autoridades públicas competentes, na procura de uma ordem internacional onde o fator incerteza predomina. Conforme enuncia JÚLIO PEREIRA (2012), temos vindo a assistir a uma mudança de paradigma, principalmente desde as duas últimas décadas do século passado, "pela passagem de um mundo tendencialmente bipolar para um mundo onde se multiplicam os atores globais, inclusive de natureza não estatal, configurando entre eles relacionamentos atípicos e obrigando à reformulação do conceito de política externa dos Estados". De alguma forma, a globalização fomenta a atuação destes atores, alterando "radicalmente os parâmetros de intervenção e resposta das

[6] Para ULRICK BECK (2015, p. 106), os novos riscos globais são detentores de três características: "1 – Deslocalização*:* as suas causas e efeitos não estão limitados a um local ou espaço geográfico, são, por princípio, omnipresentes; 2 – Imprevisibilidade – as suas consequências são, por princípio, incalculáveis; no fundo, são riscos «hipotéticos», baseando-se num desconhecimento produzido pelas ciências e num dissenso normativo; 3 – Não-compensabilidade: o espaço de segurança da Primeira Modernidade não excluía os danos (…) porém, estes eram passíveis de compensação, era possível anular (com recurso a dinheiro, etc.) os seus efeitos nocivos". Quanto ao carácter da imprevisibilidade, compreende que o risco "resulta da importância eminente da impossibilidade de saber". Contudo, "é preciso renovar, aprofundar e alargar simultaneamente as pretensões do Estado em termos de conhecimento, controlo e segurança" (p. 107).

autoridades públicas, confrontadas com desafios decorrentes de novas interações entre pessoas, empresas e Estados"[7].

No contexto da Estratégia Nacional de Combate ao Terrorismo, aprovada pela Resolução do Conselho de Ministros n.º 7-A/2015 de 20 de fevereiro, e dos desafios instalados pelas novas ameaças à segurança nacional, torna-se urgente o acesso a "meios operacionais consagrados pela primeira vez de modo transparente e expresso na lei positiva", com vista à proteção de um conjunto de garantias presentes na Carta dos Direitos Fundamentais da UE e na Convenção Europeia dos Direitos do Homem.

De acordo com a comunicação da Comissão Europeia a propósito da Agenda Europeia para a Segurança[8], "as ameaças estão a tornar-se cada vez mais diversificadas e internacionais, sendo de natureza cada vez mais transnacional e transetorial", algo que requer "uma resposta eficaz e coordenada a nível europeu". Neste sentido, é de relevar o facto de a Comissão Europeia observar que "todas as medidas em matéria de segurança têm de respeitar os princípios de necessidade, da proporcionalidade e da legalidade, bem como prever as devidas garantias de responsabilização e de recurso judicial", indo ao encontro do Art. 52.º, n.º 1 da CDFUE. A referida comunicação culmina com a necessidade de aproximação das dimensões interna e externa da segurança, sendo de especial relevo a referência associada à importância dos dados das comunicações, que "podem igualmente ser eficazes para a prevenção e a repressão do terrorismo e da criminalidade organizada"[9].

[7] O Ex-Secretário-Geral do SIRP atesta assim que a sociedade atual "é, portanto, caracterizada pela atomização dos agentes de ameaça e pela multiplicação exponencial da informação, que implica a dificuldade em destrinçar o essencial do acessório e em antecipar e desconstruir situações de desinformação, fatores que têm contribuído para a complexidade da atividade de *intelligence*, agravada pela diluição da distinção entre ameaça externa e interna".

[8] Tratando-se de uma agenda partilhada entre a União e os Estados-Membros na criação de um espaço de segurança interna da UE que exija uma resposta coordenada a nível europeu, com especial incidência em matérias como o terrorismo, a criminalidade organizada e a cibercriminalidade, onde a proteção dos cidadãos seja assegurada em plena conformidade com os direitos, liberdades e garantias fundamentais.

[9] A Agenda estabelece três prioridades de atuação, entre as quais, uma resposta forte da UE ao terrorismo e ao fenómeno dos combatentes terroristas estrangeiros, o combate à criminalidade transnacional grave e organizada e a cibercriminalidade – que exigem ação imediata, uma vez que se tratam de domínios claramente interligados de ameaças transnacionais.

No entanto, tal como denotam J. G. CANOTILHO & V. MOREIRA (2007), "O desenvolvimento dos meios tecnológicos e o crescente recurso a meios eletrónicos que deixam «pegadas eletrónicas» (movimentação de contas bancárias, comércio eletrónico, portagens eletrónicas, utilização da telefonia móvel, visita de sites na Internet, meios de videovigilância eletrónica, etc.) tornam cada vez mais importantes as garantias contra o tratamento e a utilização abusiva de dados pessoais informatizados". Neste relacionamento entre os cidadãos e os meios tecnológicos, apontam que existe uma tensão inquestionável entre vários direitos, liberdades e garantias (i.e., desenvolvimento da personalidade, dignidade da pessoa, intimidade da via privada)[10].

Segundo o Ac. do TC n.º 403/2015, que discorreremos mais aprofundadamente adiante, "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". Falamos de dados obtidos no âmbito da prestação de serviços de comunicações eletrónicas, ou seja, dos dados de comunicações eletrónicas.

As questões relacionadas com a vigilância e privacidade tornaram-se proeminentes nas "*information societies*" - fortemente dependentes das tecnologias eletrónicas, fomentadas desde de 1970. Desta forma, as tecnologias da informação e comunicação incrementaram não só o desenvolvimento destas sociedades, como incitaram o poder dos sistemas de vigilância das mesmas. Destacando outro período igualmente importante relacionado com a vigilância é de referir o início do século XXI, quando se incentivou a uma resposta internacional concertada ao terrorismo global[11].

É certo que ao longo dos últimos anos surgiram novas ameaças, com cada vez maior grau de complexidade e que determinam um reforço concertado das sinergias disponíveis ao seu combate, tornando a cooperação entre países cada vez mais

[10] v. *Constituição da República Portuguesa Anotada*, 2007, pp. 550.
[11] v. D. LYON - *Surveillance Power and Everyday Life*…, 2007.

importante. Cumpre referir que contribuiu para a alteração de paradigma um conjunto de acontecimentos que fomentaram o acesso a dados de tráfego, como os atentados terroristas de Madrid (2004) e Londres (2005). No combate ao terrorismo que se alastrava pela Europa, verificou-se a necessidade de aceder aos dados de tráfego para finalidades de investigação criminal, pelo que devemos considerar a Diretiva de 2006/24/CE, de 15 de março como "legislação de emergência"[12]. Esta Diretiva previa a obrigação dos fornecedores de serviços de comunicações eletrónicas conservarem determinados dados, com vista a garantir a disponibilidade destes para efeitos investigação, deteção e repressão de crimes graves (Art. 1.º, n.º 1)[13].

Por outro lado, descortinando a atuação dos Serviços de Informações, tal como salienta FERNANDO MARTINS (2010, p. 144), "a falta de cultura de segurança em Portugal tem conduzido à tendência de se considerar que Portugal não tem ameaças nem inimigos e, por isso, não são preocupantes, nem prioritárias, grandes medidas de segurança". Ainda assim, atente-se que "As diferentes ameaças, a sua correta classificação e a produção de Informações sobre isso, estão na base dos processos de decisão dos Governos, para que, possam ser implementados as devidas medidas de segurança". Nesta senda, SÓNIA REIS & M. BOTELHO DA SILVA (2007, p. 9), quanto à atuação dos Serviços de Informações portugueses, estes redundavam na impossibilidade de procederem a interceção de comunicações e respetiva gravação, fossem telefónicas ou realizadas através de outro meio técnico (designadamente por meio da Internet ou fax, bem como acederem à mera listagem de comunicações efetuadas), quando a generalidade dos serviços de informações europeus poderiam a eles recorrer[14].

O acesso de serviços do Estado aos dados de telecomunicações e Internet é sem dúvida um tema amplamente discutido na regulação europeia da Sociedade da

[12] Cf. D. Masseno - Será constitucional o regime de acesso aos "Dados de Tráfego?", 2010

[13] Segundo o Art. 2.º, n.º 2 da mesma Diretiva, esta retenção de dados seria aplicável aos dados de tráfego, aos dados de localização e dados conexos necessários para identificar o assinante ou o utilizador registado, salvaguardando desde logo neste número que a Diretiva não seria aplicável ao conteúdo das comunicações eletrónicas.

[14] Os autores apelam que atendendo ao contexto de ameaça atual, bem como à generalidade dos países europeus disporem desses meios de produção de informações, "seria de ponderar remover o limite constitucional do n.º 4 do Art. 34.º da Lei Fundamental, de modo a permitir-se a interceção de comunicações em condições cuidadosamente disciplinadas".

Informação: se por um lado desenvolvem a produção de informações, já que promovem uma atuação antecipada dos Serviços de Informações como primeira linha de defesa e segurança dos Estados, por outro, verifica-se a necessidade de salvaguardar direitos, liberdades e garantias.

Acompanhamos JORGE BACELAR GOUVEIA (1991, p. 701) quando reflete sobre as preocupações do Direito Constitucional substancialmente na preservação da liberdade e privacidade da pessoa relativamente ao uso da informática. Neste sentido repara que a "consagração de direitos fundamentais é inteiramente legitimada pelo perigo acrescido que a multiplicação da capacidade de memorização e processamento e a faculdade de interconexão de dados inerentes à sua utilização representam para esses valores".

Avançado ao nível da legislação, segundo o Art. 2.º do Tratado da União Europeia (TUE), "A União funda-se nos valores do respeito pela dignidade humana, da liberdade, da democracia, da igualdade, do Estado de direito e do respeito pelos direitos do Homem", princípio este que foi integrado na Constituição da República Portuguesa (CRP)[15]. O desígnio da segurança é desde logo alcançado no Art.º 9.º da CRP quando se estabelece que constituem tarefas fundamentais do Estado "Garantir a independência nacional e criar as condições políticas, económicas, sociais e culturais que a promovam"[16] e "Garantir os direitos e liberdades fundamentais e o respeito pelos princípios do Estado de Direito Democrático"[17].

Como adverte ALICE FEITEIRA (2015, p. 27), na senda dos complexos riscos e ameaças às democracias, afere-se um compromisso social de segurança que decorre de "uma dogmática construtiva, alicerçada nos valores da justiça, da segurança e da liberdade". Enfatiza assim que, "Ao nível da legitimidade da administração [da segurança] pode entender-se que os *pressupostos da democracia* determinam-se pelos níveis de opacidade *versus* transparência, pela definição de critérios de

[15] "As disposições dos tratados que regem a União Europeia e as normas emanadas das suas instituições, no exercício das respetivas competências, são aplicáveis na ordem interna, nos termos definidos pelo direito da União, com respeito pelos princípios fundamentais do Estado de direito democrático" (cf. Art. 8.º, n.º 4 da CRP).
[16] Alínea a) do Artigo 9.º da CRP.
[17] Alínea b) do Artigo 9.º da CRP.

legitimidade e de legitimação, em que se concretizam os procedimentos formais e materiais da "burocracia" administrativa da segurança, e pela natureza ontológica de um direito administrativo "blindado" pela tutela de valores e bens públicos como a segurança interna e externa e os interesses vitais do Estado".

2. Das Significações dos Dados de Telecomunicações e Internet

Antes de partirmos para a definição mais concreta de dados de tráfego, devemos começar por defini-los enquanto "dados pessoais". A alínea a) do Art. 2.º da Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro[18], delimita "dados pessoais" como "(…) qualquer informação relativa a uma pessoa singular identificada ou identificável; é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".

Para efeitos do Regulamento Geral de Proteção de Dados[19], que revogou a Diretiva 95/46/CE, de 24 de outubro, de acordo com o n.º 1 do Art. 4.º, trata-se de "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via telefónica ou a um dos mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular".

Circunscrevendo-nos aos dados resultantes das comunicações eletrónicas, decorre do Ac. do TC n.º 486/2009 (Processo n.º 4/09) a exposição de uma tríplice de dados inerentes aos processos de telecomunicações[20], considerando "…os dados

[18] Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
[19] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril.
[20] Por referência aos Pareceres Consultivos da Procuradoria-Geral da República n.º 16/94, votado em 24/06/1994, 16/94 – complementar, votado a 02/05/1996, 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 onde se constatou que "os elementos funcionais, desde logo, os dados de tráfego, na medida em que permitem a identificação ou identificabilidade da

relativos à conexão à rede, ditos dados de base; os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação e os dados gerados pela utilização da rede (p. ex., localização do utilizador, localização do destinatário, duração da utilização, data e hora, frequência), dados de tráfego; dados relativos ao conteúdo da comunicação ou da mensagem, dados de conteúdo". Verificando-se, mais tarde que o Tribunal Constitucional convocou a definição anteriormente explanada no Ac. do TC n.º 486/2009.

Na Convenção do Conselho da Europa sobre o Cibercrime[21], adotada em Budapeste em 23 de novembro de 2001, o termo "dados relativos ao tráfego" refere-se a "quaisquer dados informáticos relacionados com uma comunicação efectuada através de um sistema informático e produzidos por este enquanto elemento da cadeia de comunicação, contendo indicação da origem, do destino, do percurso, da hora, da data, do volume e da duração da comunicação, ou do tipo de serviço subjacente". A adaptação ao direito interno desta Convenção, que resultou na Lei n.º 109/2009, de 15 de setembro (conhecida como a Lei do Cibercrime), seguiu quase a mesma definição, constituindo dados de tráfego "os dados informáticos[22] relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo de serviço subjacente" (cf. al. c) do Art. 2.º). No Brasil existe uma definição de "Registro de Conexão"[23], de modo que se trata do "conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço de IP utilizado pelo terminal para o envio e recebimento de pacotes de dados, entre outras que permitam identificar o terminal de acesso utilizado".

comunicação (direção, destinatário, local, hora, duração), integram já elementos suficientemente relevantes da comunicação justificando a proteção do sigilo".

[21] Pela convicção dos Estados-Membros da "necessidade de prosseguir, com carácter prioritário, uma política criminal comum que vise proteger a sociedade da criminalidade no ciberespaço, nomeadamente através da adoção de legislação adequada e da melhoria da cooperação internacional" (Preâmbulo).

[22] Para efeitos da mesma Lei, consideram-se "Dados informáticos", "qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função" (al. b) do Art. 2.º).

[23] Assente no Art. 4.º XVII da Resolução n.º 164, de 28 de maio de 2013, que aprova o Regulamento do Serviço de Comunicações Multimídia.

A Diretiva 2002/58/CE, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas[24], define dados de tráfego como "quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos da facturação da mesma", de acordo com a al. b) do Art. 2.º. 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", bem como os que consistam no formato revestido em que a comunicação é enviada pela rede (considerando 15.º). Foram definidos, nos termos da al. c) do Art. 2.º, "dados de localização" como "quaisquer dados tratados numa rede de comunicações electrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações electrónicas publicamente disponível". Importa enfatizar o Art. 15.º, na medida em que foi reafirmada a possibilidade de retenção destes dados: ou seja, é confirmada a possibilidade de que "Os Estados-Membros podem adoptar medidas legislativas para restringir o âmbito dos direitos e obrigações previstos (…) sempre que essas restrições constituam uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional, a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas. […] Para o efeito, os Estados-Membros podem designadamente adoptar medidas legislativas prevendo que os dados sejam conservados durante um período limitado…".

No nosso ordenamento jurídico, os dados de tráfego são definidos no n.º 1, alínea d), do Art. 2.º da Lei n.º 41/2004, de 18 de agosto[25], como "quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos da facturação da mesma". O Art. 6.º da mesma Lei discorre especificamente sobre os "Dados de Tráfego". Assim, é

[24] Que revogou a Diretiva 97/66/CE (transposta pela Lei n.º 69/98, de 28 de outubro).
[25] Transposição da Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas.

permitindo às empresas que oferecem redes e ou serviços de comunicações eletrónicas o tratamento de dados necessários à faturação dos assinantes e ao pagamento de interligações, especificamente: "a) Número ou identificação, endereço e tipo de posto do assinante; b) Número total de unidades a cobrar para o período de contagem, bem como o tipo, hora de inicio e duração das chamadas efectuadas ou o volume de dados transmitidos; c) Data de chamada ou serviço e número chamado; d) Outras informações relativas a pagamentos, tais como pagamentos adiantados, pagamentos a prestações, cortes de ligação e avisos" (n.º 2).

A Diretiva 2006/24/CE, de 15 de março[26], que altera a Diretiva 2002/58/CE, estabeleceu no seu Art. 2.º, n.º 2, alínea a) que "dados" serão "os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou o utilizador".

Segundo a proposta de Lei que originou o Decreto n.º 426/XII[27], que discorreremos adiante, os dados de tráfego "dizem respeito a circunstâncias das comunicações, e não ao próprio conteúdo da comunicação". Nesta senda, é referido que os dados cujo tratamento se visava permitir ao SIRP se enquadravam no conceito de "dados sensíveis" no âmbito do Art. 7.º, n.º 1, da Lei de Proteção de Dados Pessoais, "dado o seu carácter especialmente intrusivo na privacidade alheia e considerando a própria natureza da informação, relacionada com a vida privada dos titulares dos dados a quem respeitam", segundo foi explanado no Parecer N.º 24/2017, da Comissão Nacional de Proteção de Dados (CNPD) sobre o Projeto de Lei n.º 480/XIII-2.ª do CDS-PP[28]. Em momento anterior, a CNPD já se havia

[26] Subjacente a uma reafirmação do Conselho da necessidade de aprovar com a maior brevidade possível medidas comuns relativas à conservação de dados de telecomunicações (10.º considerando), acompanhada da consideração do potencial dos dados de tráfego e dos dados de localização na investigação, deteção e repressão de infrações penais (11.º considerando).

[27] Relativo ao Regime jurídico do Sistema de Informações da República Portuguesa (revoga 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).

[28] Viria, por isso, a CNPD concluir que o "o projeto de lei em análise não vem obviar aos obstáculos constitucionais assinalados pelo Tribunal Constitucional, no Acórdão n.º 403/2015 […], uma vez que as soluções propostas visam, por um lado conferir aos SIRP atribuições quase-policias, manifestamente incompatíveis com o Art. 4.º, n.º 1, da Lei n.º 30/84 […], e, por outro lado, judicializar o processo de aquisição e acesso de informações, enquadrando-o num procedimento de autorização na dependência da seção penal do Supremo Tribunal de Justiça, pretendendo, com isso, insinuar uma natureza criminal (ou garantística) comparável à do processo penal, para, assim, legitimar o acesso a dados relativos às comunicações, o que se revela manifestamente insuficiente quando comparado com as garantias que o processo penal atribui ao

pronunciado no Parecer n.º 29/98, quando referiu que existe o mesmo sigilo da correspondência, no âmbito da proteção constitucional, uma vez que a norma "… abrange quer o denominado "tráfego" da comunicação quer o conteúdo desta".

Como é descrito no Parecer n.º 38/2017 da CNPD[29], sobre a Proposta de Lei n.º 79/XIII/2.ª (GOV), que aprova o regime especial de acesso a dados de base e a dados de tráfego[30] de comunicações eletrónicas pelo SIRP, "o simples acesso a um sitio na Internet implica o estabelecimento de uma comunicação entre o equipamento do utilizador da Internet e o sistema que disponibiliza o referido sítio, sendo certo que para o seu estabelecimento a prestadora dos serviços de comunicações eletrónicas recolhe informação relativa ao endereço de IP (*Internet Protocol*) que foi atribuído ao equipamento que o cidadão está a ligar-se (URL), a data e hora do acesso, a localização, etc. (…), trata-se de um conjunto alargado de informação relativa a uma pessoa singular identificada ou identificável no âmbito de uma comunicação e que revela muito da sua vida privada" (p. 8). Sobre a frequência do fluxo comunicacional importa atender ao facto do parecer enaltecer que "nos dias de hoje ocorrem comunicações mesmo quando o utilizador do equipamento de comunicação não o aciona direta e intencionalmente: as atualizações do correio eletrónico, que se realizem de x em x minutos, as mensagens que recebem nos chats, etc., o que significa que as comunicações são praticamente constantes, mesmo quando os cidadãos utilizadores dos equipamentos nada fazem". Assim, este Parecer concluiu que dado ao facto de as comunicações constituírem "um meio permanente e generalizado de interação (…) revelam múltiplas dimensões da vida privada e familiar, as normas que tutelam aquelas dimensões humanas fundamentais têm de ser interpretadas abrangendo, no seu âmbito de proteção, todos os meios de comunicação e todos os danos pessoais a eles referentes".

arguido, num todo coerente, materialmente robusto e procedimentalmente tipificado, estranho ao regime ora proposto".

[29] Antes da emissão deste parecer, a CNPD já se teria pronunciado sobre o Parecer n.º 24/2017, a propósito do Projeto de Lei n.º 480/XII-2.ª (CDS-PP) já referido anteriormente neste estudo.

[30]Na medida em que "…o tratamento destes dados permite identificar quem faz ou recebe chamadas (mesmo as falhadas), quem envia ou recebe SMS, MMS, correio eletrónico, quem acede à Internet e a que sítios na Internet, portanto permitindo conhecer aspetos da vida provada e familiar das pessoas: onde se encontram ou estiveram (o que é evidente quando transportem o telemóvel ligado), com que regularidade estabelecem os contactos, que sítios da Internet consultam, etc." (p. 2v.).

Conforme advoga SCHUSTER et al. (2017, p. 77) acerca da preponderância que estes dados assumem: "*Despite the fact that metadata, by definition, does not contain the content of a message, its combination and analysis can reveal an extraordinary amount of information. The application of novel data fusion, analysis and processing techniques that work on large amounts of structured and unstructured data from different sources, commonly called Big Data Analytics, allows to identify patterns and relations, and to draw conclusions about very intimate details on people's habits and associations*".

A utilização cada vez mais disseminada de aparelhos tecnológicos leva a que os "*metadata*" se reproduzam de forma massiva na nossa interação com os meios de comunicações à nossa disposição: "*Smart home appliances, telecare, autonomous cars, and of course smartphones are already available today. These generate massive amounts of data that is related to the human beings operating or using these environments*"[31].

O mesmo entendimento é dado por RON DEIBERT (2015, p.10), quando aponta que, "*We leave a trail of digital "exhaust" wherever we go. Data related to our personal lives are compounded by the numerous and growing Internet-connected sensors that permeate our technological environment. The term "Internet of Things" refers to the approximately 15 billion devices (phones, computers, cars, refrigerators, dishwashers, watches, even eyeglasses) that now connect to the Internet and to each other, producing trillions of ever-expanding data points. These data points create an ethereal layer of digital exhaust that circles the globe, forming, in essence, a digital stratosphere*".

O Ac. do TC n.º 403/2015 refere que os dados de tráfego discutidos são informação em si mesmos[32], na hipótese de permitirem o estabelecimento de "conexões entre pessoas e situações, tomando como ponto de partida a existência pretérita de uma determinada comunicação", desta forma, não se prevê uma

[31] SCHUSTER et al. (2017, p. 77) continuam referindo que "*The ability of deriving personal details from all communication metadata, not to mention snooping on the actual content of messages or private data, is raising severe concerns of privacy advocates, civil rights activists, politicians, technologists and citizens*".
[32] Em contraposição ao termo "metadados", definido pela ciência da computação como "dados sobre dados".

"extrapolação analítica realizada com base na existência dessa comunicação e das relações que ela indica, não com base no conteúdo da própria comunicação" (p. 8271 do Diário da República).

3. Da *Intelligence* à Potencialidade dos Dados de Telecomunicações e Internet

Acompanhamos o entendimento que a produção de informações se desenvolve através de "um *processo metodológico próprio"*, inerentemente "da cultura, das condições históricas, geográficas, políticas, económicas, sociais securitárias e de defesa de cada Estado"[33].

JOSÉ LUCENA (1991, p. 152) discorre acerca da importância das informações no estudo da ameaça[34]. Admite que as informações são definidas através de uma tríade de aceções: na aceção do "conhecimento"; na aceção do conjunto de "actividades" destinadas a obter esse conhecimento; e na aceção de "organização", por via à obtenção do conhecimento - através do desenvolvimento planeado e sistemático daquele conjunto de atividades.

Para JORGE SILVA CARVALHO (2009), substantivamente, "a actividade de informações consiste num processo especializado – através do qual certo tipo de informação é solicitada, recolhida/pesquisada recorrendo a meios específicos, analisada/processada e divulgada – que se traduz no trabalho sistemático desenvolvido no quadro de uma organização específica criada com o objectivo de atingir um produto final – o conhecimento específico necessário à tomada de decisões. Não é, pois, o mero plural de informação". Desta forma, entende que um serviço de informações deve seguir a sua atividade em "defesa dos interesses e na prossecução dos objectivos do Estado". Sublinhe-se que, para o efeito, deve antecipar ameaças, pela abordagem a "realidades e fenómenos que, na maioria dos casos, não constituem, ainda, ameaças à segurança nacional dos Estados".

[33] RUI PEREIRA & ALICE FEITEIRA. – *Serviços de Informações*, 2015, p. 340.
[34] Para aprofundar a temática do relacionamento entre as ameaças e a produção de informações, v. *Tipologia e Hierarquização das Ameaças, A importância das informações. Tipos de Sistemas de Informações*, in *Revista Nação e Defesa…".*

Nesta senda, RUI PEREIRA & ALICE FEITEIRA (2015) concretizam que "…a atividade de produção de informações, ou de *intelligence*, […] destina-se a municiar os decisores políticos, ou outros destinatários legítimos, de conhecimento que permita reduzir o nível de incerteza, pelo que requer uma forma estruturada de análise de informação disponível, que devidamente valorada e agregada, contribuirá para essa tomada de decisões".

Nas palavras de CARLOS RUIZ MIGUEL (2006, p. 11), a produção de informações poderá ser vista como "*Un instrumento cualificado para que la democracia pueda defenderse a sí misma es la existencia de servicios de inteligencia que puedan averiguar quienes son y qué propósitos tienen los enemigos de la democracia a fin de ser más eficazmente combatidos a través de las medidas expressamente previstas en la Constitución*".

A importância da recolha de informação consubstancia-se na sua transformação em "inteligência". É desde a segunda metade do século XX, e principalmente depois da queda do muro de Berlim (1989) que existiu uma clara introdução dos Serviços de Informações nas estruturas constitucionais dos Estados Democráticos. Os serviços de inteligência devem cumprir as suas funções constitucionais atribuídas, sendo que para o efeito, para além de serem capazes de obter informação, é essencial que sejam capazes de transformá-la em inteligência, promovendo desta forma a essência dos seus serviços no domínio do apoio à decisão do poder político. Mais tarde, após a Guerra Fria e depois do 11 de setembro, assistiu-se a um processo de recondicionamento dos destes serviços face às novas ameaças[35].

Como sintetiza ARMÉNIO MARQUES FERREIRA (2007), a produção de informações poderá ser traduzida num conjunto de "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

[35] M.ª VILLALOBOS - *El Control de los Servicios de Inteligencia en los Estados Democraticos*, 2008, p. 2.

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".

Acompanhamos assim RUI PEREIRA & ALICE FEITEIRA (2015, p. 341), na medida em que "…o ciclo de informações entendido como o processo de obtenção de dados, através da identificação de problemas e da definição de estratégias de pesquisa, de processamento, de interpretação, de avaliação e da difusão de informações, isto é de previsões fiáveis e seguras, destinadas ao consumidor final, não é estanque". Pelo que, "em razão da amplitude e diversidade dos desafios colocados ao Estados e aos cidadãos, impõe o recurso a métodos analíticos interdisciplinares, quanto à determinação de fontes, à aplicação de critérios analíticos, à definição de matrizes de decisão, à configuração de hipóteses competitivas, à cenarização, à comparação de dados, à aplicação de modelos matemáticos, designadamente no quadro domínio do cálculo de probabilidades, à definição de diagramas de influência e à avaliação, necessariamente subjetiva, resultante da interação do conhecimento de especialistas e analistas".

Do ponto de vista das suas atribuições, JOSÉ LUCENA (1991, p. 152) defende que "o esforço primordial e permanente dos sistemas de informações (…) será obviamente orientado no sentido de obter todo o conhecimento possível sobre as ameaças reais ou potenciais que põem ou podem vir a pôr em risco a consecução dos objetivos políticos concretos nacionais[36]". A jusante, o "esforço desenvolve-se não só em permanência, (…), mas também em fases sucessivas, tendo em vista a percepção das ameaças, a sua configuração e a avaliação da sua periculosidade e probabilidade de concretização para se aquilatar da dimensão de risco que tais ameaças comportam".

[36] J. LUCENA (1991, p. 153) acredita que as informações consistem "num persistente esforço para obter indícios de comportamentos coactivos enquadrados nos cenários concebidos, indícios que, devidamente analisados e interpretados, permitam definir o mais objectivamente possível o contorno da ameaça pelo conhecimento da sua origem e meios que utiliza, e pela dedução da sua motivação e da sua finalidade".

Segundo M.ª VILLALOBOS (2008, p. 2), caberá aos Serviços de Informações «*poner a disposición del ejecutivo un conjunto de información política, económica, científica, técnica y militar, debidamente contrastada, valorada e interpretada y capaz de orientar la acción de gobierno tanto en su proyección exterior como interio*r».

Para ALICE FEITEIRA (2015, p. 20), a atividade de *intelligence* do Estado de direito democrático apresenta uma "natureza específica", atuando ao nível da "produção de análise estratégica de forma a garantir aos Estados, ou a outras entidades legítimas, o acesso ao conhecimento, no sentido técnico de "informações", com a finalidade da tomada de decisão esclarecida que, em tese geral, sustenta a obtenção de vantagens competitivas no quadro do interesse nacional". Assim, podemos afirmar que a essência da inteligência dos serviços é baseada na sua capacidade de apoiar o decisor político a tomar decisões relativas à segurança e defesa do Estado (M.ª VILLALOBOS, 2008)[37]. Neste sentido, tal como revê C. RUIZ MIGUEL (2006)[38]: "*Todo estudio del régimen jurídico de los servicios de inteligencia debe hacer constar las premisas básicas o fundamentos que justifican la existencia de los mismos. Sólo un planteamiento correcto sobre el fundamento de los servicios de inteligência nos permite dar una respuesta coherente a los problemas que plantea el Derecho de los servicios de inteligencia y, entre ellos, la cuestión de cómo se deben organizar, qué competencias tienen y a qué controles se someten. Existen dos fundamentos para instaurar un servicio de inteligencia. Uno es «político», en virtud del cuál los servicios de inteligencia contribuyen a la mejor realización de ciertas tareas políticas como son la defensa militar, la seguridad política exterior (relaciones internacionales) y la seguridad política interior (defensa de la Constitución). El otro es «administrativo», según el cual este tipo de órganos sirven para conseguir «seguridad pública». Aunque la «política» permite encontrar una raíz común a los objetivos de defensa militar, relaciones internacionales y*

[37] Continua VILLALOBOS (2008, p. 2) referindo que "*Por eso, todos los Estados del mundo tienen necesidad de contar con unos servicios que faciliten la toma de decisiones en materias de política exterior y relaciones internacionales, y que en materias de política interior eviten situaciones que atenten contra la seguridad del Estado*".

[38] v. *Problemas actuales del derecho de los servicios de inteligencia*, in *Inteligencia Y Securidad I*, p. 50.

defensa de la Constitución, no parece posible encontrar un «meta-fundamento» común que englobe también el objetivo de conseguir «seguridad pública»".

Importa considerar no presente estudo o conhecimento transmitido por JÚLIO PEREIRA (2016), na medida em que lembra que "os serviços de informações podem dar um importante contributo em sede de investigação mas principalmente no domínio de prevenção criminal"[39]. Tal como referem SÓNIA REIS & MANUEL BOTELHO DA SILVA (2007, p. 9) a "missão nuclear das informações corresponde ao universo da segurança interna e externa e desenrola-se a montante da atividade de polícia e da atividade de investigação criminal, sem prejuízo de poderem existir serviços de informações que desempenhem simultaneamente algumas destas funções, o que não sucede entre nós". Desta forma, os autores acrescentam que a missão das informações em Portugal pode relacionar-se ainda com a "promoção de outros objetivos do Estado", para além dos usualmente associados, como o desenvolvimento económico – que contribui em determinada medida para a "preservação da ordem e tranquilidade públicas". Nesta senda, a atividade de informações deve procurar, fundamentalmente, potenciar as políticas públicas de segurança (legislativas ou administrativas) "com um conhecimento rigoroso da realidade que possibilite a sua formulação ótima, mas não se destina diretamente à investigação processual penal ou à manutenção da ordem pública".

A legitimação do contributo dado na prossecução da atividade dos Serviços de Informações pode estabelecer-se numa tríade de interesses[40], conforme apresentam RUI PEREIRA & ALICE FEITEIRA (2015): "i) interesses do Estado – (no domínio do exercício de poderes de soberania: diplomáticos, militares, e executivos) ii) interesses da comunidade – (na defesa dos valores de cidadania: direitos, liberdade e garantias e, em geral, dos valores constitucionalmente protegidos) – e, ainda, quando

[39] Sobre a compreensão da simbiose entre a produção de informações e investigação criminal: v. o contributo de JÚLIO PEREIRA - *Os Serviços de Informações e a Prevenção e Investigação Criminais*, in *Liber Amicorum* Manuel Simas Santos, 2016, p.799-814.

[40] Nesta senda, segundo ALICE FEITEIRA (2015, p. 21) importa averiguar se os agentes, funcionários e dirigentes dos serviços de informações, no respeito do poder hierárquico instituído detêm um poder discricionário: "ou seja, se podem fazer uso de critérios de escolha independentes dentro dos parâmetros de legalidade". Da mesma forma que, "a noção de *accountability*, essencialmente relacionada com a teoria democrática da acção pública no domínio da segurança, e, em particular, no âmbito da actividade dos serviços de informações tem de ser considerada".

assim é permitido: iii) de interesses privados (no âmbito da denominada inteligência competitiva, ou inteligência económica[41])".

Concisamente, a atividade de produção de informações baseia-se na "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"[42].

Nesta esteira, cumpre distinguir os diferentes tipos de informações com base na sua forma de obtenção: mais concretamente, as informações provenientes de fontes humanas são consideradas HUMINT (*Human Intelligence*), ou de meios técnicos, SIGINT (*Signals Intelligence*). Dentro da SIGINT podemos subdistinguir formas específicas, como IMINT (*Imagery Intelligence*), ELINT (*Electonics Intelligence*), COMINT (*Communications Intelligence*), entre outras. Assim, a utilização dos dados de telecomunicações para produção de informações insere-se no âmbito da COMINT.

Contextualizando, o Relatório da COMISSÃO DE VENEZA (2015, p. 8) concretiza:

> "*However, the most significant development (…) relates to signals intelligence. Signals intelligence or SIGINT is a collective term referring to means and methods for the interception and analysis of radio (including satellite and cellular phone) and cable-borne communications. Traditionally, signals intelligence was mainly used to obtain military (defence) intelligence and, secondarily, foreign or diplomatic intelligence. Thus, it was primarily the domain of military or*

[41] S. REIS & M. BOTELHO DA SILVA (2007, p. 1) apontam para o valor acrescentado das atribuições dos SIRP no desenvolvimento económico do país. Se por um lado o SIED pode explorar os mercados viáveis à exportação da produção das empresas Portuguesas, as fontes energéticas, o desenvolvimento da tecnologia e a preservação ambiental, o SIS poderá desenvolver estratégias contra a ameaça da espionagem, quer no âmbito económico ou investigação científica. Desta forma "a actuação dos Serviços de Informações não deve privilegiar interesses particulares de agentes económicos privados, cuidando antes de optimizar as condições gerais necessárias ao bom desempenho de agentes relevantes para a prossecução dos interesses nacionais".

[42] Acrescentando que a informação "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", cf. desenvolvido no Ac. do TC n.º 403/2015, p. 8270 do Diário da República, 1.ª série – N.º 182 – 17 de setembro de 2015.

> *external intelligence agencies. However, as a result of processes of globalization, together with the creation of the internet, the distinctions between internal and external security are no longer so clear cut. (…) As explained further in the next section, signals intelligence now has considerable impact on internal security and on the human rights of individuals*".

Na opinião de EDWARD FELTEN (2013, p. 7), através da sua estruturação, os "*metadata*" conseguem inevitavelmente ser reveladores de detalhes da vida pessoal de um cidadão. Explicita igualmente que a produção dos mesmos é inevitável muito pela utilização massificada dos meios de telecomunicação à disposição dos cidadãos[43]. Como caracteriza o Professor da *Princeton University*:

> "*Mobile phones are today ubiquitous, and their use necessarily requires reliance on a service provider to transmit telephone calls, text messages, and other data. These communications inevitably produce telephony metadata, which is created whenever a person places a call. There is no practical way to prevent the creation of telephony metadata, or to erase it after the fact. The only reliable way to avoid creating such metadata is to avoid telephonic communication altogether*".

Adverte para a possibilidade de o tratamento destes dados permitir a construção de um "s*ocial graph*", dando para o efeito alguns exemplos que merecem a nossa consideração:

> "*Metadata can identify our closest relationships. Two people in an intimate relationship may regularly call each other, often late in the evening. If those calls become less frequent or end altogether, metadata will tell us that the relationship has likely ended as well—and it will tell us when a new relationship gets underway. More generally, someone you speak to once a year is less likely to be a close friend than someone you*

[43] Continua defendendo a seguinte argumentação: "*Metadata can expose an extraordinary amount about our habits and activities. Calling patterns can reveal when we are awake and asleep; our religion, if a person regularly makes no calls on the Sabbath or makes a large number of calls on Christmas Day; our work habits and our social attitudes; the number of friends we have; and even our civil and political affiliations*" (p. 10).

> *talk to once a week. Analysis of metadata on this scale can reveal the network of individuals with whom we communicate—commonly called a social graph*" (p. 10).

A importância do acesso a estes dados é aferida, desde logo, através do artigo 3.º da Lei Orgânica n.º 4/2017, de 25 de agosto, quando atribui aos Oficiais de informações do SIS e do SIED a possibilidade de terem acesso a dados de base e de localização de equipamento para efeitos de "produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada e no seu exclusivo âmbito". Ou seja, a sua importância é aqui aferida pela magnitude das ameaças que a partir do seu acesso se visam combater.

Na exposição de motivos da Proposta de Lei n.º 345/XII/4.ª (GOV), depreendemos o alinhamento necessário dos Serviços de Informações nacionais com os seus congéneres, motivado, desde logo, pelo Conceito Estratégico de Defesa Nacional em vigor. Ou seja, "enquanto serviços públicos, com caraterísticas e objetivos muito específicos e responsabilidades que recaem no cerne das funções soberanas e inalienáveis do Estado de Direito constitucionalmente estabelecido, os serviços de informações portugueses evidenciam a subsidiariedade do seu planeamento estratégico aos alinhamentos, alianças e vetores globais da ação governativa, aos grandes desígnios nacionais e à política externa". Pelo que interessa debater a "convergência da condução das atividades do SIRP com as referências fundamentais de Portugal foi sufragada de forma inequívoca pelo Conceito Estratégico de Defesa Nacional, aprovado pela Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril, documento que enfatiza o papel das informações enquanto ativo estratégico de Portugal".

A potencialidade da utilização dos dados de telecomunicações e Internet favorece a cada vez mais necessária antecipação do Estado face a possíveis ameaças. Assim, JORGE SILVA CARVALHO (2009), a propósito da potencialidade da antecipação pela adequada atuação dos Serviços de Informações, adverte que "essa

antecipação é fundamentada pela necessidade de prevenção face à possibilidade de ocorrência de danos graves à segurança nacional, sendo sobretudo um instrumento de *prima ratio* do Estado, instrumento que permite intervir num primeiro momento, resguardando para um segundo a utilização progressiva dos instrumentos do seu poder coercivo, as Forças de Segurança, em sentido estrito, os órgãos de investigação criminal e as Forças Armadas, *ultima ratio* da segurança nacional".

II. A ATUAÇÃO DE SERVIÇOS DE INFORMAÇÕES CONGÉNERES EM MATÉRIA DE ACESSO AOS DADOS DE TELECOMUNICAÇÕES E INTERNET

De entre os Estados-Membros, existem pelo menos três que regulam fortemente as condições impostas da *Signals Intelligence*, sendo eles a França, a Alemanha e Reino Unido[44]. Assim, iremos discorrer seguidamente sobre a legislação destes três Estados europeus. A nossa escolha baseou-se, em primeiro lugar, pelo facto de os três países selecionados apresentarem mais bibliografia sobre a matéria, já que existe um robusto interesse pelo meio académico acerca do debate desta área de intervenção do Estado. O segundo facto de tratarmos apenas a legislação de três Estados, deveu-se obviamente a uma questão de economia de tempo e espaço de análise no decurso do estudo em apreço.

1. Reino Unido

O Reino Unido dispõe de três serviços de *intelligence*, o *Secret Intelligence Service* (*SIS*), também conhecido como *MI6 e* direcionado para o exterior, o *Government Communications Headquarters* (*GCHQ*), direcionado para a *SIGINT*, e o *Security Service*, conhecido comumente como *MI5*, direcionado para a produção de informações internas.

A produção de informações no Reino Unido é regulada pelo *Intelligence Services Act (ISA),* pelo *Human Rights Act* e pelo *Regulation of Investigatory Powers* Act (*RIPA*), sendo esta última a lei que regula os poderes das entidades públicas no âmbito da vigilância e investigação, bem como da interceção das comunicações.

Conforme temos vindo a assistir, o Reino Unido tem sofrido vários ataques terroristas ao longo dos últimos anos. Em 2015, após os atentados em Paris, o Primeiro-Ministro à data, David Cameron, apostava no investimento e intensificação das capacidades dos serviços de informações britânicos:

[44] Agência Europeia Direitos Fundamentais (2015, p. 22).

> "*The more we learn about what happened in Paris, the more it justifies the full-spectrum approach that we have discussed before in the House. When we are dealing with radicalised European Muslims, linked to ISIL in Syria and inspired by a poisonous narrative of extremism, we need an approach that covers the full range: military power, counter-terrorism expertise, and defeating the poisonous narrative that is the root cause of this evil… we will make a major additional investment in our world-class intelligence agencies*[45]*".*

De acordo com o Relatório Anual do "*Intelligence and Security Committee of Parliament*" de 2016-2017, a escala da ameaça terrorista que o Reino Unido enfrenta foi considerado sem precedentes, verificando-se um acréscimo em termos no número de investigações em curso e do número total dos indivíduos de interesse para os serviços de informaçções ("*individuals of interest*")[46].

De acordo com *Intelligence Services Act* (*ISA*) o SIS, sob a autoridade do Secretário de Estado, é incumbido de obter e fornecer informações sobre as ações ou intenções de pessoas que estão fora das Ilhas Britânicas; e desempenhar outras tarefas relacionadas com as ações ou intenções dessas pessoas (Art. 1, n.º 1). Por outro lado, o GCHQ tem como funções: monitorizar ou intercetar emissões eletromagnéticas, acústicas, entre outras, e qualquer equipamento que produza tais emissões e obter informações delas derivadas; bem como fornecer aconselhamento e assistência sobre matérias como linguagem utilizada para questões técnicas e criptografia. Tais funções devem ser exercidas de acordo com o interesse da segurança nacional, no interesse do bem-estar económico do Reino Unido e no apoio à prevenção ou deteção de criminalidade grave (cf. Art. 3.º).

Não existe no Reino Unido nenhum regime legislativo exclusivo que se detenha da interceção de comunicações. Pelo contrário, as leis e procedimentos instituídos

[45] *HOUSE OF COMMONS*, durante o *Daily Hansard: "Statement on G20 and the Paris attacks".*
[46] cf. ponto 22 do Relatório Anual (2016-2017). No âmbito do *Justice and Security Act* 2013 é exigível que o Comité faça um Relatório Anual ao Parlamento sobre o desempenho das suas funções. Esses relatórios são submetidos primeiramente ao Primeiro Ministro, que é obrigado a considerar, em consulta com o Comité para a Segurança e Justiça, se qualquer assunto deve ser excluído por interesse da segurança nacional.

variam de acordo com o corpo que requer a interceção, de acordo com o *RIPA*. O *RIPA* veio incrementar as capacidades do *ISA*, na medida em que estabelece processos de autorização distintos para efetivar garantias que se aplicam à interceção de comunicações (conteúdo das comunicações) e à interceção de dados de comunicações (dados de tráfego, etc.).

De acordo com Art.os 5.º e 81.º do *RIPA*, para que o Secretário de Estado possa autorizar um mandado de interceção de comunicações (e não de aquisição de dados de tráfego), ele deve ter em consideração se a medida é proporcional e necessária ao objetivo que se augura alcançar, tendo como finalidade a proteção dos interesses da segurança nacional, prevenção e deteção criminalidade grave, salvaguarda do bem-estar económico do Reino Unido dos atos ou intenções dos indivíduos fora das Ilhas Britânicas, ou dar efeito a um acordo mútuo internacional.

Por outro lado, o *RIPA* discorre sobre o acesso a "*communications data*" em determinadas circunstâncias, na medida em que os dados de comunicações não incluem o conteúdo de uma comunicação, mas as informações relacionadas com o uso de um serviço de comunicações. Pela leitura do regulamento, verificamos que os requisitos para obter uma autorização neste âmbito é menos rigorosa e a lista de organismos que podem solicitar esta autorização é mais vasta. Assim, de acordo com o Art. 22.º do *RIPA*, a obtenção destes dados é possível quando se trate de salvaguardar o interesse da segurança nacional; prevenir e detetar de criminalidade ou ameaças à ordem; defender o bem-estar económico do Reino Unido; atuar no interesse da segurança pública ou com o objetivo de proteger a saúde pública; de finalidades de acesso ou cobrança qualquer imposto, taxa ou outra imposição, contribuição ou encargo a pagar a um departamento governamental; e casos de emergência, de forma a impedir a morte, o ferimento ou alguns danos à saúde física ou mental da pessoas, ou a sua mitigação.

O segundo capítulo (parte I) do *RIPA* discorre sobre os poderes conferidos a autoridades públicas na aquisição dos dados de comunicações *("communications*

data[47]*").* Assim com o "*Code of Practise*" instituído pelo governo do Reino Unido[48] realça que:

> "*The term 'communications data' embraces the 'who', 'when', 'where', and 'how' of a communication but not the content, not what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication including text, audio and video. It can include the address on an envelope, the time and duration of a communication, the telephone number or email address of the originator and recipient, and sometimes the location of the device from which the communication was made. It can also include data relating to unsuccessful call attempts i.e. when the person being dialled does not answer the call, but where the network has been able to connect it successfully. It does not include data relating to an unconnected call i.e. when a call is placed, but the network is unable to carry it to its intended recipient. It covers electronic communications (not just voice telephony) and also includes postal services*" (p. 13).

O "*Code of Practise*" faz ainda referência ao princípio da necessidade, na medida em que: "*Necessity should be a short explanation of the event, the person and the communications data and how these three link together. The application must establish the link between the three aspects to be able to demonstrate the acquisition of communications data is necessary for the statutory purpose specified*" (p. 22), bem como ao princípio da proporcionalidade da medida adotada: "*This should include explaining how the level of intrusion is justified when taking into consideration the*

[47] De acordo com o Art. 21.º, n.º 4 do *RIPA, "communications data"* constituem: *"(a)any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted; (b)any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person— (i)of any postal service or telecommunications service; or (ii)in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system; (c)any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service".* Também os dados da forma de "*traffic data*" se encontram definidos no Art. 21.º, n.º 6 do RIPA.

[48] Home Office - *"Acquisition and Disclosure of Communications Data: Code of Practice", março de 2015.*

benefit the data will give to the investigation. This justification should include confirmation that relevant less intrusive investigations have already been undertaken where possible. For example, the subscriber details of a phone number may be obtainable from a phone book or other publically available sources[49]" (p. 23).

2. França

No caso Francês, de acordo com ME CÉCILE DOUTRIAUX (2014, p. 3), o sigilo da correspondência eletrónica só pode ser violado pela autoridade pública, em casos excecionais previstos na lei, dentro dos limites por ela fixados:

> "*Si des considérations de sécurité nationale peuvent affecter les garanties offertes aux citoyens par les lois nationales et internationales, la nécessité de combattre la criminalité terroriste ne saurait justifier que l'on étende indéfiniment les interceptions de sécurité et des limites sont posées pour éviter les abus. En effet, il ne peut être porté atteinte au secret des correspondances électroniques que par l'autorité publique, à titre exceptionnel, dans les seuls cas de nécessité d'intérêt public prévus par la loi et dans les limites fixées par celle-ci*".

O Gabinete do Primeiro-Ministro Francês demonstrou preocupação em regular de forma compreensiva e coerente o quadro legal de atuação dos serviços de inteligência, principalmente no contexto dos atentados de janeiro de 2015, perpetrados em França[50].

A França dispõe de seis serviços de *intelligence*: a *Direction générale de la sécurité extérieure (DGSE),* a *Direction du renseignement militaire (DRM)* e a *Direction de la protection et de la sécurité de la defense (DPSD)* – na dependência do Ministério da Defesa; enquanto que a *Cellule de traitement du renseignement et*

[49] Acrescendo ainda um exame da proporcionalidade da aplicação da medida, incluindo uma consideração dos direitos (em casos particulares, como a liberdade de expressão) do indivíduo e um equilíbrio destes direitos com o benefício que a medida possa trazer à investigação em curso.

[50] "*La France est l'une des dernières démocraties occidentales à ne pas disposer d'un cadre légal cohérent et complet pour régir l'action de ses services de renseignement. En juillet 2014, le Président de la République et le Gouvernement ont décidé de répondre à cette lacune par une loi spécifique. Les attentats perpétrés en France en janvier 2015 et l'intensité de la menace terroriste ont souligné l'importance et l'urgence de cette réponse*" (Dossier de presse, Conseil des ministres, p.7).

action contre les circuits financiers clandestins (TRACFIN) e a *Direction nationale du renseignement et des enquêtes douanières (DNRED*) se encontram na dependência do Ministério das Finanças; por último, sob a alçada do Ministério do Interior encontra-se a *Direction centrale du renseignement intérieur (DCRI).*

Em França existem várias agências de *intelligence*, conforme apresentamos, contudo, pelo menos as interceções de comunicações em grande escala são conduzidas maioritariamente pela Diretoria Geral de Segurança Externa (*Direction Générale de la Sécurité Extérieure*), sendo a informação produzida partilhada com os restantes Serviços de Informações do Estado francês.

A interceção das comunicações é prevista pela [51], adotada a junho de 2015, que veio alterar o *Code de la sécurité intérieure* (entre outra legislação), entrou em vigor a 3 de outubro de 2015, com a nomeação do *président de la Comission nationale de controle des techniques de renseignement (CNCTR)*[52].

O "Código da Segurança Interior" *(Code de la sécurité intérieure)* estatui desde logo no Art. L. 801-1 que "o respeito pela privacidade, em todos os seus componentes, incluindo o sigilo de correspondência, a proteção de dados pessoais e a inviolabilidade lar, é garantido por lei", sendo que "a autoridade pública só pode interferir com ela em casos de necessidade de interesse público previstos por lei, dentro dos limites estabelecidos pela lei e em conformidade com o princípio da proporcionalidade"[53].

---

[51] *LOI n° 2015-912 du 24 juillet 2015*. De acordo com a exposição de motivos *(Expose des Motifs)* desta lei*: "C'est pourquoi, rompant avec l'approche fragmentée qui a prévalu depuis un quart de siècle, le présent projet de loi relatif au renseignement vise, pour la première fois en France, à offrir un cadre légal général aux activités des services de renseignement, alliant détermination des principes, définition des echniques et renforcement du contrôle. Ce cadre juridique rassemble des dispositions préexistantes rénovées, notamment en matière d'interceptions des correspondances et d'accès administratif aux données de connexion, et des dispositions nouvelles, notamment en ce qui concerne certaines techniques de sonorisation de lieux, de captation de données ou de localisation en temps réel d'objets ou de personnes. En parallèle des contrôles administratifs internes et du contrôle parlementaire exercé par la délégation parlementaire au renseignement, le projet de loi confie à une autorité administrative indépendante et au Conseil d'Etat le soin d'exercer un contrôle strict sur la mise en œuvre des techniques autorisées*".

[52] De acordo com o Art. 26.º *"la présente loi entre en vigueur au lendemain de la publication au Journal officiel du décret nommant le président de la Commission nationale de contrôle des techniques de renseignement*".

[53] Tradução livre cf. o Art. L.801-1 "*Le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données personnelles et l'inviolabilité du domicile, est garanti*

No que concerne à autorização e implementação das técnicas de acesso aos dados de tráfego e Internet só podem ser decididas num conjunto de situações previstas, também elas elencadas no mesmo artigo. De entre as condições impostas, para além da implementação e autorização das técnicas de acesso apenas poderem provir de autoridade com competência para o fazer, também devem ser justificadas no âmbito das ameaças, riscos e interesses fundamentais da Nação, conforme mencionados no Art. L. 811-3[54], num estrito âmbito de proporcionalidade ("*Les atteintes qu'elles portent au respect de la vie privée sont proportionnées aux motifs invoques*").

O Art. L. 851-3 do *Code de la sécurité intérieure* prevê a possibilidade de se obrigar os prestadores de serviços de telecomunicações e Internet a estabelecerem automatismos de processamento de dados com base em parâmetros pré-definidos, de forma a detetar previamente uma possível ameaça terrorista. Estes automatismos são configurados através de algoritmos que funcionam como parâmetros de seleção[55].

Estes algoritmos não procuram diretamente a identificação dos utilizadores de equipamentos de telecomunicações, mas antes identificar "*informations ou documents",* respeitando princípio de proporcionalidade. A autorização para a aplicação destes algoritmos é dada pelo Primeiro-Ministro, depois de ouvida a *CNCTR,* que deverá fornecer ao decisor político uma opinião não vinculativa sobre

par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité".

[54] Assim, para o exercício das duas missões os serviços de informações franceses especializados podem usar as técnicas mencionas no Título V da mesma Lei ("*Des Techniques De Recueil De Renseignement Soumises A Autorisation*") para o acesso a dados sobre a defesa e promoção dos interesses fundamenais da Nação. Entre eles, "a independência nacional, a integridade territorial e defesa nacional; os principais interesses de política externa, a execução dos compromissos europeus e internacionais da França e a prevenção de todas as formas de interferência estrangeira; os principais interesses económicos, industriais e científicos da França; a prevenção do terrorismo; a prevenção de violência coletiva suscetível de comprometer seriamente a paz pública; a prevenção do crime organizado e da delinquência" (tradução livre).

[55] Segundo o Art. L. 851-3: "*I.- Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, il peut être imposé aux opérateurs et aux personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste*".

os algoritmos e os parâmetros selecionados – ao autorizar o algoritmo a aplicar, o acesso aos dados recolhidos é vigente durante dois meses[56].

A *CNCTR* tem a possibilidade de aceder amplamente e controlar diretamente os dados recolhidos e ao seu tratamento, sendo avisada de quaisquer modificações e ficando possibilitada de fazer recomendações. Imaginando que o algoritmo utilizado deteta uma ameaça terrorista, o Primeiro-Ministro poderá nesse momento autorizar a identificação dos utilizadores, depois de ouvida a *CNCTR*. Após sessenta dias, estes dados devem ser destruídos, exceto no caso de serem elementos que fundamentem a existência de uma ameaça terrorista conexionada com uma ou mais dos utilizadores em causa (de acordo com o Art. L. 851-3 do *Code de la sécurité intérieure*).

Devemos considerar ainda a *Loi No. 2015-1556*, de 30 de novembro de 2015, "*relative aux mesures de surveillance des communications électroniques internationale*", sobre a interceção de dados e correspondência eletrónica emitida ou recebida no estrangeiro.

De acordo com o Art. L.851-1 do *Code de la sécurité intérieure*, os dados de tráfego constituem a "informação ou documentos tratados ou armazenados pelas suas redes [dos prestadores de comunicações eletrónicas] ou serviços de comunicações eletrónicas, incluindo dados técnicos relativos à identificação de números digitais, assinatura ou ligação a serviços de comunicações eletrónicas, a identificação de todos os números de assinante ou de ligação de uma pessoa designada, a localização do equipamento terminal utilizado e a lista de números chamados e chamadores, a duração e a data das chamadas"[57].

Se no decorrer de uma interceção existir fundada suspeita que alguém que comunique com a pessoa previamente identificada e que também possa ser de interesse à interceção em curso, a Lei permitirá a extensão do acesso a dados destas pessoas (cf. decorre do *Code de la Securite Interieure*, Art. L.852-1)[58].

[56] Caso exista a necessidade de prorrogar o pedido, a *CNCTR* deve indicar o número de acessos a autorizar e a sua relevância para a prossecução das funções em causa (Art. L.851-3, IV).
[57] Tradução livre.
[58] Decorre do Art. L.851-2 que "*Lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des*

De acordo com o Art. L. 854-1, a monitorização de comunicações que sejam emitidas ou recebidas no exterior pode ser somente autorizada com a finalidade de defender e promover os interesses fundamentais da Nação, mencionados no já referido Art. L. 811-3.

O principal órgão de fiscalização desta atividade é a já referida *Commission Nationale de Contrôle des Techniques de Renseignement* (*CNCTR*), prevista no Título III do Livro VIII do *Code de la sécurité intérieure*, que veio substituir a *Comission nationale pour les interceptions de securité* (*CNCIS*)[59]. Importa referir que a CNCTR é composta por nove membros, incluindo dois senadores, e dois membros da Assembleia Nacional ("*Deux députés et deux sénateurs, désignés de manière à assurer une représentation pluraliste du Parlement*"), dois membros do Conselho de Estado (pelo menos com grau de Conselheiro de Estado, nomeados pelo Vice-Presidente do Conselho de Estado), dois magistrados do "*Cour de cassation*" (nomeados pelo presidente e pelo Ministério Público) e uma pessoa qualificada pelo seu conhecimento acerca de comunicações eletrónicas, nomeado sob proposta do presidente da "*l'Autorité de régulation des communications électroniques et des postes*"[60].

O requerimento de interceção das comunicações deve ser remetido ao *CNCTR*, que fornece a opinião sobre o pedido ao Primeiro-Ministro[61]. Em casos de extrema urgência e para os fins mencionados nos parágrafos 1.º, 4.º e 5.º do já referido Art. L. 811-3, o Primeiro-Ministro, ou um dos delegados mencionadas no Art. L. 821-4, podem excecionalmente emitir a autorização sem a opinião prévia da *CNCTR*, que deverá ser avisada o quanto antes (cf. o Art. L. 821-5 do *Code de la sécurité intérieure*).

informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes".

[59] Conforme decorre da Loi No. 2015-912, *du 24 juillet 2015 relative au renseignement*, Art. 21.º.

[60] cf. decorre do Art. L. 831-1.

[61] Decorre do Art. L. 821-3 que "*La demande est communiquée au président ou, à défaut, à l'un des membres de la Commission nationale de contrôle des techniques de renseignement parmi ceux mentionnés aux 2° et 3° de l'article L. 831-1, qui rend un avis au Premier ministre dans un délai de vingt-quatre heures. Si la demande est examinée par la formation restreinte ou par la formation plénière de la commission, le Premier ministre en est informé sans délai et l'avis est rendu dans un délai de soixante-douze heures*".

Ainda de acordo o Art. L. 821-4, a opinião do *CNCTR* não é vinculativa, mas sempre que o Primeiro-Ministro contrarie a Comissão e autorize determinado acesso, deve fundamentar a sua decisão à *CNCTR.*

3. Alemanha

O Acórdão *Weber Saravia* v. *Germany*[62] refere que "*In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed*".

A Alemanha, tal como Portugal mantém uma separação estrita entre serviços de *intelligence* e órgãos de polícia criminal. Uma separação mais estrita entre a polícia e os serviços de inteligência foi incrementada depois da II Grande Guerra, de forma a prevenir uma acumulação de esforços entre as atividades de ambos – sobretudo pela atuação da *Gestapo*.

Os Serviços de Informações alemães podem aceder, intercetar e solicitar dados de comunicações armazenados, sendo subordinados a determinados procedimentos instituídos por lei. Pelos meios que utilizam e funções que desempenham, estes serviços são sujeitos a apertados controlos de cariz administrativo e parlamentar, mormente órgãos parlamentares especializados e uma supervisão parlamentar geral.

O Governo alemão dispõe três Serviços de Informações, são eles o *Bundesamt für Verfassungsschutz – BfV* (Serviço Federal para a Proteção da Constituição), o *Militärische Abschirmdienst – MAD* (Serviço de Proteção Militar) e o *Bundesnachrichtendienst – BND* (Serviço Federal de Informações). A Lei Federal da

[62] N.º 54934/00, de 29 de junho de 2006 (parágrafo 95).

Proteção da Constituição ("*Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz*")[63] prevê a subordinação do "Serviço Federal para a Proteção da Constituição" (*BfV*) ao Ministério Federal Interior, impedindo que este seja dependente de qualquer departamento policial (§2, para. 1) - constituindo o seu principal objetivo a proteção da ordem democrática livre, bem como a existência e a segurança da Federação e dos países (§1, para.1). A Lei prevê ainda a obrigação do *BfV* cooperar com os restantes Serviços de Informações no sentido de proteger a Constituição (§1, para. 2). O Art. 3.º da referida Lei Federal discorre sobre as tarefas das autoridades de proteção da Constituição. Desde logo, estas autoridades têm como tarefa a recolha e análise de informações, em particular de informações fatuais e pessoais, notícias e documentos (§3, para. 1).

Na prossecução das suas missões o *BfV* está habilitado para, em casos individuais, solicitar dados de tráfego armazenados pelos serviços de telecomunicações para efeitos comerciais, tais como dados que permitam identificar o utilizador de um serviço de telecomunicação, as informações sobre o início e o fim da comunicação, bem como a extensão do respetivo uso de equipamento e informações sobre os serviços usados pelo utilizador (§8a, para 1. e para. 2).

O *Militärische Abschirmdienst* (*MAD)* encontra-se na dependência do Ministério Federal da Defesa, sendo as suas funções semelhantes ao já discorrido *BfV*. A Lei do Serviço de Proteção Militar (*Gesetz über den militärischen Abschirmdienst)*[64] apresenta como principais responsabilidades da *MAD* a recolha e análise de informações sobre os esforços anticonstitucionais e as atividades adversas dos serviços secretos, a interceção de informações para a avaliação da situação de segurança das forças alemãs e das forças aliadas, bem como fornecer avaliações de segurança e precauções técnicas relacionadas com a segurança na proteção de matérias classificadas (§1).

[63] Legislação atualizada disponível para consulta em https://www.gesetze-im-internet.de/bverfschg/BJNR029700990.html [consultada a 26/06/2018].
[64] Disponível e atualizada em https://www.gesetze-im-internet.de/madg/ [consultada pela última vez a 26/06/2018].

Por último, cabe referir o *Bundesnachrichtendienst* (*BND* - Serviço Federal de Informações)[65], que pertence à Chancelaria Federal (responsável pela sua coordenação e supervisão) e tem como tarefas a recolha e avaliação das informações sobre países estrangeiros de importância para a política externa e segurança da República Federal da Alemanha (§1). Este serviço de informações está autorizado a solicitar informações sobre correspondência postal ou de telecomunicações, recorrer a instituições financeiras, companhias aéreas e prestadores de serviços de Internet, bem como aceder às informações necessárias para o desempenho das suas funções, incluindo dados pessoais de todas as autoridades e inspeção de registos oficiais.

Após delinearmos os três serviços de informações alemães, e aproximando-nos do escopo da abordagem ao acesso aos dados de telecomunicações pelos mesmos, importa começar por referir que o Art. 10.º da Constituição Alemã estatui que a privacidade da correspondência, correio ou das telecomunicações é inviolável, na medida em que as restrições só podem ser impostas de acordo com a lei vigente. Se a restrição serve para proteger a ordem livre e democrática, ou a existência e segurança da federação alemã, ou de um estado alemão, a lei poderá estabelecer que a pessoa afetada não será informada da medida tomada. Estas restrições não se aplicam a comunicações externas, exceto se envolverem intervenientes de nacionalidade alemã.

Segundo o Tribunal Constitucional Federal Alemão (*Bundesverfassungsgericht*), o acesso aos dados de tráfego pode apenas acontecer caso o serviço de informações esteja autorizado a solicitar estes elementos, bem como apenas no caso de existir legislação que obrigue os prestadores de serviços de telecomunicações a ceder estes dados[66]. A lei das telecomunicações (*Telekommunikationsgesetz*), exige que os prestadores de serviços de telecomunicações cumpram imediatamente a solicitação dos serviços de informações.

[65] A organização, as tarefas e os poderes gerais do *BND* estão plasmados na *Gesetz über den Bundesnachrichtendienst*. Disponível em http://www.gesetze-im-internet.de/bndg/index.html [consultada a 26/06/2018].

[66] Decisão de 14 de julho de 1999 – 1 *BvR* 2226/94. Disponível em https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1999/07/rs19990714_1bvr22269 4en.html [Acedido a 26/06/2018].

Neste sentido, é permitido aos supramencionados serviços de informações acederem, intercetarem e solicitarem dados armazenados pelos prestadores de serviços de telecomunicações[67], por via da "Lei sobre a limitação do sigilo postal e de telecomunicações" (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*). De acordo com o Art. 1.º da desta Lei, o *BND* está habilitado para, no seguimento das atribuições, monitorizar e registar telecomunicações, abrir e inspecionar o correio sujeito a sigilo - encontrando-se subjugado ao controlo de uma comissão de supervisão parlamentar e por uma comissão especial (Comissão G-10).

Nem todas as atividades de SIGINT na Alemanha se encontram devidamente reguladas, contudo a "Lei do Serviço Federal de Informações"[68] estatui que estes serviços estão autorizados a coletar e avaliar as informações necessárias sobre países estrangeiros de importância para a política externa e de segurança para a República Federal da Alemanha, sendo que nestas informações estão incluídos os dados pessoais – e o seu processamento é regido pela mesma Lei (Art. 1.º, n.º 2).

Na Alemanha existe a Comissão G-10[69], composta por quatro membros dirigidos por um juiz com funções de presidência. O principal papel desta Comissão é implementar medidas de fiscalização relacionadas com a restrição do Art. 10.º da Constituição alemã - no âmbito da correspondência e sigilo das telecomunicações. Esta Comissão é então responsável pela autorização de pedidos de interceção de comunicações, verificando-se que tem também o poder de controlo dos acessos, não só no momento da recolha de informações, mas também ao longo do seu processamento e utilização das informações recolhidas para as finalidades que foram exigidas. O Ministro do Interior desempenha igualmente um papel importante na aceitação dos pedidos exigidos pelos Serviços de Informações, já que apenas

[67] As obrigações dos prestadores de serviços de telecomunicações estão previstas no Art. 2.º.

[68] Denominada; "*Gesetz über den Bundesnachrichtendienst*". Disponível para consulta em http://www.gesetze-im-internet.de/bndg/BJNR029790990.html [consultado pela última vez a 23/06/2018].

[69] Esta Comissão é composta por quatro membros ativos e quatro membros suplentes, que não precisam ser membros efetivos do parlamento. Já o presidente da Comissão do G 10 deve estar qualificado para servir como juiz, com a necessária formação académica e prática judicial, ao contrário dos comissários que não precisam de ser juízes. Assim, verifica-se uma lacuna, na medida em que não existe uma legitimidade política, por não se tratar de um órgão parlamentar, nem analisa com o rigor e escrutínio judicial as operações dos serviços de informações.

mediante a sua aprovação é que os mesmos são submetidos a uma decisão final por parte da Comissão G-10 (cf. Art. 15.º, n.º 6).

Algumas atividades de SIGINT não estão devidamente regulamentadas. A Lei do Serviço Federal de Informações incumbe o BND de recolher e analisar as informações necessárias para produção de inteligência estrangeira, que seja importante para a política externa e de segurança da República Federal da Alemanha[70] - ficando o *BND* possibilitado de executar operações SIGINT que envolvam dois países estrangeiros ou dentro de um único país estrangeiro, desde que o sinal intercetado não tenha conexão com a Alemanha. Esta atividade não se encontra assim ao abrigo da Lei da restrição da correspondência e das telecomunicações (Lei G-10), adotada em aplicação do n.º 2 do Art. 10.º da Constituição Alemã. Consequentemente, este método está fora das obrigações de fiscalização da Comissão G-10, onde vigora exclusivamente o controlo parlamentar.

A comumente denominada Lei G-10 (Lei da restrição da privacidade da correspondência e das telecomunicações) prevê as "restrições estratégicas" (*Strategische Beschränkungen*), que autoriza o *BND* a intercetar comunicações com origem ou destino da Alemanha (Seção 3 da Lei). De salientar que esta possibilidade é apenas permitida com a indicação de determinados seletores ou termos de pesquisa (*Suchbegriffe*), sendo estes seletores[71] que irão direcionar a recolha de elementos. Para além destes elementos, o *BND* deverá especificar igualmente qual a região/área de interesse e a percentagem de comunicações a intercetar (que não pode exceder os 20% da capacidade total das telecomunicações do canal) – segundo o Art. 10.º, n.º 4 da referida Lei.

[70] De acordo com o Art.ˢ 1, n.º 1 e 2.º, n.º 1 (*Gesetz über den Bundesnachrichtendienst*).
[71] Estes seletores podem ser números de telemóvel, endereços de *e-mail* ou determinadas palavras. A lista dos seletores é sujeita à análise prévia da Comissão G-10, que admite quais são admissíveis e necessários, sendo a respetiva lista válida por um período renovável de três meses.

III. DO SISTEMA DE INFORMAÇÕES DA REPÚBLICA PORTUGUESA

1. A Evolução histórica do quadro jurídico-normativo do SIRP e as suas atribuições

De forma a compreendermos o legado e razão das suas mutações, torna-se necessário discorrer, ainda que brevemente, acerca da evolução histórica do quadro jurídico-normativo do SIRP na suas diferentes asserções, limitações e potencialidades ao longo dos anos.

No caso português, podemos admitir que existiu uma depreciação dos Serviços de Informações fruto da imagem "repressiva e atentatória" conhecida no contexto do Estado Novo[72]. Neste senda, SÓNIA REIS & MANUEL BOTELHO DA SILVA (2007, p.3) contestam as atuações da Polícia de Vigilância e Defesa do Estado (PVDE, desde 1933), bem como posteriormente da Polícia Internacional de Defesa do Estado[73] (PIDE, criada em 1945) e da Direção-Geral de Segurança (conhecida como DGS, criada em 1969), que eram marcadas por ingerências grosseiras na privacidade dos cidadãos, detenções discricionárias, interrogatórios exaustivos, privações de liberdade e recurso a torturas – "procedimentos em geral fundados em motivos ideológicos e políticos e destituídos de fundamentação jurídica", atuando como "uma verdade polícia política". As atividades levadas a cabo por estas instituições procuravam sobremaneira o controlo dos opositores através de "funções efetivas francamente diversas dos atuais serviços de informações"[74].

[72] Num discurso histórico apresentado por D. VITKAUSKAS (1999, p. 3) "… *where a state was totalitarian, its leaders "knew how to rule with the help of secret police, but not with the secret ballot". A domestic security intelligence service in such a country was therefore a very important tool of the government, aimed at repression and control of its own citizens*".

[73] Cf. JORGE BACELAR GOUVEIA - *Os Serviços de Informações*…, 2013, p. 68: "Tudo de agrava ainda mais pela ideia de que a atividade da PIDE-DGS nem sequer era primordialmente de informações do Estado, mas fundamentalmente de controlo e de perseguição dos opositores do regime político de então".

[74] Cf. constatam S. REIS & M. BOTELHO DA SILVA (2007) sobre a panorama nacional, "os Serviços de Informações não só não desempenham funções policiais e de investigação criminal como também têm meios de atuação francamente restritos para o desempenho da sua atividade de estrita pesquisa e produção de informações". Algo que, segundo os autores, "trata-se de uma realidade que só se pode compreender à luz da História dos Serviços de Informações em Portugal" (p. 2).

No estrito quadro da CRP, apesar dos progressos legislativos que foram acontecendo, no período de 1976 até 1988, não existiu nenhuma norma constitucional que discorresse sobre os Serviços de Informações. Seria apenas em 1989, pela concretização da revisão constitucional, que existiram avanços no domínio dos Serviços de Informações e segredo de Estado[75], sob a referência ao "Regime dos serviços de informações" como matéria da reserva relativa de competência legislativa da Assembleia da República [Art. 168.º, n.º 2, al. r)] [76]. Mais tarde, pela revisão de 1997, deu-se a inclusão do "Regime do sistema de informações da República" na reserva absoluta de competência legislativa da Assembleia da República, sob a exigência de lei orgânica - cf. a al. q) do n.º 1 do Art. 164.º.

Desde a fundação legal do SIRP, em 1984, foram várias as alterações legislativas que têm caracterizado a atuação dos Serviços. Desde logo, a partir da publicação da Lei-Quadro n.º 30/84, de 5 de setembro, foram definidas as bases gerais do Sistema de Informações da República Portuguesa (Art. 1.º). Inicialmente, foram previstos três Serviços de Informações: o Serviço de Informações Estratégicas de Defesa (SIED); o Serviço de Informações Militares (SIM); e o Serviço de Informações de Segurança (SIS). Neste sentido, estabeleceram-se as regras relativas ao funcionamento, direção e controlo dos seus órgãos constituintes, de acordo com determinado curso de funcionamento e poder, bem como foi tida em conta a sua dependência tutelar e a sujeição a estruturas de fiscalização, com referência às suas missões, deveres e responsabilidades[77]. O SIRP era definido como uma estrutura de serviço público que tinha como objetivos a produção de informações necessárias à salvaguarda da independência nacional e à garantia da segurança interna - delimitados

[75] Sobre a matéria do Segredo de Estado, vide ARMÉNIO MARQUES FERREIRA, in *Enciclopédia de Direito e Segurança*, Coimbra, Almedina, 2015, pp. 373-378; JORGE BACELAR GOUVEIA, in *Estudos de Direito Público*, Cascais, 2000.

[76] Cf. SÓNIA REIS. & MANUEL BOTELHO DA SILVA. – *O sistema de informações da República Portuguesa*, 2007.

[77] Na perspetiva de JÚLIO PEREIRA (2012[2], p. 5), neste modelo o legislador pretendeu assinalar de forma um conjunto de ónus e limitações, designadamente: um acentuado controlo das suas atividades; a repartição estanque da competência de produção de informações entre um serviço interno e um serviço externo; separação radical entre as atividades de produção de informações e a atividade de polícia; uma proibição estrita de envolvimento dos Serviços de Informações em atividades policiais e simultânea proibição do envolvimento de entidades policiais em ações de inteligência.

por uma moldura de princípios de atuação no quadro democrático do Estado de Direito[78].

Em 1985, procedeu-se à regulamentação dos Serviços de Informações. Assim, o Decreto-Lei n.º 225/85, de 4 de julho criou o Sistema de Informações de Segurança (SIS)[79]. Só mais tarde, o Decreto-Lei n.º 254/95, de 30 de julho instituiu o Sistema de Informações Estratégicas de Defesa e Militares (SIEDM)[80]. Também de relevo no enquadramento histórico dos Serviços portugueses cabe referir os Decretos-Leis n.º 224/85 e 226/85, ambos de 4 de julho, na medida em que o primeiro veio estabelecer a orgânica do SIED, e por seu turno o segundo que reformou os Serviços de Informações Militares (SIM) – através da sua incorporação no SIRP.

De forma geral, no que concerne à produção de informações, devemos atender ao facto de que esta atividade assumiu maior relevância como "instrumento de segurança do Estado"[81] a partir de 1997, pela IV revisão constitucional – com a indicação de que a legislação desta atividade é de competência da Assembleia da República, conforme decorre da alínea q) do Art. 164.º da CRP. A primeira revisão constitucional, com a extinção do Conselho da Revolução e a submissão do poder militar ao poder civil, bem como a criação da Lei de Defesa Nacional, datada de 1982, vieram a considerar um sistema de informações de âmbito nacional (em moldes semelhantes aos que atuavam nos países democráticos europeus). Decorre desta iniciativa a publicação da 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 e 15/95, de 30 de abril (que extinguiu o SIM, serviço que nunca existiu e atribui ainda ao SIEDM competência exclusiva de produção de informações estratégicas de defesa e militares), 75-A/97 , de 22 de julho (que modificou as regras de nomeação para o Conselho de Fiscalização dos Serviços

[78] Nos termos constantes no n.º 2 do artigo 2.º da Lei n.º 30/84, de 5 de setembro.
[79] Segundo JORGE SILVA CARVALHO (2009), "no que concerne ao SIS, as principais dificuldades residiam nas limitações ao nível das infra-estruturas e insuficiência de meios operacionais".
[80] Relativamente ao SIEDM, JORGE SILVA CARVALHO (2009) advoga que se colocavam "numa primeira linha, problemas de insipiência organizativa, típicos de um serviço jovem, para além de questões decorrentes da necessidade de projecção externa e aprofundamento da operacionalidade do Serviço".
[81] Tal como explana JORGE BACELAR GOUVEIA – "Os serviços de informações de Portugal: organização e fiscalização" 2013, p. 66.

de Informações), e pela Lei Orgânica n.º 4/2004, de 6 de novembro – sendo nesta última onde foram estabelecidos os princípios em matéria de recolha e tratamento de informações - complementada por outras, designadamente, a Lei n.º 9/2007, de 19 de fevereiro, que estabelece a orgânica do Secretário-Geral do SIRP (SGSIRP), do SIED e do SIS. Com a aprovação da Lei Orgânica n.º 4/2004, de 6 de novembro, estabeleceu-se um marco de referência da configuração das informações em Portugal, por uma alteração de grande magnitude à Lei-Quadro do SIRP – principalmente, pela reformulação da sua liderança e coordenação, bem como a atribuição de funções ao Secretário-Geral do SIRP. Decorre da Lei Orgânica n.º 4/2004[82], de 6 de novembro e da Lei n.º 9/2007, de 19 de fevereiro, a organização da estrutura dos Serviços de Informações, formada por uma direção unificada centrada do Secretário-Geral do SIRP, na dependência direta do Primeiro-Ministro[83]. Estas alterações legislativas visaram, principalmente, alterar o paradigma das dimensões externa e interna da segurança, muito devido ao esbatimento que esta diferenciação foi sofrendo ao longo das décadas. A Lei Orgânica n.º 4/2004 visou ainda ampliar o poder do Conselho de Fiscalização do SIRP, na medida que englobam na sua esfera as informações militares, alterando a sua designação de Conselho de Fiscalização dos Serviços de Informações para Conselho de Fiscalização SIRP. Da mesma forma, em vez do SIED depender do Ministro da Defesa Nacional e do SIS depender do Ministro da Administração Interna, passaram a depender direta e hierarquicamente do Secretário-Geral do SIRP, sendo este último integrado na Presidência de Conselho de Ministros, é subordinado do Primeiro-Ministro. Para além destas alteraçõs, a Lei veio introduzir um regime de coordenação, controlo e direção unificado no Secretário-Geral do SIRP.

Conforme abordam SÓNIA REIS & BOTELHO DA SILVA (2007, p. 6), "o objetivo destas modificações foi claramente o de obter ganhos de eficiência e de

[82] Segundo JÚLIO PEREIRA (2012[2], p. 5) "A distinção estanque entre segurança externa e segurança interna que enformava o espírito da Lei-Quadro foi perdendo sentido, conduzindo a que também por cá fosse premente alterar o modo de funcionamento do SIRP, o que veio a suceder em novembro de 2004, com a aprovação da Lei nº 4/2004, de 6 de novembro".

[83] O Art. 3.º, n.º 1 da LOSIRP consagra que "Ao Secretário-Geral incumbe dirigir superiormente, através dos diretores do SIED e do SIS, no respeito da Constituição e da lei, a atividade de produção de informações necessárias à salvaguarda da independência nacional e dos interesses nacionais e à garantia da segurança externa e interna do Estado Português".

coordenação da actuação dos Serviços de Informações, propiciados por uma direcção superior e pela previsão da possibilidade de se criarem estruturas comuns ao SIED e ao SIS, na área da gestão administrativa, financeira e patrimonial[84]".

Não poderíamos deixar de fazer uma referência, ainda que breve, ao papel do Secretário-Geral do SIRP na contextualização histórica dos Serviços de Informações. De acordo com a Lei-Quadro, o Secretário-Geral é equiparado para todos os efeitos legais (exceto a sua nomeação e exoneração) a Secretário de Estado, tal como decorre do Art. 19.º, n.º 1. De acordo com o n.º 3, alínea a) do mesmo artigo, cabe ao Secretário-Geral "conduzir superiormente, através dos respetivos diretores, a atividade do Serviço de Informações Estratégicas de Defesa e do Serviço de Informações de Segurança e exercer a sua inspeção, superintendência e coordenação, em ordem a assegurar a efetiva prossecução das suas finalidades institucionais".

Como expõem SÓNIA REIS & MANUEL BOTELHO DA SILVA (2007), através da Lei-Quadro, o Secretário-Geral do SIRP assume uma dupla natureza, por um lado uma natureza puramente administrativa, e por outro uma natureza política ("um misto de dirigente superior de 1.º grau, v.g. director-geral, e de membro do Governo especializado nos Serviços de Informações"). Para JORGE SILVA CARVALHO (2009), a criação do papel de Secretário-Geral tratou-se de uma "solução inovadora também porque criou, pela primeira vez, um órgão ou organismo de segurança numa óptica de Segurança Nacional, integrando, ao seu nível, as informações de segurança interna e de segurança externa ou de defesa nacional contribuindo, também, assim para se tornar um melhor parceiro internacional, particularmente no espaço da União Europeia". Também JÚLIO PEREIRA (2012[2], p. 6) aponta que "Esta solução veio a dar frutos, permitindo, pela primeira vez, o funcionamento dos Serviços de Informações no quadro de um verdadeiro sistema orgânico, o que até então nunca sucedera, com partilha efetiva de informações sobre várias matérias e sem duplicação de atividades nos dois Serviços ou sobreposição de

[84] Cf. adverte JORGE BACELAR GOUVEIA (2018, p. 723) "A razão de ser para a criação destas estruturas comuns radicou na economia de escala e na conveniência da uniformidade de certas práticas resultantes de haver atividades administrativas servindo os dois serviços de informações, tal parecendo evidente nos aprovisionamentos ou na formação doutrinária".

análises, para além de uma ação coerente também do ponto de vista do relacionamento externo, que passou a competir diretamente ao Secretário-Geral".

Constituem ainda órgãos do SIRP, o Conselho de Fiscalização do SIRP: como órgão de Fiscalização parlamentar da atividade do Secretário-Geral e dos Serviços de Informações, que abordaremos mais aprofundadamente adiante; o Conselho Superior de Informações: como um órgão interministerial de consulta e coordenação em matéria de informações, sendo presidido pelo Primeiro-Ministro; e a Comissão de Fiscalização de Dados do SIRP: outro órgão de fiscalização da atividade dos centros de dados dos Serviços de Informações, com sede na Procuradoria-Geral da República.

O SIS e o SIED, "do ponto de vista da organização administrativa Portuguesa, inserem-se na Administração Pública Direta, apresentando-se como serviços do Estado em sentido estrito". Sendo que no plano jurídico-financeiro, são dotados de autonomia administrativa e financeira, "ao contrário do que ocorre com a generalidade dos serviços da administração directa do Estado, o que já é um indício da especialidade das suas atribuições"[85].

As atribuições do SIED e do SIS podem ser revistas nos Artigos 20.º e 21.º da LQSIRP. Neste sentido, o Art. 20.º preceitua que: "O SIED é o organismo incumbido da produção de informações que contribuam para a salvaguarda da independência nacional, dos interesses nacionais e da segurança externa do Estado Português". O Art. 21.º refere-se ao SIS como "o organismo incumbido da produção de informações que contribuam para a salvaguarda da segurança interna e a prevenção da sabotagem, do terrorismo, da espionagem e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido".

Apesar das atribuições do SIS estarem vocacionadas ao âmbito interno, a sua delimitação do âmbito territorial de atuação não obsta a que este serviço não importe o que acontece no exterior do território nacional. Isto porque, "uma visão estanque dos universos segurança externa e segurança interna está cada vez mais ultrapassada", uma vez que "a origem das ameaças à segurança externa e interna deixou de ser

[85] Cf. SÓNIA REIS & MANUEL BOTELHO DA SILVA – *O sistema de informações da República Portuguesa*, 2007.

claramente distinta, provindo, por vezes, da mesma fonte". Apesar desta circunstância, sempre que o SIS necessite de atuação do exterior, deverá recorrer ao SIED, sob pena de incorrer numa duplicação no SIS de habilitações do SIED, "numa solução pouco eficiente, do ponto de vista da economia dos meios". Para evitar tal situação, contribui de sobremaneira a orientação superior do Secretário-Geral do SIRP[86].

Ainda relativamente ao quadro jurídico-normativo, cumpre salientar o entendimento de JOSÉ FONTES (2010), ao sublinhar a carência de previsão constitucional da regulação e estruturação do SIRP - o que reflete a necessidade da intervenção ativa da Presidência da República[87]. Desta forma, alerta para uma urgência da revisão da CRP, uma vez que os Serviços de Informações apenas têm tutela *constitucional visível* ao nível do seu regime jurídico, contrariamente ao que acontece com as Forças Armadas e Forças de Polícia - que dispõem de tutela constitucional[88], quer do seu regime jurídico, quer nas funções constitucionalmente tuteladas. Concordamos, por isso, "que parece evidente que a nossa Lei Fundamental deva integrar no seu normativo uma referência aos Serviços de Informações, sendo incompreensível que a CRP não tenha até ao presente absorvido, constitucionalizando de forma menos discreta, tão importante corpo do Estado".

Nesta linha de entendimento, JORGE BACELAR GOUVEIA (2018, p. 685) aponta que "são várias as opções que o texto constitucional não versa, não lhes fazendo alusão ou sendo esse silêncio sinal de um entendimento negativo a respeito da sua possibilidade: - *a arquitetura estrutural do SIRP* (…); - *os poderes de que dispõem os serviços de informações,* designadamente na sua relação com os direitos

[86] Cf. explanado por SÓNIA REIS & MANUEL BOTELHO DA SILVA, 2007, p. 8.

[87] Prossegue salientando que, "Em consequência e, da mesma forma, defendemos que deveria competir ao Presidente da República a designação do Secretário-Geral do SIRP sob proposta do Executivo. Recordamos que designar, ouvido ou sob proposta do Governo, um conjunto de titulares de estruturas políticas, administrativas e até judiciais. O exercício desta competência nunca colocou em causa a sobrevivência do princípio da separação dos poderes constitucionalmente previsto no artigo 111.º como uma das basilares instituições estruturantes da organização do poder político em Portugal, nem diminuiu ou alterou, a dignidade dos órgãos de soberania: «Presidente da República» e «Governo»" (pp. 48 e 49).

[88] "… se é verdade que em 30 anos Portugal avançou rapidamente na modernização e aperfeiçoamento das suas estruturas políticas, económicas, sociais e culturais, não é menos verdade que o mesmo ritmo não se aplicou a todas essas importantes reformas" – cf. JORGE BACELAR GOUVEIA - *Os Serviços de Informações de Portugal: Organização e Fiscalização*, 2012.

fundamentais dos cidadãos; - *as atribuições dos serviços de informações nas tarefas que se colocam aos organismos da Segurança Nacional*(…).

Cabe referir que ALICE FEITEIRA (2015, p. 21) adverte acerca do facto de "a análise do enquadramento constitucional e infra-constitucional dos serviços de informações não esgota as possibilidades de conhecimento do direito que lhes é aplicado, mas antes pressupõe a aferição de todo o meio circundante – interesses nacionais a salvaguardar, procedimentos internos, ética e meios de acção – aspectos que perpassam a noção de democratização dos serviços de informações como um valor inerente à respectiva juridicidade". Torna-se notório que "existe um problema de legitimação democrática dos serviços de informações, considerando que estes se encontram impedidos de fazer prova do seu valor acrescentado".

Temporalmente, a evolução histórico-legislativa da atividade dos Serviços de Informações pode ser organizada em cinco períodos, conforme delineia JORGE BACELAR GOUVEIA (2018):

- 1.º período (1974-1984): compreende a ausência de serviços de informações, quando a função de produção de informações era assegurada pelos militares;

- 2.º período (1984-1995): ocorre a criação do Sistema de Informações da República Portuguesa, no papel do SIED, do SIS e do SIM (Serviços de Informações Militares), sem funcionamento efetivo do SIED;

- 3.º período (1995-2000): consolidação de dois serviços de informações, o SIS e o SIEDM (Serviços de Informações Estratégicas e Militares). De referir a segunda alteração, pela Lei N.º 15/96, de 30 de abril, no reforço das competências do Conselho de Fiscalização dos Serviços de Informações, uma terceira alteração incrementada pela Lei n.º 75-A/97.

- 4.º período (2004-2007): pela criação do cargo do Secretário-Geral do Sistema de Informações da República Portuguesa, responsável pela coordenação superior do SIED e do SIS. As informações militares passariam para a alçada do Estado-Maior-General das Forças Armadas, abandonando o SIED. A ação da Lei Orgânica n.º 4/2004, de 6 de novembro contribuiu fortemente para a melhoria da eficiência da

produção de informações, desde logo aumentando também poderes de fiscalização aos órgãos competentes. Segundo o autor existiram quatro melhorias significativas decorrentes desta Lei: a centralização da coordenação de informações, a condução da atividade de cada um dos Serviços de Informações, a manutenção da autonomia administrativa e financeira de cada um dos serviços, bem como a exclusão das informações militares do SIRP.

- 5.º período (2007-…): criação de estruturas administrativas comuns no âmbito do SIRP, além da incrementação de meios operacionais, pela aprovação da Lei n.º 9/2007, de 19 de fevereiro.

Alcançamos a visão futurista de JÚLIO PEREIRA (2012[2], p. 2) ao enfatizar que os "grandes desafios das Informações prendem-se na verdade com o futuro, situação esta que, num quadro de mudança e de incerteza como o que hoje vivemos apela mais que nunca à necessidade do desenvolvimento das competências nos campos da prospetiva e da cenarização, que temos de incorporar de forma crescente e nos desafiam de todas as formas possíveis: na doutrina, no que respeita à Teoria das Informações e à configuração clássica do ciclo da sua produção; na praxis, atendendo ao uso das novas tecnologias da comunicação e a ampliação de métodos analíticos; nos recursos humanos, com a necessidade de mudanças expressivas nos critérios de recrutamento e de formação inicial, contínua e treino, implicando a conciliação das diferentes gerações de oficiais de informações, a promoção da excelência, a conservação e a transmissão da memória e do conhecimento e o rigor das atitudes e dos comportamentos".

Noutro prisma, FERNANDO MARTINS (2010, p. 144) aponta a falta de cultura de segurança em Portugal como uma razão para considerar a ausência de ameaças e de inimigos, pelo que não será prioritário ou sequer importante a adoção de reforçadas medidas de segurança. Contudo, as recentes ameaças têm vindo a contribuir para uma alteração deste paradigma, pois "as diferentes ameaças, a sua correta classificação e a produção de informações sobre isso, estão na base dos processos de decisão dos Governos, para que, possam ser implementadas as devidas medidas de segurança", sobretudo de forma atempada.

Face ao percurso que acabamos de demarcar, estamos em crer que os Serviços de Informações prossigam um caminho de determinação do seu estabelecimento na promoção da proteção do Estado e dos seus interesses, conforme iremos abordar no Capítulo IV.

2. Os princípios regentes da atuação dos Serviços de Informações

Não podemos deixar de acompanhar a perceção transmitida por JORGE BACELAR GOUVEIA (2018) quando refere que "o Estado de Direito incorpora a atividade de produção de informações, bem como os organismos que as produzem, dentro da juridicidade pública, com tudo o que isso implica de fundamento e de limite à sua intervenção, serviços de informações que, a despeito do uso da palavra "secretos", o não são porque só existem e agem dentro da juridicidade, e não fora dela".

Neste sentido, conforme indica M.ª VILLALOBOS (2008, p. 1) "*La expression "servicios de inteligencia" ha cobrado relevancia en los Estados constitucionales, en detrimento de la tradicional "servicios secretos" (...) es la diferencia entre unos servicios de inteligencia democráticos y unos servicios secretos que constituyen un "Estado dentro del Estado" y que funcionan sin ajustarse a ningún tipo de control legal ni democrático, situándose al servicio del poder político establecido para el mantenimiento del mismo*"[89]. A autora considera como fundamental o elemento democrático, na medida em que o constitucionalismo democrático limita as atuações dos poderes públicos porque as submetem a determinados controlos[90].

S. BORAZ & T. BRUNEAU (2006, p. 28) informam acerca do necessário equilíbrio da atuação dos Serviços de Informações no quadro democrático:

[89] A este propósito S. REIS & M. BOTELHO DA SILVA (2007, p.3) comentam que o termo "secretas" trata-se de uma expressão "destituída de rigor", uma vez que "a actuação dos Serviços de Informações se pauta hoje pela mais estrita legalidade", tendo também em consideração que que são objeto de "um tipo de controlo e de regime de fiscalização excepcional".

[90] Nas suas palavras, "*Pero junto al elemento constitucional, es fundamental el elemento democrático, de manera que el constitucionalismo actual es democrático, o, dicho de outra manera, las Constituciones democráticas limitan las actuaciones de los poderes públicos porque las someten a controles*" (p. 2).

> *"Democracy requires openness in the flow of information and discussion, while intelligence work often demands secrecy. Maintaining agencies to do such work in the midst of a generally open political culture is a challenge for any democracy. Democratizing or newly democratic countries, however, must deal with the even more arduous task of transforming intelligence bureaucracies that once served undemocratic regimes*".

Os Serviços de Informações desenvolvem uma ação discreta e silenciosa na prossecução das missões que estão legalmente incumbidos, pela representação da tutela do interesse nacional e a defesa dos valores constitucionalmente estabelecidos, a sua *ratio*[91]. Pelo quadro legal vigente, a atividade de produção de informações encontra o seu desenvolvimento acautelado por um conjunto de princípios de atuação que iremos discorrer seguidamente.

2.1. Princípio da Constitucionalidade e da Legalidade

Tal como refere JORGE BACELAR GOUVEIA (2018), "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"[92] [93].

Este princípio encontra-se vigente pelo Art. 3.º, n.º 1 da LQSIRP, de forma que "Não podem ser desenvolvidas atividades de pesquisa, processamento e difusão de informações que envolvam ameaça ou ofensa aos direitos, liberdades e garantias consignados na Constituição e na lei".

2.2. Princípio da Especialidade

[91] RUI PEREIRA & ALICE FEITEIRA. – *Serviços de Informações*, 2015, p. 340.
[92] v. *Os princípios da Produção de Informações*, in *Direito da Segurança*, 2018, p. 706; GOUVEIA, J. B. - *Os Serviços de Informações de Portugal: Organização e fiscalização*, in *Estudos de Direito e Segurança*, Almedina, 2007, pp. 181-182.
[93] Atentar igualmente o estudo de MARIA CONCEPCION PEREZ VILLALOBOS - *Derechos Fundamentales y Servicios de Inteligencia*, de 2002.

Conforme continua o Professor JORGE BACELAR GOUVEIA (2018) "a atividade dos serviços de informações está limitada às suas atribuições, não podendo desenvolver-se em domínio que lhe não tenha sido concedido"[94].

Este princípio encontra-se plasmado no Art. 3.º, n.º 3 da LQSIRP, quando estipula que "Cada serviço só pode desenvolver as atividades de pesquisa e tratamento das informações respeitantes às suas atribuições específicas, possam ter interesse para a consecução das finalidades do Sistema de Informações da República Portuguesa".

2.3. Princípio da Restrição Funcional

Segundo JORGE BACELAR GOUVEIA (2018), "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". Desta forma, o Art. 4.º, n.º 1 da LQSIRP estabelece que "Os funcionários ou agentes, civis ou militares, dos serviços de informações previstos na presente lei não podem exercer poderes, praticar atos ou desenvolver atividades ou âmbito ou competência específica dos tribunais ou das entidades com funções policiais".

Conforme explanam SÓNIA REIS & MANUEL BOTELHO DA SILVA (2007), os Serviços de Informações não desempenham qualquer função policial nem intervêm no processo penal. Verifica-se, que não representam órgãos de polícia criminal para efeitos do Código de Processo Penal (CPP), uma vez que considerando a alínea c) do n.º 1 do artigo 1.º desse diploma não se configuram como entidade ou agente policial. Por outro lado, também não assumem a qualidade de autoridade de polícia para qualquer outra finalidade, uma vez que o artigo 15.º da Lei de Segurança Interna não integra na sua lista referência ao SIED ou ao SIS, "o que redunda igualmente em impossibilidade de intervir no processo penal enquanto autoridade de

[94] Pelo que, "Por força do princípio da especialidade, os serviços de informações não podem confundir-se com a atividade que é protagonizada por outras funções, atividades e estruturas públicas, mesmo que de um modo geral concorram para a Segurança do Estado" - Cf. JORGE BACELAR GOUVEIA - *Os Serviços de Informações*…", 2012, p. 82.

polícia criminal a que a alínea d) do n.º 1 do artigo 1.º CPP se refere". Desta forma, afere-se que o impedimento de intervirem no âmbito do processo penal é ainda reafirmado pelo disposto no artigo 4.º da Lei Quadro do SIRP e nos n.os 2 e n.º 3 do artigo 6.º da Lei n.º 9/2007, de 19 de Fevereiro.

A propósito da atuação dos sistemas de informações em democracia, J. CHITO RODRIGUES (2011) refere que "quando os serviços de informações que por lei servem o Estado, através dos governos legitimamente eleitos, para defesa do país e da própria democracia passam a servir as polícias, ainda que sob o pretexto da ameaça terrorista, estamos no limiar da perda dos direitos e garantias dos cidadãos. Estamos no limiar de doença grave da Democracia", pelo que devemos acautelar cuidadosamente os limites da sua atuação.

2.4. Princípio da Exclusividade

O Princípio da Exclusividade é validado no sentido de que os Serviços de Informações prosseguem funções que não competem a mais nenhuma entidade pública, ou seja, da mesma forma que estão proibidos de exercer funções policiais ou intervirem no âmbito do processo penal - pois é atividade de competência dos OPC - a atividade de produção de informações é de única e exclusiva competência do SIRP.

Conforme apontam SÓNIA REIS & BOTELHO DA SILVA (2007) através do princípio da exclusividade da atuação do SIRP, pretende-se evitar que os órgãos de polícia criminal possam "pré-selecionar alvos". Caso assim não fosse, existia a possibilidade de o processo penal ser preferencialmente orientado contra estes alvos, sob violação do princípio da legalidade processual penal. Acompanhamos a opinião dos autores, quando defendem que, caso as informações fossem misturadas com a investigação criminal, fomentariam irremediavelmente uma "focagem preferencial em certos grupos ou indivíduos, por motivos discricionários ou políticos, permitindo que apenas estes sofram consequências penais das duas condutas". Da mesma forma que este princípio "consubstancia o reverso da proibição de estes Serviços desempenharem funções policiais ou de investigação criminal, por defender valores similares".

A LQSIRP vem estabelecer este princípio de atuação, quando no seu Art. 6.º estabelece que "É proibido que que outros serviços prossigam objetivos e atividades idênticos aos dos previstos da presente lei".

Findada a exposição dos elementares princípios regentes da atuação do SIRP no âmbito da LQSIRP, JORGE BACELAR GOUVEIA (2018) expõe um conjunto de princípios garantidos na LOSIRP que não podemos deixar de fazer referência pela sua pertinência ao tema em abordagem. Deste logo, o *princípio da juridicidade e do interesse público* (uma vez que "O SIED e o SIS estão exclusivamente ao serviço do Estado e exercem as respetivas atribuições no respeito da Constituição e da lei, de acordo com as finalidades e objetivos do SIRP – cf. Art. 3.º, n.º 4); pelo *princípio do respeito pelos direitos fundamentais*[95], já que o Art. 6.º, n.º1 estabelece que "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"; por seu turno, é retomado o *princípio da exclusividade*, quando refere que "Aos membros do Gabinete e aos funcionários e agentes referidos no número anterior 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" (Art. 6.º, n.º 2); o *princípio do sigilo*: "Toda a atividade de pesquisa, análise, interpretação, classificação e conservação de informações desenvolvida no âmbito do SIRP está sujeita ao dever de sigilo, nos termos definidos pela Lei-Quadro do SIRP (Art. 5.º, n.º 3); por último, é discorrido o *princípio da não publicidade de atos*, já que, "Quando fundadas razões de segurança ou relacionadas com a especificidade do serviço o justifiquem, podem os membros do Governo intervenientes determinar, referindo-o expressamente, a dispensa de publicação dos atos necessários à execução dos diplomas do SIRP" (cf. Art. 8.º).

[95] Adianta ainda que "…é a afirmação de uma singular limitação protagonizada pela legislação dos serviços de informações para não autorizar sequer quaisquer restrições legítimas ao exercício de direitos fundamentais dos cidadãos, colocando estes organismos numa posição de menor poder em relação a outros, que lidam com a aplicação de limitações a tais direitos, *maxime* os órgãos policiais e de investigação criminal" (p. 709).

IV. DA ATUAÇÃO DO SIRP E DO ACESSO AOS DADOS DE TELECOMUNICAÇÕES E INTERNET

1. A Segurança e a Liberdade no contexto das novas ameaças

A estreiteza entre o avanço legislativo que abordamos e o permanente debate da paralelização dos valores Segurança e Liberdade é inegável, num contexto de constante confrontação entre a adoção de políticas públicas necessárias à manutenção do espaço securitário e a possibilidade de ferir outros valores estabelecidos num Estado democrático, mormente a Liberdade e a Privacidade.

Referimo-nos mais exatamente à salvaguarda do Art. 27.º, n.º 1 da CRP, quando estabelece que "Todos têm o direito à liberdade e à segurança", obrigação prestacional do Estado perante os cidadãos. Para o efeito, "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" (cf. Art. 18.º, n.º 2, da CRP). Nesta senda, conforme explica JORGE MIRANDA (2003), "A segurança é o ambiente do Direito, mas nunca pode prevalecer sobre o próprio Direito".[96]

Ora, neste sentido, a Constituição consagrou a reserva da intimidade da vida privada (Art. 26.º) como um direito autónomo, o que lhe confere amplitude suficiente para englobar aspetos variados do nosso quotidiano e do nosso relacionamento com a sociedade. Ainda nesta senda, o Art. 70.º do Código Civil estabelece que "a lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça à sua personalidade física ou moral" e o Art. 80.º – com a epígrafe "Direito à reserva sobre a intimidade da vida privada" – estatui que: "1. Todos devem guardar reserva quanto à intimidade da vida privada de outrem. 2. A extensão da reserva é definida conforme a natureza do caso e a condição das pessoas". Assim, o normativo implica que, na concretização

[96] v. JORGE MIRANDA. - *Constituição e Cidadania: Terrorismo e direitos fundamentais*, Coimbra Editora, 2003, p. 319.

da extensão da reserva da intimidade da vida privada de outrem, depende de dois critérios: "a natureza do caso" e a "condição das pessoas" (n.º 2).

J.J. GOMES CANOTILHO & V. MOREIRA (2007) reconhecem que "o conjunto de direitos fundamentais relacionados com o tratamento informático de dados pessoais arranca de alguns "direitos-mãe" em sede de direitos, liberdades e garantias. É o caso do direito à dignidade da pessoa humana, do desenvolvimento da personalidade, da integridade pessoal e da autodeterminação informativa".

Tal como informa J. GOMES CANOTILHO (2007), "O segredo não é compatível com as liberdades e direitos do homem. Ao segredo acrescenta-se um novo perigo para o cidadão: «a digitalização dos direitos fundamentais». Contrapondo-se à ideia de *arcana praxis*, tende hoje a ganhar contornos um direito geral à autodeterminação informativa que se traduz, fundamentalmente, na faculdade de o particular determinar e controlar a utilização dos seus dados pessoais. (…) Este direito de autodeterminação pode exigir a criação de meios de defesa jurisdicionais e, nesse sentido, apontam já hoje convenções internacionais e o direito de *Habeas Data* consagrado na Constituição brasileira de 1988 (cfr. Ac. TC n.º 182/89, in DR, I, n.º 51, de 2/3/89)"[97].

Desta forma, e importante para base de análise deste trabalho, pode "afirmar-se que quanto mais os dados relacionam a dignidade, a personalidade e a autodeterminação das pessoas, tanto mais se impõem restrições quanto à sua utilização e recolha (banco de dados). É neste contexto que se situam dois problemas fundamentais relativos ao processamento de dados informáticos: (1) determinação das *categorias* de dados; (2) graduação das ingerências necessárias à proteção de outros bens constitucionais"[98].

Face a ameaças, como o fenómeno terrorista, a criminalidade organizada[99], e a criminalidade transnacional verificadas nos últimos anos, têm vindo a ser adotadas e

[97] v. *Direito Constitucional e Teoria da Constituição*, p. 514.
[98] v. *Constituição da República Portuguesa Anotada*, p. 551.
[99] Como informa JOSÉ MANUEL ANES (2010, p. 213), "o crime organizado deve ser entendido como a prática, por um grupo de indivíduos caracterizados por uma relação hierárquica, com funções especificamente atribuídas, em associação de esforços, de actos previstos e puníveis numa determinada ordem jurídica como

reforçadas medidas securitárias, sendo certo que frequentemente estas medidas constituem "sérios ataques à autodeterminação informativa do cidadão"[100]. Nesta medida, não podemos deixar de acompanhar o alerta deixado por JORGE MIRANDA (2003, p. 319), quando adverte que "o pior que poderia acontecer aos regimes liberais e pluralistas do Ocidente seria, a pretexto do terrorismo, afastarem-se dos grandes princípios jurídicos que tanto custou a conquistar e a sedimentar nas suas Constituições, nas suas leis e nas suas culturas cívicas. O pior que poderia acontecer seria, afinal, a pretexto do terrorismo, ficarem abalados os fundamentos do Estado de Direito". Assim, resta-nos acautelar cuidadosamente as medidas que tomamos, de forma a minimizar possíveis riscos de ilegalidades.

Numa perspetiva não só histórica mas igualmente holística, "«…a legitimação democrática dos serviços de informações não assenta exclusivamente no enquadramento constitucional e infraconstitucional que rege as respetivas competências, meios e missões, sendo preenchida igualmente pela compreensão da comunidade política quanto aos valores e interesses socialmente relevantes e a proteger pelos serviços de informações, contribuindo também para essa avaliação o lastro histórico dos serviços de informações junto dessa comunidade"[101].

Conforme sublinha o parecer do CFSIRP relativo ao primeiro semestre de 2016, as ameaças que os serviços de informação visam detetar e prevenir não desapareceram nem diminuíram, pelo que é de grande conveniência dotar os serviços, em particular o SIS de meios que permitam a deteção de tais ameaças, atuando num integral respeito dos direitos, liberdades e garantias, de forma a todos os limites constitucionais e legais sejam tidos em consideração.

crimes, na prossecução de um fim coletivamente estabelecido e aceite, podendo este ser ou não, de per si, também crime."

[100] Conforme prossegue, o Artigo 26.º da CRP veio expressamente consagrar a reserva da intimidade da vida privada, como fazendo parte do direito, com maior amplitude, do desenvolvimento da personalidade. "Esta proteção foi sendo adotada por algumas Constituições dos Estados europeus, que garantem um direito à privacidade, embora, nalguns casos, essa proteção se refira à inviolabilidade do domicílio e da correspondência" - vide CATARINA SARMENTO E CASTRO - *O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro*, 2005, p. 1.

[101] v. RUI PEREIRA & ALICE FEITEIRA - *Serviços de Informações*, Lisboa: Almedina, 2015.

A propósito das informações trazidas a público por Edward Snowden[102] sobre a vigilância massificada praticada pelos Estados Unidos da América, Edward Felten[103], Professor da Universidade de Princeton, contesta a legalidade do programa conduzido pela *National Security Agency* (NSA) no acesso aos "*metadata*", explicando que a vigilância em massa[104] consegue ser especialmente intrusiva:

> "Consideremos a seguinte hipótese: uma jovem liga para o seu ginecologista; de seguida, liga para a sua mãe e, de imediato, para um homem com quem tem falado ao telefone repetidas vezes ao longo dos últimos meses, sempre depois das 23 horas; pouco depois, a jovem liga para um centro de planeamento familiar que também faz interrupções de gravidez. Destes pontos surge uma linha narrativa que não seria possível construir analisando os registos de apenas uma chamada telefónica. Neste sentido, a recolha de metadados pode, no mínimo, ser tão intrusiva quanto a interceção de conteúdo"[105] (cit. por GLENN GREENWALD, 2014).

[102] A propósito das revelações e compreesão do seu impacto, é interessante acompanhar os estudos de Elizabeth Atkins - *Spying on Americans: At What Point Does the NSA'S Collection and Searching of Metadata Violate the Fourth Amendment?;* Zygmunt Bauman, Didier Bigo, Paulo Esteves, Elspeth Guild, Vivienne Jabri, David Lyon, R. B. J. Walker – "After Snowden: Rethinking the Impact of Surveillance", In *International Political Sociology*, Volume 8:2, 1 junho 2014, págs. 121–144; Ron Deibert – "The Geopolitics of Cyberspace after Snowden", In *Current History*, janeiro 2015.

[103] Crítico do programa de vigilância massificada levada a cabo pelos EUA através da *Section 215* do *Patriot Act* (mais conhecida como "*Verizon Order" – "that requires the production of "call detail records" or "telephony metadata").*

[104] Conforme adverte ME CÉCILE DOUTRIAUX (2014, p. 9), "*La possibilité pour un État d'invoquer des considérations de sécurité nationale pour amoindrir les droits des citoyens est forcément préoccupante et on ne peut totalement écarter les risques d'abus. Toute personne qui fait l'objet d'une mesure de surveillance, basée sur des motifs de sécurité nationale, doit bénéficier de garanties contre l'arbitraire. Cela étant, le système de cybersurveillance pourrait trouver en lui-même sa propre limite puisque la captation des données en masse, qui consiste à tout intercepter au motif que cela pourrait toujours servir un jour, n'est pas véritablement efficace puisque seule l'analyse fine des données interceptées est utile*".

[105] A este propósito, E. FELTEN salienta que "… as escutas telefónicas podem ser bastante complexas devido a especificidades linguísticas, utilização de calão, conversas vagas, utilizações de códigos e outros aspetos que, por definição ou por acaso, escondem o seu significado". Assim, "O conteúdo das chamadas é muito mais difícil de analisar de forma automatizada devido à sua natureza não estruturada" pelo que, em oposição "os metadados são matemáticos: claros e objetivos e, por isso, fáceis de analisar" (cf. citado por GLENN GREENWALD, 2014). EDWARD FELTEN (2013, p. 6) confirma, a propósito da vigilância levada a cabo pela *NSA* que "*The contents of calls are far more difficult to analyze in an automated fashion due to their unstructured nature. The NSA would first have to transcribe the calls and then determine which parts of the conversation are interesting and relevant. Assuming that a call is transcribed correctly, the NSA must still try to determine the meaning of the conversation: When a surveillance target is recorded saying "the package will be delivered next week," are they talking about an order they placed from an online retailer, a shipment of drugs being sent through the mail, or a terrorist attack? Automatically parsing and interpreting such information, even with today's most sophisticated computing tools, is exceptionally difficult*".

O Acórdão n.º 486/2009, de 5 de novembro do TC[106] refere que "o acesso aos dados de tráfego exprime uma invasão diferente, mas não de menor intensidade, que a interceção das comunicações telefónicas". De acordo com o mesmo arresto, "a possibilidade de aceder à intensidade dos contactos com determinado posto telefónico constitui uma verdadeira intromissão na intimidade dos cidadãos visados". Por outro lado, "o acesso à localização celular é indiscutivelmente uma intromissão penetrante na esfera da privacidade e intimidade do cidadão", visto que "este meio representa um autêntico controlo à distância do cidadão facultando acesso a todos os seus movimentos". Assim, "não procede o pressuposto de que a escuta de uma comunicação é mais invasiva que o acesso aos dados de tráfego ou/e à localização celular", sendo que "muitas vezes uma comunicação não evidência mais que um diálogo de conteúdo inócuo – seja porque os interlocutores não o pretendem fazer ao telefone -, mas a circunstancia de se aceder ao número de vezes que se liga para determinado aparelho já pode ter um conteúdo forte e o acesso à localização celular é em si mesmo profundamente invasivo do direito à privacidade".

A CNPD revela no seu Parecer 38/2017 que "as comunicações englobam ainda os acessos aos sítios na Internet, por também tais operações implicarem comunicação eletrónica, para além dos acessos a partir das aplicações (apps) e outros carregamentos e atualizações de informação que os equipamentos vão fazendo automaticamente nas redes de comunicação eletrónica, sem exigir da parte do utilizador uma intervenção positiva e direta". Assim, critica a "visão tradicional" das comunicações eletrónicas segundo a jurisprudência nacional. Para a CNPD, o ponto 13 do Ac. do TC n.º 403/2015 é exemplo disso mesmo, uma vez que se reporta a "comunicações individuais efetivamente realizadas ou tentadas e só essas é que estão cobertas pelo sigilo das comunicações", o que não encontra correspondência com o quadro jurídico nacional e europeu que vigora atualmente na imensidão de possibilidades de comunicações digitais ("supondo que as comunicações individuais são as efetivamente realizadas ou tentadas, quando em rigor as comunicações individuais abrangem ainda todos os *push* de informação").

[106] Referente ao Processo n.º 4/09 - *Diário da República*, 2.ª série, N.º 215, de 5 de novembro de 2009.

Como preceitua JOSÉ LUCENA (1991, p. 128), "Não admira, por isso, que tudo quanto aparente pôr em causa, de modo significativo e mais ou menos iminente, a segurança seja motivo de especial preocupação". Na opinião do autor, o conceito de segurança "pode ser considerado como incluindo apenas a garantia da independência, da soberania, da integridade territorial e da unidade do Estado ou pode ser entendido como abrangendo todo o conjunto de interesses, que podem ir desde a garantia de acesso a matérias-primas essenciais até à protecção de investimentos e de cidadãos nacionais no estrangeiro, desde cinturas de segurança a zonas de influência neutralizadas, desde o controlo do nível de capacidade militar de adversários potenciais e vizinhos até à uniformidade dos regimes e sistemas políticos, etc., etc." transformando-se assim numa "aspiração de ilimitada expansão" e preponderância.

Para CATARINA SARMENTO E CASTRO (2005, p. 24) trata-se de "encontrar o equilíbrio entre o direito à autodeterminação informativa e o direito à segurança, o que não deixa de ser a procura da harmonia entre a liberdade individual (neste caso, essencialmente informática) e a segurança: a primeira, sem a segunda, gera o caos e a anarquia, a segunda, sem a primeira, conduzirá à construção de Estados totalitários".

WOOD & BALL (2006, p. 5)[107] defendem que vivemos atualmente numa "Sociedade Vigilante", quer pelas vídeo câmaras através das quais somos constantemente vigiados (em centros comerciais, ruas e áreas residências), quer pelas informações que somos obrigados a prestar quando viajamos, pela análise feita ao nossos hábitos de consumo (através do rastreio das nossas pesquisas na Internet), etc. – ou seja, são várias as razões que nos levam a focar nos perigos e riscos, a partir dos quais são adotadas determinadas medidas de segurança, e não nos focarmos nos verdadeiros objetivos e valores sociais associados à liberdade – desta forma, aquilo que seria inicialmente considerado invasivo, torna-se normalizado e aceite pela

[107] Os autores apresentam a definição de "*Surveillance Society"* como "*...a society which is organised and structured using surveillance-based techniques. To be under surveillance means having information about one's movements and activities recorded by technologies, on behalf of the organisations and governments that structure our society. This information is then sorted, sifted and categorised, and used as a basis or decisions which affect our life chances. Such decisions concern our entitlement and access to benefits, work, products and services and criminal justice; our health and well-being and our movement through public and private spaces*".

opinião pública. Os autores vão mais longe, acreditando que ficámos tão "hipnotizados" com aquilo que são soluções de alta tecnologia no combate ao crime, terrorismo e fraude que nos esquecemos de procurar outras soluções, que por vezes poderiam sem mais apropriadas e menos invasivas do que as primeiras[108].

Acompanhando igualmente a perspetiva de "vulgarização" imposta pela "demandada da segurança", conforme veicula M. GUEDES VALENTE (2008), "O recurso, quer no plano legiferante que no plano operacionalizante da norma legitimadora, imbuído do espírito securitário *ab initio*, a meios de obtenção de prova ou instrumentos de combate (representação) ao crime de natureza excecional induz à vulgarização dos meios que só excecionalmente deviam ser utilizados, quando os menos onerosos e agressivos para o cidadão – arguido ou não – se mostrassem inidóneos e inadequados e incapazes de obter a prova ou a descoberta da verdade".

Se por um lado corremos o risco de normalizar determinadas medidas de segurança que poderão ser invasivas à nossa privacidade. Por outro lado, existe um domínio que estamos inevitavelmente a ceder a terceiros. Neste sentido, SCHUSTER et al. (2017, p. 77) apontam para uma tríade de *stakeholders* associados à discussão de privacidade *online* e vigilância em massa: i) Estado e Autoridades de Segurança (*state agencies and law enforcement authorities)* ii) negócios (*businesses world*), e iii) cidadãos, sendo certo que cada um destes grupos apresenta níveis de interesse diferenciados pela matéria, conflituando entre eles por vezes. Segundo os autores, o Estado e as Autoridades de Segurança argumentam que a privacidade é secundária à segurança nacional; para o mundo dos negócios, os dados recolhidos permitem uma maior customização da oferta, pelo conhecimento das necessidades dos consumidores e conhecer nichos de mercado; já os cidadãos gostam de aproveitar alguns dos benefícios de serviços e buscas *online* cada vez mais customizadas, carros autónomos, entre outras. Concluem assim que se trata de um fenómeno geracional, ou seja, "*This is a generational phenomenon, with the digitally native generation apparently being more inclined to surrender some of their privacy than older*

[108] Na medida em que "*The surveillance society has come about almost without us realising. However, this does not mean that all this is acceptable: understanding the effects of surveillance and the impacts they have on our personal lives and on society is crucial*" (p. 4).

generations[109]*"*. Para os autores, mesmo que preocupados com questões de privacidade, os utilizadores consideram que o valor monetário baixo ou inexistente por transferência de uma aplicação de telemóvel gratuita supera a sua privacidade. Nesta senda, considera-se que vários utilizadores estão dispostos a ceder parte da sua privacidade em detrimento de informação privada, e sem disposição para pagarem por maior proteção da sua privacidade.

Devemos desde logo abordar o acesso aos dados de telecomunicações e Internet numa perspetiva de incremento da qualidade da atividade de *intelligence*, isto significa que devemos alcançar o seu papel preponderante na missão do SIS e do SIED. Contudo, conscientes de que é certo que a constante evolução tecnológica e a capacidade de produção de informações decorrente desta evolução fomentam novos riscos para a sociedade. Neste sentido M.ª VILLALOBOS (2008, p. 3) concretiza que:

> "*Las Respuestas que requieren los nuevos riesgos no dependen tanto de la cantidad de información como de la adecuada valoración e interpretación que se hace de ésta. Pero es cierto que las fuentes de información tienen en la actualidad una dimensión inabarcable para cualquier servicio de inteligencia. Es la inteligencia multimedia que ha trasladado el processo de inteligencia al processo de análisis desbordando la función de los servicios de inteligencia que, en no pocas ocasiones se vem obligados a acudir a empresas privadas de gestión de estos recursos y a grupos especializados*".

A propósito da necessidade de evolução da atuação do Serviços de Informações britânicos, OMAND ET AL. (2012, p. 9)[110] apontam no caminho do acompanhamento do desenvolvimento social paralelamente à adequação da produção

[109] Continua referindo que "*Even when users are concerned about their privacy, they value it very low in monetary terms. Many users are willing to give away personal data for a small price and would pay even less for increased protection of their privacy*" (p. 77)

[110] O estudo dos autores visa demonstrar as potencialidades das rederes sociais (*Facebook*, *Twitter*, etc.) como parte integrante da produção de informações, em particular no âmbito da "*social media intelligence"* (*SOCMINT*) - desde a sua contribuição decisiva na segurança pública, na identificação de fenómenos criminosos e na prevenção de ameaças e desordens públicas.

de informações. Neste sentido, à medida que a sociedade se desenvolve e adota novas formas de comunicação, relacionamento e organização, é vital que os organismos públicos, mormente os órgãos de polícia criminal e a comunidade de *intelligence* possam acompanhar essas mudanças. Contudo, advertem que "*at the heart of national security is public understanding and support for the steps being taken to keep us safe*". Assim sendo, é exigível à legitimidade democrática que os métodos de recolha e tratamento de informações à disposição dos Serviços de Informações sejam introduzidos por via de uma base legal firme, baseada na compreensão política do incremento das capacidades destes e no conhecimento da sociedade civil acerca dos instrumentos que são utilizados: "*even if the operational details of the sources and methods used must sometimes remain secret*".

Nesta senda, temos ainda de ponderar a sua atuação mediante a sujeição a segredo de Estado, acompanhamos RUI PEREIRA & ALICE FEITEIRA (2015) na medida em que a legitimação material subsiste já que surge a "dificuldade de os serviços de informações – pela natureza das atividades que desenvolvem e pela sujeição das suas atividades ao segredo de Estado – fazerem prova, de forma imediata, do seu valor acrescentado junto da comunidade".

Tal como sublinha ALICE FEITEIRA (2015, p.26), o exercício coercivo do poder do Estado no domínio da segurança não se encontra apenas determinado aos princípios da legalidade, proporcionalidade e adequação de meios: assim, num "Estado de matriz liberal, a relação comunicacional entre a administração e os cidadãos, bem como a eficiência das actividades públicas, deve espelhar uma visão integrada da sociedade quanto à natureza dessas actividades, dos meios afectos e da sua necessidade, de forma a garantir um consenso social quanto ao exercício dessas competências".

Tal como vislumbra JORGE SILVA CARVALHO (2009), a produção de informações constitui uma das atividades centrais do Estado, num mundo profundamente globalizado, sempre que esta mesma atividade se assume como algo de "verdadeiro e nobre serviço público". Para o autor a produção de informações deve constituir "a primeira linha da defesa e de segurança num mundo em que as ameaças

que afectam os interesses dos Estados assumem contornos indefinidos, de onde o puro poder militar já não é suficiente para as combater com absoluta eficácia". Assim elabora-se a referência ao mundo em que vivemos de modo tal que "para se obter vitórias, para se ter sucesso, para se evitar derrotas definitivas é necessário actuar mais rapidamente que os nossos adversários, decidir de forma mais precisa e adaptarmo-nos perfeitamente às mudanças, o que se traduz visivelmente em «vantagens comparativas»".

Acompanhamos D. VITKAUSKAS (1999, p. 54), ao confirmar que o papel de um serviço de *intelligence* é composto por vários elementos interlocutórios que refletem a necessidade de promovermos um equilíbrio adequado entre as diferentes necessidades sentidas numa sociedade democrática. Para o autor, este equilíbrio é necessário, de forma a que se proteja, por exemplo, a segurança nacional, respeitando na mesma medida os direitos humanos e as liberdades fundamentais dos cidadãos, através de mecanismos que sirvam o Estado – assegurando, ao mesmo tempo, autonomia suficiente de forma a estarem protegidos de pressões e devaneios políticos. Adotando a perspetiva que, "*The willingness of states to constantly look for improvement in the search of this balance will confirm their dedication to the principles upon which democratic societies function*".

Entendemos que é inegável que o instrumento de produção de informações patente na solução legalmente prevista atua sobre um conjunto de dados previamente delimitados através de uma análise prévia devidamente fundamentada, como analisaremos adiante. Assim sendo, trata-se de um método consideravelmente menos intrusivo da intimidade dos alvos do que caso se tratasse do acesso ao conteúdo das comunicações.

Acrescem as finalidades que auguram alcançar, na medida em que se tratam do combate a ameaças cujo a seu carácter e implicações são vulgarmente debatidos da sociedade civil. Entendemos, por isso, tratar-se de um meio de *intelligence* que os serviços devem dispor face às necessidades securitárias discutidas ao nível do quadro político e social atual.

2. Enquadramento Legislativo da Proteção de Dados e o Sigilo das Telecomunicações

2.1 Em Portugal

O acesso a dados relacionados com as comunicações eletrónicas tem sido uma matéria amplamente regulamentada, algo que se deve, principalmente, a pressões comunitárias (Cf. ponto 10 do Ac. do TC n.º 403/2015).

De acordo com o Art. 2.º da CRP a "A República Portuguesa é um Estado de direito democrático, baseado na soberania popular, no pluralismo de expressão e organização política democráticas, no respeito e na garantia de efectivação dos direitos e liberdades fundamentais e na separação e interdependência de poderes, visando a realização da democracia económica, social e cultural e o aprofundamento da democracia participativa". Tal como ensinam J.J. GOMES CANOTILHO & V. MOREIRA (2007, p. 205) "Na sua vertente de Estado de direito, o princípio de Estado de direito democrático, mais do que constitutivo de preceitos jurídicos, é sobretudo conglobador e integrador de um amplo conjunto de regras e princípios dispersos pelo texto constitucional, que densificam a ideia de *sujeição do poder a princípios e regras jurídicas*, garantindo aos cidadãos liberdade, igualdade e segurança". Assim, "Ao Estado incumbe não apenas «respeitar» os direitos e liberdades fundamentais, mas também «garantir a sua efectivação»" (p. 208).

Também importa enfatizar que "O Estado subordina-se à Constituição e funda-se na legalidade democrática", de acordo com o n.º 2 do Art. 3.º da CRP. Conforme ensinam J.J. GOMES CANOTILHO & VITAL MOREIRA (2007, p. 216), este preceito "reitera o princípio da constitucionalidade do Estado, ou seja, de que ele não se encontra acima ou à margem da Constituição mas antes submetido a ela (princípio da juridicidade constitucional vinculativa de todos os poderes do Estado)" pelo que "O Estado não é sujeito da Constituição, é o seu objecto".

Em Portugal, desde 1976, que a Lei Fundamental dispõe que "1 – Todos os cidadãos têm o direito de acessos aos dados informatizados que lhe digam respeito,

podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei" (Art. 35.º), complementado que a lei deverá definir o conceito de dados pessoais, bem como as condições do eventual tratamento de forma automática, a sua conexão, transmissão e finalidades, garantindo a sua adequada proteção (n.º 2). O n.º 3 do Art. 35.º assegura que "é proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei". É indiscutível que o Art. 35.º da CRP é relevante no âmbito da definição legal de dados pessoais, no sentido em que os dados de tráfego estão incluídos nesta aceção, que vai ao encontro das decisões do TJUE (Cf. Acórdãos *Digital Rights Ireland Ltd.* e *Tele 2*). Para CATARINA SARMENTO E CASTRO (2005, p. 1) "O direito consagrado no artigo 35.º traduz-se num feixe de prerrogativas que pretendem garantir que cada um de nós não caminhe nu, desprovido de um manto de penumbra, numa sociedade que sabe cada vez mais acerca de cada indivíduo. É um direito a não viver num mundo com paredes de vidro, é um direito a não ser transparente, por isso, desenha-se como um direito de proteção, de sentido negativo".

Segundo o Parecer elaborado pela CNPD sobre a Proposta de Lei n.º 79/XIII/2.ª (Parecer 38/2017), "…quando consideramos a tutela prevista pelo artigo 7.º da Carta, pelo artigo 8.º da CEDH e pelos artigos 26.º, 34.º e 35.º da CRP, esta tem de ser assegurada, segundo uma leitura atualista, cobrindo todas as realidades de comunicação que a tecnologia hoje oferece e, portanto, protegendo as dimensões humanas fundamentais que por via dos tratamentos dos dados pessoais são atingidas" (p. 3). Também significante é o Parecer N.º 24/2017 da CNPD, tornando-se perentório quanto à opinião de que o projeto de lei 480/XIII/2.ª (CDS-PP) visa conferir natureza criminal ao acesso a dados pessoais, no sentido em que "para que esse acesso se constitua como constitucionalmente aceitável e, ao mesmo tempo, retirar essa natureza criminal para que se mantenham prerrogativas de atuação compreensíveis, dentro das fronteiras de atribuições dos SIRP e sujeitas à sua reconhecida especificidade, como é disso exemplo o recurso ao segredo de Estado", em que, em contrapartida, "sincronizadamente se constituem como inadmissíveis no quadro do acesso e utilização dos dados de comunicações dos visados, a quem não pode deixar de se reconhecer um conjunto de garantias e direitos constitucionalmente

previstos", o que constitui "uma natureza híbrida" no processo de acesso, que acaba por "negar esses mesmos direitos constitucionalmente consagrados aos visados pela produção de informações/investigações dos SIRP" (p. 17).

O Art. 26.º, n.º 1 da CRP estatui que "A todos são reconhecidos os direitos à liberdade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação", pelo que caberá à lei estabelecer "garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias" (n.º 2 do mesmo artigo).

Nesta égide importa referir ainda o Art. 34.º, n.º 1 da CRP, pela proteção da inviolabilidade do domicílio e do sigilo da correspondência e dos outros meios de comunicação privada, de forma a 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" (n.º 4 do mesmo artigo).

Importa rever no domínio do Código Civil o seu Art. 70.º, que estabelece que "a lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça à sua personalidade física ou moral" e o Art. 80.º – com a epígrafe "Direito à reserva sobre a intimidade da vida privada" – estatui que: "1. Todos devem guardar reserva quanto à intimidade da vida privada de outrem. 2. A extensão da reserva é definida conforme a natureza do caso e a condição das pessoas".

2.2. Na União Europeia

A União Europeia, ao criar as suas políticas comuns de manutenção do espaço partilhado de liberdade, segurança e justiça, deu azo à criação de um enquadramento jurídico no sentido da proteção dos dados pessoais e para a cooperação entre entidades judiciárias e policiais. O Tratado de Lisboa explicitou que "A União funda-se nos valores do respeito pela dignidade humana, da liberdade, da democracia, da

igualdade, do Estado de direito e do respeito pelos direitos do Homem" (Art. 2.º do TFUE).

O Art. 16.º salvaguarda o "direito à proteção dos dados de caráter pessoal", ao prever que o Parlamento Europeu e o Conselho devem estabelecer "normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do direito da União, e à livre circulação desses dados", conforme o n.º 2.

Constituindo a proteção dos dados pessoais, bem como o respeito pela vida privada, valores fundamentais, os Art.os 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia são elevados à base jurídica de enquadramento legal das medidas propostas da União Europeia neste âmbito. Dado aos desafios colocados pela evolução tecnológica constante, bem como das ameaças que nos determinamos a combater, desde o terrorismo à criminalidade organizada, tem vindo a ser estabelecido um conjunto de instrumentos legislativos no âmbito da Proteção de Dados Pessoais. O Decreto-Lei n.º 188/81, de 2 de julho, fundou os princípios gerais das comunicações, sendo que, posteriormente, as 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, estabeleceram o tratamento dos dados pessoais gerados pelas telecomunicações. Refira-se a este propósito a imposição de limites "pela sua natureza e pelo fim a que se destinam, é garantida a inviolabilidade e o sigilo dos serviços de telecomunicações de uso público" que decorre do n.º 2 do Art. 17.º da Lei n.º 91/97, de 1 de agosto.

Mais tarde, viria a ser aprovada a Lei de Proteção de Dados Pessoais – Lei n.º 67/98, de 26 de outubro que transpôs para o ordenamento jurídico nacional 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. No seu Art. 2.º refletia que o "tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais".

Posteriormente, surgiu a Lei n.º 69/98, de 28 de outubro – que transpôs a Diretiva 97/66/CE, do Parlamento Europeu e do Conselho. Esta Lei veio regular o tratamento de dados pessoais e a proteção da privacidade no setor das telecomunicações, suplementando as disposições da Lei da Proteção de Dados. Através deste diploma, o prestador de serviços de telecomunicações ficou obrigado a adotar um conjunto de medidas técnicas e organizacionais conducentes à garantia da segurança dos serviços de telecomunicações acessíveis ao público (Art. 4.º, n.º 1), bem como, garantir a confidencialidade e o sigilo das comunicações através dos serviços de telecomunicações acessíveis ao público e das redes públicas de telecomunicações (Art. 5.º, n.º 1).

Importa igualmente referir nesta senda, os Decretos-Leis n.os 290-A/99 e 290-B/99, ambos de 30 de julho, a partir dos quais, no âmbito da exploração dos serviços, os seus prestadores ficam encarregues de "providenciar, no que for necessário e estiver ao seu alcance, no sentido de assegurar e fazer respeitar, nos termos da legislação em vigor, o sigilo das comunicações do serviço prestado, bem como o disposto na legislação de proteção de dados pessoais e da vida privada" (cf. alínea e) do n.º 2).

A Diretiva 97/66/CE viria a ser revogada, dando lugar à 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 (mais comumente denominada Diretiva relativa à privacidade e às comunicações eletrónicas). Esta nova Diretiva procurou salvaguardar o respeito dos direitos fundamentais e reforçar o cumprimento dos princípios contemplados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais.

A Diretiva 2002/58/CE promoveu, sobretudo, uma *proteção horizontal* dos dados pessoais e da privacidade dos utilizadores de serviços de comunicações publicamente disponíveis autonomamente das tecnologias utilizadas por estes, adaptando, desta forma, a Diretiva que revogou ao "desenvolvimento dos mercados e das tecnologias de comunicações eletrónicas". Tal facto, deveu-se às capacidades e possibilidades de tratamento de dados pessoais que o acesso às redes digitais

permitiu. No seu considerando 6.º, é referido que a Internet estaria a "derrubar as tradicionais estruturas do mercado, proporcionando uma infraestrutura mundial para o fornecimento de uma vasta gama de serviços de comunicações eletrónicas", presenteando a "capacidade crescente em termos de armazenamento e de processamento informático de dados relativos a assinantes e utilizadores".

A Diretiva 2002/58/CE (transposta pela Lei n.º 41/2004, de 18 de agosto que revoga a Lei n.º 69/98) previu no seu Art. 15.º, que os Estados-Membros pudessem adotar medidas legislativas no sentido de restringir direitos e obrigações previstas no Art. 5.º ("Confidencialidade das Comunicações) e 6.º (Dados de Tráfego") e nos n.os 1 a 4 do Art. 8.º e 9.º ("Dados de Localização para além dos dados de tráfego"), sempre que as devidas restrições constituíssem uma "medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional, a defesa, a segurança pública, e a prevenção, a investigação, a deteção e a repressão de infrações penais ou a utilização não autorizada do sistema de comunicações eletrónicas" (n.º 1).

Consideramos assim que as Diretivas comunitárias suprarreferidas, vulgarmente consideras *Privacy Directives* (95/46/CE, 97/66/CE e 2002/58/CE) contribuíram sobremaneira para a proteção que viria a ser concedida em relação aos dados pessoais pelos Estados Membros da UE, em virtude da obrigatoriedade da sua transposição[111]. Devemos considerar também o Regulamento n.º 45/2001, do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados. Cumpre neste sentido, referir o Regulamento 2016/679, do Parlamento Europeu e do Conselho, relativo à proteção das pessoas singulares no que diz respeito ao tratamento

[111] CATARINA SARMENTO E CASTRO - *O direito à autodeterminação informativa e os novos desafios gerados*…, 2005, p. 8.

de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE, bem como as Diretivas 2016/680[112] e 2016/681[113], do Parlamento e do Conselho.

Tendo em linha de consideração o n.º 4 do Art. 1 da Lei n.º 41/2004, de 18 de agosto[114], importa salvaguardar a admissibilidade prevista: "As excepções à aplicação da presente lei que se mostrem estritamente necessárias para a protecção de actividades relacionadas com a segurança pública, a defesa, a segurança do Estado e a prevenção, investigação e repressão de infracções penais são definidas em legislação especial", ou seja, não impede a possibilidade de existência de legislação específica que restrinja em alguma medida a sua aplicação, nomeadamente, no que respeita à inviolabilidade das comunicações, no decorrer de investigação e repressão de infrações penais[115].

Assim, na sequência deste diploma, de forma a criar um conjunto amplo de garantias concertantes ao modo de acesso e conservação dos dados de tráfego e de localização das comunicações com finalidades de investigação, deteção e repressão de crimes graves por parte das autoridades, foi aprovada a Lei n.º 32/2008[116], de 17 de julho. A Lei n.º 32/2008, de 17 de julho, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes publicas de comunicações consiste numa transposição da Diretiva n.º 2006/24/CE, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, definindo eficazmente "crimes graves" (são definidos no Art. 2.º, n.º 2, al. g) como "crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada,

[112] Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão das infrações penais ou execução de sanções penais, e à livre circulação desses dados.
[113] De 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.
[114] Que revoga a Lei n.º 69/98, de 28 de outubro
[115] A Lei n.º 41/2004, de 18 de agosto, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, foi alterada pela Lei n.º 46/2012, de 29 de agosto, que transpõe a Diretiva n.º 2009/136/CE.

[116] De referir que a Comissão Nacional de Proteção de Dados considerou que a Lei n.º 32/2008 contraria a Constituição e o Direito da EU, distinguindo um conjunto de argumentos explanados na Deliberação n.º 641/2017.

sequestro, rapto e tomada de reféns, crimes contra a identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima". A mesma Lei apresenta os prazos de conservação (Art. 6.º), bem como nas garantias processuais inerentes (Art. 9.º). Os "Dados" constituem "os dados de tráfego e os dados de localização, bem como os dados conexos necessários para identificar o assinante ou utilizador".

A Agenda Europeia para a Segurança (2015) colocou em especial destaque o respeito pelos valores inerentes às sociedades abertas, nomeadamente ao princípio do Estado de Direito e aos direitos enunciados na Carta da União Europeia, limitando as restrições destes últimos a estritos critérios de necessidade e proporcionalidade[117], favorecendo as respetivas garantias de controlo jurisdicional (Art. 52.º, n.º 1).

No entendimento dado pelo Tribunal de Justiça da União, que pelo Acórdão *Digital Rights Ireland Ltd*. (Processos n.ºs C-293/12 e C-594/12) veio a invalidar a Diretiva 2004/26/CE, os "dados [de tráfego], considerados no seu todo, são suscetíveis de permitir tirar conclusões muito precisas relativamente à vida privada das pessoas cujos dados foram conservados, como hábitos da vida quotidiana, os locais em que se encontraram de forma permanente ou temporária, as deslocações diárias ou outras, as atividades exercidas, as relações sociais e os meios sociais frequentados", considerando que a ingerência nos direitos fundamentais garantidos pelo Art. 7.º (Respeito pela vida privada e familiar) e pelo Art. 8.º (Proteção de dados pessoais) da Carta "é de grande amplitude e deve ser considerada particularmente grave". Porém, o acórdão vai mais longe, referindo que a conservação e a utilização posterior dos dados serem efetuadas sem que o assinante ou o utilizador registado disso sejam informados é suscetível de gerar no espírito das pessoas abrangidas, o sentimento de que a sua vida privada é objeto de vigilância constante (tal como

[117] Para JORGE BACELAR GOUVEIA (2015, p.33) *In Enciclopédia de Direito e Segurança*: "O *princípio de proporcionalidade* deve ser inserido na ideia geral do princípio do Estado de Direito como dimensão material do mesmo". A sua configuração "assenta numa limitação material interna à atuação jurídico-pública de caráter discricionário, contendo os efeitos excessivos que eventualmente se apresentem na edição das providências de poder público de cariz ablatório para os respetivos destinatários". Assim sendo, trata-se de um conceito desdobrável em três vertentes: a) a adequação; b) a necessidade; c) a racionalidade ou proporcionalidade em sentido estrito (p.34).

constatou o advogado-geral nos n.os 52 e 72 das suas conclusões). Neste sentido, é crucial para o Tribunal que se analise a "proporcionalidade da ingerência observada".

O referido Acórdão conclui que "no que respeita ao carácter necessário da conservação dos dados imposta pela Diretiva 2006/24, cabe observar que é verdade que a luta contra a criminalidade grave, designadamente a criminalidade organizada e o terrorismo, assume primordial importância para garantir a sua segurança pública, e a sua eficácia pode depender em larga medida da utilização das técnicas modernas de investigação. No entanto, tal objetivo de interesse geral, por muito fundamental que seja, não pode, por si só, justificar que uma medida de conservação como a que foi instituída pela Diretiva 2006/24 seja considerada necessária para efeitos da referida luta"[118].

Fica assim a dúvida se deverão ou não os prestadores de serviços de comunicações móveis recusar-se a conservar os dados de tráfego. Quanto a esta questão, ou seja, se os operadores podem recusar-se a aplicar os artigos 4.º a 6.º e 9.º da Lei n.º 32/2008, de 17 de julho, pelos quais surge a obrigação de conservação de dados de tráfego e a obrigação da sua transmissão às autoridades competentes sempre que haja despacho devidamente fundamentado de um juiz de instrução, DAVID SILVA RAMALHO & JOSÉ DUARTE COIMBRA (2015)[119] distinguem entre se "devem" ou "podem" fazê-lo, por apresentação de uma resposta dual: 1 – "não o devem fazer", no sentido em que "não têm essa obrigação", pela exigência da não aplicação do Direito nacional contrário ao Direito da União Europeia, num princípio do primado[120]. Assim, "por mais extensiva que seja a dimensão 'Estado' para efeitos de aplicação do primado, não parece possível afirmar que sujeitos privados estejam obrigados a desaplicar leis nacionais em sua obediência", não sendo previsível, por isso, qualquer consequência jurídica para o facto dos prestadores continuarem a

[118] MANUEL D. MASSENO (2014), revela uma simplificação impressionista que "enquanto a Diretiva 2006/24/CE do Parlamento Europeu, de 15 de março de 2006 correspondeu a uma rendição da Europa perante o temor, e o terror, da *Al-Qaeda*", o Acórdão de 8 de abril de 2014 (*Digital Rights Ireland*) "foi proferido no quadro da indignação cidadã face à vigilância generalizada e sem controle independente pelos Estados, denunciada por Edward Snowden".

[119] v. "A declaração de invalidade da diretiva 2006/241CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves", In *Liber Amicorum: Manuel Simas Santos*, 2015

[120] Cf. prevê o n.º 3 do Art. 4.º do TUE

aplicar a Lei n.º 32/2008. Em alternativa, 2 – "O certo, porém, é que o podem fazer" por "não sofrerem consequências" pela não conservação ou transmissão de dados conservados, "*maxime*, a aplicação das contraordenações previstas no Art. 12.º da Lei n.º 32/2008, de 17 de julho". Neste caso vigora a regra do primado, bem assim o dever de desaplicação de atos nacionais em toda a sua extensão. Assim, DAVID SILVA RAMALHO & JOSÉ DUARTE COIMBRA (2015) opinam sobre uma aplicação do anterior regime da Lei n.º 41/2004[121], em que o termo de conservação de dados de tráfego ocorre durante o período de contestação ou reclamação pagamento após a prestação do serviço (seis meses)[122].

Para o estudo adiante da Comissão de Controlo Prévio visada no Decreto n.º 426/XII, interessa realçar o ponto 62 do Acórdão *Digital Rights Ireland*, na medida em que "o acesso aos dados conservados pelas autoridades nacionais competentes [ao abrigo da Diretiva 2006/24] não está sujeito a 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".

A Sentença do Tribunal Constitucional da Alemanha (Sentença n.º 10/2010, de 2 de março) viria a considerar inconstitucional a Lei da Emenda da Vigilância das Telecomunicações (*Gesetz zur Neuregelung der Telekommunikationsüberwachun*), de 21 de dezembro de 2007, advinda da transposição da Diretiva de 2006, fundamentado a decisão no facto da Lei ter provocado um legítimo alarme social, ter restringido acentuadamente Direitos Fundamentais garantidos pela *Grundgezets* (Art. 10.º sobre a Confidencialidade das Telecomunicações e o Direito à Autodeterminação Informacional) e não ter sido previsto o Princípio da Proporcionalidade e da Certeza, ao não especificar claramente os crimes a que seria aplicável, possibilitando o acesso

[121] Nos termos do n.º 3 do Art. 6.º, acrescentado a Lei n.º 23/96, de 26 de julho, na redação dada pela Lei n.º 12/2008, de 26 de fevereiro.

[122] Assim os autores verificam, que a Lei nacional de converteu "em instrumento de cumprimento facultativo, isto da ótica dos sujeitos privados primariamente destinados à sua aplicação" - tratando-se de "uma hipótese – certamente rara, mas habilitada pelos efeitos específicos do Acórdão DRI".

a um número excessivo de autoridades. A acompanhar esta Decisão, também o Tribunal Constitucional da Roménia (Decisão n.º 1258, de 8 de outubro de 2009) considerou inconstitucional a Lei n.º 298/2008. A fundamentação desta sentença apoiou-se no facto da medida poder perigar os próprios direitos fundamentais ao segredo da correspondência, à privacidade e à liberdade de expressão, protegidos pela Constituição Romena (Art.os 26.º, 28.º e 30.º), a DUDH (Art.os 12.º e 19.º) e a CEDHLF (Art. 8.º e 10.º) [123].

De grande amplitude foi também o Acórdão *Schrems*, de 6 de outubro de 2015 (C-362/14), pela posição do Tribunal ao apontar que, "No que respeita ao nível de proteção das liberdades e direitos fundamentais garantido dentro da União, uma regulamentação dessa proteção que implique uma ingerência nos direitos fundamentais garantidos pelos Art.os 7.º e 8.º da Carta deve, segundo a jurisprudência constante do Tribunal de Justiça, estabelecer regras claras e precisas que regulem o âmbito e a aplicação de uma medida e imponham exigências mínimas, de modo a que as pessoas cujos dados pessoais estejam em causa disponham de garantias suficientes que permitam proteger eficazmente os seus dados contra os riscos de abuso e contra qualquer acesso e qualquer utilização ilícita desses dados".

Nesta senda, não podemos de deixar de fazer referência à já consolidada jurisprudência do TJUE. Desde logo, o Acórdão de 22/10/2001, *Roquette Frèrres* (Processo n.º C-94/00) apontou para a existência de um "princípio geral de direito comunitário que consagra a proteção contra as intervenções arbitrárias e desproporcionadas do poder público na esfera da atividade privada de uma pessoa singular ou coletiva".

Consideramos que, o TJUE tem acatado a constitucionalização da proteção de dados pessoais constante quer no Tratado sobre o Funcionamento da União Europeia, quer na Carta dos Direitos Fundamentais da União Europeia. O princípio do primado do direito da União sobre os direitos nacionais é acolhido na nossa Constituição através do n.º 4.º do Art. 8.º, quando refere que "As disposições dos tratados que regem a União Europeia e as normas emanadas das duas instituições, no exercício

[123] v. MANUEL DAVID MASSENO (2010) - *Será constitucional o regime de acesso aos "Dados de Tráfego?*

das respetivas competências, são aplicáveis na ordem interna, nos termos definidos pelo direito da União, com respeito pelos princípios fundamentais do Estado de direito democrático". Devemos atender, no entanto, ao facto do Direito da UE não ser aplicável aos serviços de inteligência, que estão sob a alçada da soberania nacional, regulados por isso através de legislação especial, como sucede em Portugal por decorrência da alínea q) do Art. 164.º da CRP.

2.3. Os Instrumentos Internacionais

Passamos de seguida a elencar um conjunto de instrumentos de cariz internacional que regulam e salvaguardam o acesso aos dados de telecomunicações. Algumas das passagens e artigos que mencionados não são exclusivos da proteção de dados pessoais, na medida em que antes garantem a proteção da vida privada.

Importa equacionar nesta dimensão o Art. 12.º da Declaração Universal dos Direitos do Homem (DUDH) ao declarar que "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência".

Porquanto, o Art. 8.º da Convenção Europeia dos Direitos do Homem (CEDH) estabelece que "qualquer pessoa tem o direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência". Nos termos do n.º 2 do mesmo artigo, é aludido que "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 prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros".

Por seu turno, é de referir a importância dos Art.os 7.º ("Respeito pela vida privada e familiar") e 8.º ("Proteção de dados pessoais") contemplados da Carta dos Direitos Fundamentais da União Europeia (CDFUE). Enquanto o Art. 7.º prevê que "Todas as pessoas têm o direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações", o Art. 8.º estipula que "Todas as pessoas têm

o direito à proteção de dados de carácter pessoal que lhes digam respeito" (n.º 1), devendo estes dados serem "objeto de um tratamento leal" (n.º 2) – assegurando que o cumprimento destas normas é sujeito a fiscalização por "parte de uma autoridade independente" (n.º 3).

Cabe igualmente referir, a propósito do n.º 2 do referido Art. 8.º da CDFUE, o Acórdão de 09/11/2010, *Volkerund Markus Schecke* (Processos n.ºs C-92/09 e C-93/09), quando o Tribunal de Justiça considerou que este direito estaria indissocialvelmente relacionado com o direito ao respeito da vida privada consagrado no Art. 7.º da CDFUE (de acordo com o ponto 47 do referido Acórdão).

No mesmo sentido, refira-se o caso *Malone c. Reino Unido* (Acórdão de 02/08/1984, queixa n.º 8691/79), na medida do qual o TEDH entendeu que o acesso e o uso de dados respeitantes a tráfego de comunicações constituem matéria diretamente relacionada pelo âmbito do já exposto Art. 8.º da Carta Europeia dos Direitos do Homem.

3. O Acórdão n.º 403/2015 do Tribunal Constitucional

Nos termos da alínea d) do n.º 1 do Art. 197.º da Constituição, a proposta de Lei n.º 345/XII/4.ª foi aprovada por larga maioria na Assembleia da República, dando lugar ao Decreto da Assembleia da República n.º 426/XII[124].

Como justificação do regime da Proposta de Lei n.º 345/XII/4.ª, no contexto da ainda recente Estratégia Nacional de Combate ao Terrorismo, aprovada pela Resolução do Conselho de Ministros n.º 7-A, de 20 de fevereiro, bem como pelos "desafios que são colocados pelas novas ameaças à segurança nacional", considerando-se "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

[124] Pela introdução de um novo quadro orgânico-funcional, o Decreto n.º 426/XII da Assembleia da República visou reunir e harmonizar ao longo do mesmo diploma um conjunto de aspetos que se encontravam dispersos entre outros diplomas legais. Desde logo, propõe revogar a Lei n.º 9/2007, de 19 de fevereiro, bem como o Decreto-Lei n.º 225/85, de 4 de julho, o Decreto-Lei n.º 370/91, de 7 de outubro e do Decreto-Lei n.º 254/95, de 30 de setembro.

Convenção Europeia dos Direitos do Homem". Desta forma, 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".

A Proposta de Lei n.º 345/XII/4.ª cria uma entidade, a "Comissão de Controlo Prévio"[125] (Cf. Art.os 35.º a 38.º), que visaria conceder a autorização prévia do "acesso à informações e dados necessários, numa dada operação, segundo um exigente procedimento legal, que visa a sindicância do acesso a dados pessoais que possa por em causa a reserva da intimidade da vida provada, a efetuar por três juízes".

Desta forma, "o que se pretende é, não o acesso a conteúdo 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, (…), matéria que tem melhor inserção sistemática em sede do Art. 78.º (Acesso a dados de informação)".

Ao abrigo do n.º 1 do Art. 278.º da CRP, o Presidente da República submeteu um pedido de fiscalização abstrata preventiva da constitucionalidade referente à norma constante do n.º 2 do Art. 78.º do Decreto n.º 426/XII da Assembleia da República, que "Aprova o Regime Jurídico do Sistema de Informações da República Portuguesa". Importa desde logo considerar que o regime foi aprovado por excessiva maioria, superior a dois terços dos Deputados em efetividade de funções.

Como ponto de partida para a análise do Ac. do TC n.º 403/2015, importa apresentarmos o artigo sujeito a apreciação. Neste caso, o Art. 78.º está presente na seção 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):

[125] Quando à sua composição, de acordo com o Art. 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".

> "Artigo 78.º
> Acesso a dados e informação
>
> 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, contidos 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 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".

Na sessão plenária de 27 de agosto de 2015, o Tribunal Constitucional pronunciou-se sobre a inconstitucionalidade da norma constante no n.º 2 do Art. 78.º do referido Decreto, na medida em que entendeu que o preceito sindicado – ao permitir que os Oficiais dos Serviços de Informações da República Portuguesa possam aceder a dados de tráfego, de localização ou outros dados conexos de comunicações, mediante a autorização prévia da Comissão de Controlo Prévio – comporta uma ingerência nas telecomunicações proibida pelo n.º 4 do Art. 34.º da Constituição. Da mesma forma, o Tribunal Constitucional entendeu que a autorização prévia e obrigatória da Comissão de Controlo Prévio não equivale ao controlo existente no âmbito do processo criminal.

Esta decisão foi explanada no Ac. do TC n.º 403/2015 (Processo nº 773/15), que iremos discorrer nesta seção. Importa referir que o Conselheiro Teles Pereira votou vencido esta decisão e que existiu declaração de voto pela Conselheira Maria Lúcia Amaral. Iremos discorrer sobre a argumentação clara e objetiva de ambos os Conselheiros ao longo deste segmento da dissertação, dada a riqueza discursiva das suas declarações.

Relembramos que, segundo o n.º 4 do Art. 34.º da CRP, "É proibida toda a inferência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvo os casos previstos na lei em matéria de processo criminal". Acatando o entendimento tomado pelo TC, a CRP estabeleceu de forma indireta um limite à atividade de *intelligence* através do Art. 34.º, n.º 4. Ou seja, a obtenção de informações através de meios técnicos, nomeadamente por via da "ingerência (…), nas telecomunicações e nos demais meios de comunicação" apenas pode ser viabilizada do decorrer do processo penal. Indiretamente, por força desta norma, a atividade de *Signals Intelligence* (SIGINT), mais propriamente por via de *Communications Intelligence* fica comprometida.

O Tribunal Constitucional começou por apresentar uma distinção entre o *direito à autodeterminação comunicativa*, pela vigência do Art. 34.º, n.º 4 da CRP, do *direito à autodeterminação informativa*, razão da existência do Art. 35.º da CRP. Desta forma, o Tribunal considerou que os dados de tráfego estão integrados no conceito de telecomunicações, por vigência da proibição da ingerência destes pelo Art. 34.º, n.º 4 da Constituição. Interessa aqui considerar que a Exposição de Motivos da Proposta de Lei do Governo que deu origem ao Decreto considerou que os dados de tráfego seriam considerados "dados pessoais", na medida do Art. 35.º da CRP e não ingerência nas comunicações, de acordo com o n.º 4 do Art. 34.º da CRP[126].

[126] Debruçando-nos na exposição de motivos, evidencia-se um acautelamento na medida em que: "Efetivamente, admite-se, no artigo 78.º da presente proposta 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)"

Face à norma constitucional do já referido Art. 34.º, n.º 4, importaria ao Tribunal Constitucional aferir se: "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 equivale ao controlo existente no processo criminal?"[127].

O Acórdão começa desde logo por delimitar o objeto de análise, neste caso, refere-se somente ao "acesso aos *metadados*, enquanto dados – estruturais ou descritivos – produzidos no âmbito ou em conexão com um processo de telecomunicações, registados e conservados pelas respetivas operadoras" – dado que o requerente transcreve no Art. 3.º o segmento da Exposição de Motivos da Proposta de Lei n.º 345/XII. Desta feita, não é objeto de análise a possibilidade de acesso dos Oficiais do SIS e do SIED a informação de outra natureza senão as inerentes ao processamento das telecomunicações. Ao que o TC esclarece que a fiscalização preventiva da constitucionalidade da norma contida no n.º 2 do Art. 78.º não acarreta a possibilidade de acesso dos Oficiais de Informações a informação bancária e fiscal, conforme prevista no Decreto n.º 426/XII.

O Acórdão começa por demonstrar a necessidade de "caracterizar o tipo de dados em causa e saber se o acesso aos mesmos é merecedor de proteção constitucional". Neste sentido, é acompanhado o Art. 2.º, n.º 1, alínea d), da Lei n.º 41/2004, de 18 de agosto, sobre Segurança nas Telecomunicações, que 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 de faturação da mesma".

Nesta senda, o TC informa que 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" encontram-se diretamente relacionados com o conceito de *dados de tráfego*, pela aplicação do disposto no Art. 6.º da Diretiva n.º

[127] Ou seja, "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".

2002/58/CE[128], e do disposto na Lei n.º 41/2004, de 18 de julho (conforme explicitamos anteriormente).

Interessou ao TC começar por delinear o "tipo de dados em causa", para assim partir para a consideração se o acesso aos mesmo é merecedor de proteção constitucional (Cf. ponto 9 do Acórdão). O TC considera que numa dada 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".

Entende que devido ao facto de se tratar de informação que permite "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", são considerados "dados de tráfego", afirmando que a definição dos mesmo já se encontra explanada no nosso ordenamento jurídico[129].

O Acórdão discorre sobre a regulamentação legal do acesso a dados de comunicações, desde logo sobre o holofote comunitário, passando posteriormente pelos vários instrumentos internacionais.

Compreende o TC que "O acesso aos dados das comunicações efetivamente realizadas ou tentadas põe em causa direitos fundamentais das pessoas envolvidas no ato comunicacional", visto que "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*)". Entende desta forma que, "mesmo que não haja acesso ao conteúdo, a interconexão entre dados de tráfego pode fornecer um perfil complexo e completo da

[128] Cf. o considerando 35 da Diretiva "Nas redes móveis digitais, os dados de localização que fornecem a posição geográfica do equipamento terminal do seu utilizador móvel são tratados para permitir a transmissão das comunicações. Esses dados são dados de tráfego, abrangidos pelo disposto no artigo 6.º da presente directiva". Excluindo do âmbito da norma objeto do pedido os dados decorrentes do facto de que "as redes móveis digitais podem ainda ter a capacidade de tratar dados de localização que são mais precisos do que o necessário para a transmissão de comunicações e que são utilizados para a prestação de serviços de valor acrescentado, tais como serviços que prestam aos condutores informações e orientações individualizadas sobre o tráfego".

[129] Assim, remete para o Art. 2.º, n.º 1, alínea d), da Lei n.º 41/2004, de 18 de agosto, já referido no Capítulo I, ponto 2 deste estudo ("Das significações dos Dados de Telecomunicações e Internet"). O Acórdão faz igualmente referência ao Acórdão do Tribunal Constitucional n.º 241/2002, de 29/05/2002.

pessoa em questão" – com quem mais conversa, que lugares frequenta, quais os seus horários, etc.". Deste modo, "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" – cf. ponto n.º 12 do arresto.

O Acórdão faz ainda referência à proteção da "liberdade de ação", neste sentido, um direito ao desenvolvimento da personalidade, de acordo com o qual, no relacionamento entre indivíduos, a "condução da vida de cada um é autoconformada pela sua atuação"[130]. Seguindo com a referência à "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 moderadamente 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)". Em suma, o TC refere que estes direitos encontram a sua proteção consagrada no Art. 26.º da CRP, na medida em que se encontram profundamente interligados, "constituindo a reserva da intimidade da vida privada uma dimensão do direito, mais amplo, referente ao desenvolvimento da personalidade"[131].

A Acórdão em análise a responder à primeira questão do Requerente ("deve o acesso aos dados de tráfego considerar-se uma ingerência nas telecomunicações para os efeitos previstos na norma constitucional?") remete para o precedente Acórdão nº

[130] Prossegue o Acórdão no ponto n.º 13 que "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*". Ou seja, "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", na justa medida em que "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".

[131] A este propósito o Acórdão 403/2015 faz referência à primeira formulação da definição do conteúdo do direito à reserva da vida privada, de acordo com o Acórdão n.º 128/92: "De modo que, na jurisprudência constitucional, as *comunicações privadas*, englobando o *conteúdo* e *circunstancialismos* em que as mesmas 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".

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".

Nesta senda, o TC considera que "também se entende que a área de proteção do sigilo das comunicações consagrada no n.º 4 do artigo 34.º da CRP[132], compreende tanto o conteúdo da comunicação como os dados de tráfego atinentes ao processo de comunicação". Dado que "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".

Relativamente à segunda questão colocada pelo Requerente ("pode considerar -se que a autorização prévia e obrigatória da Comissão de Controlo Prévio equivale ao controlo existente no processo criminal?"), após o TC definir o quadro de incidência da lei restritiva do direito à inviolabilidade das comunicações por via de "matéria de processo criminal", debater o conflito de um direito fundamental com outros direitos ou valores comunitários e aferir se a atividade dos Oficiais de informações do SIRP previstas nos termos do Decreto n.º 426/XII é considerada como atividade no âmbito da investigação criminal, adverte que:

> "…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

[132] Como explicitado pelo TC, "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". Este entendimento é considerado pelo facto de que "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" (p.8258)

> 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)"[133].

Importa ao TC que apesar da sua composição, a Comissão de Controlo Prévio não deixa de configurar um órgão administrativo, tornando-se "irrelevante" se é composta por magistrados judiciais – visto que estes não atuaram "na veste de entidade judicial", mas antes como membros da referida Comissão administrativa[134]. Pelo que o sistema de autorização previa concedida pela Comissão para o acesso e manutenção dos dados de tráfego não se poderá sequer equiparar ao controlo existente num processo penal, uma vez 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".

Acresce que o TC considerou que a atuação da referida Comissão de Controlo Prévio não se encontra devidamente garantida pelo Decreto em análise, visto que "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* de dados" (cf. ponto n.º 21 do Acórdão)[135].

[133] Ponto n.º 20 do Acórdão (parte inicial).
[134] Para o TC "…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" (Cf. ponto n.º 22 do Acórdão).
[135] Segundo o entendimento do TC, releva o facto de se tratar de um acesso aos dados de tráfego concedido sem o "conhecimento dos visados", o que deve ponderar um conjunto de "regras claras e determinadas que permitam saber até onde pode ir a ingerência", mantendo a necessária *segurança jurídica* e evitando o risco de arbitrariedade do acesso.

De acordo com o explanado no ponto n.º 21 do Acórdão, e acompanhando anteriores decisões do TEDH[136], o TC considera que "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"; da mesma forma, deve existir na lei com previsão dos *casos específicos* em que o acesso deve acontecer, prevendo a "fixação de um *limite de duração* da medida[137], e das regras e prazos para a eliminação dos dados de tráfego" – visto que, "Só assim se poderá falar de uma ingerência determinável e que garanta segurança jurídica aos interessados". Veremos aquando a análise da Lei Orgânica n.º 4/2017, de 25 de agosto, que o legislador viria a acautelar devidamente estas garantias.

O TC critica igualmente "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", visto que esta circunstância "também não oferece suficiente segurança à defesa dos direitos e interesses dos cidadãos" (cf. ponto n.º 23 do Acórdão).

Pelas razões expostas o Tribunal Constitucional respondeu negativamente à segunda questão colocada pelo Requerente, concluindo que "a Comissão Prévia de Controlo é um órgão administrativo que não tem poderes equivalentes a uma intervenção em processo criminal".

A Conselheira Maria Luísa Amaral votou a decisão do TC, contudo, não defendeu os fundamentos que lhe deram forma, acreditando que a base do

[136] Nomeadamente o Acórdão de 06/06/2006, *Segerstedt-Wiberg e outros c. Suécia* (queixa n.º 62332/2000); Acórdão de 02/08/1984, *Malone c. Reino Unido* (queixa n.º 8691/79); e Acórdão de 16/02/2000, *Amann c. Suíça 95* (queixa n.º 27798/95), entre outros.

[137] No ponto n.º 22 do Acórdão 403/2015, o TC retoma que "a norma [do n.º 2 do artigo 78.º do Decreto nº 426/XII] 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, porque os termos previstos na alínea c) do n.º 2 do artigo 4.º não oferecem a necessária "segurança jurídica aos potenciais lesados", uma vez que "resulta indeterminado o que podem constituir «atos que, pela sua natureza, possam alterar ou destruir o Estado de Direito democrático constitucionalmente estabelecido»". O TC considera que se trata de "uma verdadeira *indeterminabilidade*, que pode ser facilmente manipulável para permitir um acesso arbitrário aos dados de tráfego das comunicações".

entendimento deverá situar-se no facto da legislação em análise não cumprir as exigências que decorrem do disposto no n.º 2 do Art. 18.º da CRP ("A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição"), assim:

> "… a norma impugnada não definia com a precisão necessária os limites da intervenção administrativa na liberdade individual. A exigência de reserva da lei, na sua dimensão material, não se encontrava portanto (em meu entendimento) neste caso cumprida. Dizer, como de dizia no n.º 2 do Art. 78.º do Decreto da Assembleia, que tal intervenção seria legítima quando implicasse a adoção dos meios «necessário, 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" (ponto n.º 6 da declaração de voto).

A Juíza Conselheira revela ainda que, o disposto na alínea c) do n.º 2 do Art. 4.º do Decreto n.º 426/XII, "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" [138].

A Conselheira comenta ainda que:

> "A existência de Serviços de Informações – cujos fundamentos constitucionais o Tribunal pura e simplesmente não aborda -, numa ordem, como a nossa, de Estado de direito democrático, justifica-se pela

[138] O Art. 4.º, n.º 2, alínea c) do Decreto 426/XII determinava que os serviços de informações pudessem "desenvolver atividades de recolha, processamento, exploração e difusão de informações (…) adequadas 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".

> 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. […] 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" (ponto 4 da declaração de voto).

A Juíza Conselheira admite a possibilidade de imposição de "meios administrativos de defesa da Constituição, destinados a garantir a convivência adequada entre a 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 Art. 34.º da CRP". Carecendo, no entanto, ao incluir na regulação das competências do SIRP a possibilidade de interceção dos dados de tráfego, de uma gestão do acesso de forma clara e precisa da sua legitimidade, "de modo a não deixar à administração a liberdade de ponderar – sem quaisquer limites legais – da necessidade da interceção".

Complementarmente, conforme referimos inicialmente nesta seção, torna-se crucial discorrer sobre a declaração de voto do Juiz Conselheiro José António Teles Pereira, mais propriamente acerca do seu entendimento contrário, imprescindivelmente bem fundamentado, à decisão acolhida pelo Tribunal Constitucional.

O Juiz Conselheiro terá sido o único a contrariar a decisão do TC, no sentido em que o n.º 2 do Art. 78.º do Decreto n.º 426/XII é conforme com a Constituição, já que o acesso aos dados de tráfego pelos Oficiais de informações do SIRP 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". Da mesma forma que considera que (quanto à segunda questão do Requerente) autorização concedida pela 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", pelo que entende que nos termos constantes do Decreto n.º 426/XII não contrariar as exigências da Lei Fundamental"[139].

Desde logo, para o Juiz Conselheiro, o sentido que assumiu o n.º 4, Art. 34.º da CRP, mesmo após a 4.ª Revisão Constitucional[140] não se formou 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", daí 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*". Interpretativamente, o juiz considera que a referência ao "processo criminal" não afasta, "em termos absolutos", a viabilização de uma ingerência nos dados de tráfego pelos Serviços de Informações[141].

Reiteramos a posição do Juiz Conselheiro, quando advoga que, no quadro de uma democracia constitucional, são necessariamente colocados em debate os valores *Segurança e Democracia*, assumindo "a existência de uma tensão existencial

[139] Cf. p. 8279 do *Diário da República*, 1.ª série – N.º 182 – 17 de setembro de 2015.
[140] Sendo que na versão original do Art. 34.º era "4-…proibida toda a ingerência das autoridades públicas na correspondência e nas telecomunicações, salvos os casos previstos na lei em matéria de processo criminal". Em 1997, no sentido de admitir outros meios comunicacionais equivalentes que terão surgido, foram acrescentados ao texto constitucional os "demais meios de comunicação", no sentido de abarcar e adequar-se às realidades técnicas comunicacionais.
[141] "…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 acessos 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*…" – cf. pp. 8267 e 8268 do *Diário da República*.

permanentemente entre a adoção de políticas públicas promotoras de segurança e os valores democráticos". Alcança-se assim a perspetivação do domínio da segurança de acordo com o Art.º 27.º, n.º 1 da CRP, enquanto obrigação prestacional do Estado num contexto relacional de tensão entre valores constitucionais[142].

Desta forma, alcança 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[143] e potencie, ou torne racionalmente 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 (…), a espionagem e outros dos crimes contra o Estado, fundamentalmente os elencados no título v do Código Penal, constituindo estes exemplos paradigmáticos que justifica, essa intervenção precoce correspondem ao espaço de referência da defesa da Constituição".

Para o Conselheiro, é inequívoco distinguir o contexto de aquisição dos "ditos *metadados*", o que nos parece crucial e que não foi discorrido na fundamentação do Acórdão. Importa realçar, portanto, que podemos estar perante "(i) de uma aquisição de informação em larga escala, por transferência integral, para alguma autoridade

[142] Cabe-nos acompanhar as palavras do Conselheiro, na medida em que "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", de acordo com o facto de que "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" (Art. 18.º, n.º 2 da CRP).

[143] De acordo com o mesmo, "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".

pública, dos registos existentes num operador"[144], ou "(ii) de uma transferência individualizada, realizada (autorizada e controlada) caso a caso, com base numa suspeita concreta e individualizada". Desta forma denota que no caso específico da norma do Decreto n.º 426/XI, "… 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) (…), a considerar inválida a «Diretiva 2006/24/CE …»". Contrariamente ao que ocorre, "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"[145] (p. 8272 do *Diário da República*).

Importa ainda na declaração de voto a necessária advertência no sentido em que 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*", pelo que também decorre desta "classificação/enumeração sequencial" uma "inegável progressão de intensidade" (p. 8273). No que concerne à distinção entre dados de tráfego e dados de conteúdo, "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".

Apesar de o Ac. do TC n.º 403/2015 não aludir a uma inexistência de relação entre informações e investigação criminal, manteve-se num plano estritamente

[144] Tal como assistimos nos programas de recolha de dados produzidos pela *National Security Agency* (NSA), trazido a público por Edward Snowden, em 2013, bem como o denominado programa "*TEMPORA*", pelo *GCHQ* do Reino Unido.

[145] O Conselheiro realça assim que "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".

diferenciador da asserção material e orgânica de ambas as atividades. Contudo, tal como explana o Juiz Conselheiro, é atendível ainda o facto de se considerar que de acordo com uma "*geografia sistemática*" dos Serviços direcionados à produção de informações e das entidades ligadas ao processo criminal serem duas das áreas de atividade do Estado – "que, (…) 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".

Assim, lembra sobre esta relação que "forçoso, é concluir, desde logo, que se posiciona, a atividade de produção de informações, no âmbito de tutela preventiva de bens jurídicos protegidos pelo Direito Penal, no sentido de referenciáveis a ele, bens estes instrumentalmente servidos pelo direito processual penal", vigorando, por isso, uma relação de complementaridade sob a forma "conexões, não uma identidade" (p. 8275 do *Diário da República*). Contrariamente ao que é disposto no Ac. do TC n.º 403/2015 que refere que "Há, pois, uma distinção radical entre informações e investigação criminal, o que impede os oficiais de informação de intervirem no processo penal".

É ressalvado nesta senda que a importância respeitante às informações que podem ser recolhidas através dos dados de tráfego, na justa medida que são essenciais "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". De maneira tal que "negar a apontada redução teleológica[146] 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

[146] *A redução teleológica* proposta pelo Juiz Conselheiro é assumida através de duas opções interpretativas: "(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" (p. 8275).

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" (p. 8276).

Adverte ainda, para a necessidade de ilustrar o *princípio da proporcionalidade* da atuação em análise, concluindo que a norma do Art. 78.º, n.º 2 do Decreto n.º 426/XII acolhe: a) "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"; da mesma forma que denota "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)", sendo "manifestamente adequada (…) ao funcionamento do ciclo de informações, permitindo, designadamente, estabelecer a (essencial) conexão entre pessoas e lugares que aqueles Serviços tenham por carecidos de análise"[147]; e a *necessidade ou exigibilidade*, esta vertida na "impossibilidade de adoção de medidas menos intrusivas com os mesmo efeitos na prossecução do fim visado (…), precisamente para estabelecimento das apontadas conexões entre informações dispersas, em vista formação de um quadro informacional coerente"[148] (p. 8278 do *Diário da República*).

Em jeito de conclusão o Juiz Conselheiro admite a complexa verificação da *proporcionalidade em sentido estrito,* apontando um conjunto de elementos no caminho da "justa medida" da solução legislativa encontrada: "(i) a espécie de informação obtida[149]; (ii) a escala da informação[150]; (iii) o funcionamento das

[147] É feita uma referência ao fenómeno terrorista contemporâneo, na medida em que "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".
[148] Continua o Conselheiro referindo que "Os instrumentos resultantes daquele n.º 2 traduzem (…) «menor desvantagem possível» no (necessário) sacrifício de algo na esfera pessoal da reserva de intimidade, entendida como direito à autodeterminação informativa".
[149] Na medida em que os dados de tráfego afetem em menor grau a intimidade da vida privada do que os dados de conteúdo.
[150] Uma vez que não se trata de una "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", prevendo-se por isso um acesso pontual e concreto.

comissões de fiscalização; (…) (iv) o sentido das exigências de proporcionalidade" (p. 8278).

Nas palavras no Conselheiro, "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", pelo que "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" (p. 8279).

4. A importância dos Dados de Telecomunicações e Internet na produção de informações

O Clube de Berna, criado em 1971, é um grupo informal de Serviços de Informações de segurança, do qual fazem parte todos os países da União Europeia, a Noruega e a Suíça. Deste Clube, apenas aos Serviços de Informações portugueses não se previa a possibilidade de acesso a dados de tráfego, o que deixava os mesmos numa situação de aparente vulnerabilidade perante ameaças securitárias. Este aspeto faria com que a eficácia de uma cooperação efetiva entre Serviços congéneres saísse prejudicada por uma tal limitação, "ainda que de natureza constitucional, uma vez que a força de uma tal cooperação europeia depende, no fundo, da capacidade de resiliência do seu elo mais fraco", conforme explica o Parecer 2/2017 da CFDSIRP, a propósito da Proposta de Lei n.º 79/XIII/2.ª (GOV).

A dinâmica de *intelligence* procura sobretudo *conhecer "*os agentes de ameaça, descrever as suas estratégias e avaliar os potenciais impactos gerados pelas suas atividades"*; antecipar "*a emergência, evolução e mutação das ameaças, possibilitando a adoção atempada de estratégias que acrescentem resiliência em face da sua ação"*; identificar* "as vulnerabilidades especificas do Território Nacional, passiveis de serem infiltradas, exploradas ou subvertidas por agentes de ameaça

diversos"[151]. Ao encontro da explicação de JÚLIO PEREIRA (2012) "é vital para o SIRP, em apoio da função decisória do Estado, um acompanhamento permanente do ambiente estratégico internacional, onde assume particular importância o conhecimento que se obtém do Outro, atendendo à volatilidade dos seus atores e à necessidade de decisões tomadas em tempo real".

Discorridas as atribuições do SIRP, acompanhamos RUI PEREIRA & ALICE FEITEIRA (2015, p. 340), quando entendemos que a *intelligence* permite "tornar previsível (naturalmente num quadro de margem de erro aceitável) a evolução dessas realidades, determinadas em larga medida pelo impacto das decisões políticas e das estratégias sectoriais adotadas". Só assim, entendendo as informações como "um conjunto de elementos disponíveis, devidamente "recortados", valorados e interpretados, representam um instrumento de auxílio à tomada de decisão política, de natureza estratégica e tática, e uma garantia na defesa dos valores estruturantes do Estado de Direito democrático".

Segundo ARMÉNIO MARQUES FERREIRA (2007, p .69), as informações constituem "elementos de conhecimento sistematizado em quadros interpretativos, através de critérios que sobrepõem a estrutura de sentido de relação causal […] produzidas através de método próprio e preservadas da atenção e conhecimento de terceiros", revelando aí os "dois traços distintivos essências: - um método próprio; - um regime de segredo". Visando desta forma a obtenção de um conhecimento específico e necessário à tomada de decisões, as informações contrastam com a recolha da prova tendente ao exercício da ação penal.

Em primeiro lugar devemos entender o facto de que a atividade de produção de informações é "eminentemente preventiva" ao combate a determina ameaça. Neste sentido, SÓNIA REIS & BOTELHO DA SILVA (2007) refletem que as informações têm por objetivo "proporcionar ao Decisor Político[152] um conhecimento da realidade

[151] Discurso do Diretor do SIS, Adélio Neiva da Cruz, na sessão de abertura do 1.º Painel do V Seminário sobre "Ameaças Assimétricas e Planeamento Estratégico", 12/12/2017, Reitoria da Universidade Nova de Lisboa. Disponível em https://www.sis.pt/pagina/88/discurso-do-diretor-do-sis, acedido a 01/06/2018.

[152] Da mesma forma, JÚLIO PEREIRA (2012[1.], p. 6) refere que os Serviços de Informações têm como tarefa fundamental "melhorar a qualidade das decisões políticas, especialmente as que se referem aos domínios de segurança e defesa". Para o efeito, prosseguem um "processo de análise recolhem, tratam, relacionam e

que permita decisões fundamentadas em certas matérias fundamentais para o interesse público, relacionadas com a segurança interna e externa da Sociedade Portuguesa e outros interesses económicos centrais. Possibilitando a adoção de políticas públicas adequadas nesses domínios, porque assentes num conhecimento rigoroso da realidade. Trata-se, em suma, de pesquisar informação, mas também de a integrar e analisar constantemente, com a luz própria que só uma visão de conjunto permite".

Decorre do Art. 32.º, n.º 3 da LQSIRP que "As informações e os elementos de prova respeitantes a factos indiciários da prática de crimes contra a segurança do Estado devem ser comunicados às entidades competentes para a sua investigação ou instrução". A investigação criminal é considerada no artigo 1.º da Lei n.º 49/2008, de 27 de agosto como "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 provas, no âmbito do processo". O Ac. do TC n.º 403/2015, refere a determinada altura 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".

Não podemos olvidar que o Art. 21.º da Lei n.º 30/84, de 5 de setembro incube o Serviço de Informações de Segurança à produção de informações que contribuam para prevenção de três tipos de crime: sabotagem, terrorismo e espionagem. Neste sentido, e como observa JÚLIO PEREIRA (2016), é certo que a ação de polícia "não pode ser cega", na justa medida em que "o seu planeamento e execução exigem informação". Desta forma, não será difícil precisar que "A qualidade da ação de polícia, em todas as suas vertentes e naturalmente também na prevenção e investigação criminais, depende também da qualidade das informações de que disponha"[153].

ultimam informações que entregam em estado acabado ao responsável político. Entre os principais critérios desse processo analítico estão as várias técnicas de recolha de informação (*Humint, Sigint* e *Osint*), de seleção de informação, de redação da informação e, por último, de correta classificação dessa mesma informação" - constituindo num processo de simplificação e facilitação do processo decisório.

[153] Op. Cit. *Liber Amicorum Manuel Simas Santos,* p. 801

Neste âmbito, SÓNIA REIS & M. BOTELHO DA SILVA (2007) delimitam preliminarmente as fronteiras da atividade de produção de informações através da distinção desta atividade com a atividade de polícia – que "consiste na manutenção da ordem pública", relevando ainda o facto de a atividade das Informações se situar "a montante da atividade de polícia e de investigação criminal por se desenvolver independentemente da existência de *notitia criminis* ou de concretas necessidades de manutenção da ordem pública". Neste aspeto, quando é circunscrita a questões relacionadas com a segurança "a atividade das informações visa prevenir a existência de circunstâncias propícias à prática de crimes e a perda de ordem e tranquilidades públicas".

Conforme realça JÚLIO PEREIRA (2016), resulta com elevado grau de certeza que a Lei-Quadro do SIRP procurou que os Serviços de Informações tivessem também "no cerne da sua missão institucional" a prevenção, "não da criminalidade em geral, mas de categorias de crimes que, pela sua gravidade, colocam em sério risco a sociedade e o próprio Estado de direito democrático".

Citando JÚLIO PEREIRA (2007), a propósito da segurança interna no relacionamento entre investigação criminal e informações, entende-se que se tratam de "duas realidades que convivem na atividade de segurança interna, que interagem na respetiva prossecução e têm um ponto privilegiado de encontro no domínio da prevenção criminal, que representa não apenas a interface entre aqueles dois momentos, mas que constitui também o ponto de referência para os limites de intervenção dos diversos operadores do sistema"[154].

Adicionalmente, compete referir a importância da produção de informações no seio da cooperação, quer no âmbito nacional, quer no âmbito internacional. Ao nível nacional, devido à necessária cooperação entre o SIS e o SIED (sobre coordenação do SGSIRP), mas também às comunicações a transmitir às entidades competentes no domínio da investigação criminal e exercício da ação penal, quando se verifiquem factos configuráveis como ilícitos criminais, salvaguardando igualmente a

[154] JÚLIO PEREIRA - *Segurança interna: o mesmo conceito novas* exigências in *Segurança e Defesa*, n.º 3 (maio-julho, 2007)

cooperação mediada ao abrigo do Sistema de Segurança Interna. Já no âmbito internacional, interessa salvaguardar os compromissos assumidos pelo Estado Português, mais exatamente no seio da cooperação com organismos congéneres estrangeiros, bem como em organizações internacionais em que constitui parte integrante como a UE, a OTAN e a ONU.

Afigura-se necessário tomar o ponto de vista da "segurança cooperativa" como vetor de atuação do SIRP, ou seja, "as ações de cooperação tendo em vista a redução da probabilidade de conflito e a promoção da paz e da estabilidade" na manutenção de interesses comuns. Na ponderação deste tipo de cooperação, "Apesar de se verificar uma variabilidade na extensão do conceito podem-se enunciar denominadores comuns tais como o controlo de armamento, não proliferação, o desarmamento e a cooperação com Estados relevantes com base num entendimento multidimensional de Segurança" (cf. SOFIA SANTOS, 2015).

O desenvolvimento legislativo conseguido pela Lei Orgânica que iremos discorrer na próxima seção, visava que os Serviços de Informações nacionais deixassem de ser os únicos Serviços de Informações que, ao nível europeu, estivessem impedidos de aceder, com a devida autorização judicial e outras garantias de proteção dos direitos fundamentais, aos dados de tráfego, de localização ou outros dados conexos inerentes às comunicações, com finalidades de prevenção da atividade terrorista. Para JÚLIO PEREIRA (2012[2], p. 6) "Num mundo aberto e global onde o próprio indivíduo (…) se configura um ator global e onde a mudança assume um ritmo progressivamente veloz, a necessidade de partilha entre serviços congéneres é um dado adquirido presente no dia-a-dia".

Segundo o Parecer elaborado pela Presidência do Conselho de Ministros, o Projeto de Lei n.º 480/XIII/2.ª (CDS-PP) edificou a "inadiável modernização administrativa" dos Serviços de Informações a atuarem através de um "estatuto funcional obsoleto, inalterado desde 1991". Pela declaração de inconstitucionalidade da norma do n.º 2 do Art. 78.º do Decreto n.º 426/XII submetida à fiscalização preventiva, subsistiu "não apenas a necessidade de dotar os serviços de informações de meios operacionais críticos, como é o acesso a "metadados", mas também de

reconhecer que estes serviços carecem de um novo regime, atualizado à luz da mais recente reforma administrativa, depois de ter ficado à margem das sucessivas reformas legislativas ocorridas nas últimas décadas". O Gabinete do Secretário-Geral, revelava que, o facto da Lei n.º 9/2007, de 19 fevereiro, não ter sido desde logo regulada, fazia com que o SIED e o SIS continuassem a ser regidos por legislação de 1991, tendo, por isso, "perdido dignidade e competitividade face às demais entidades ao serviço das missões de salvaguarda da soberania nacional". Nesta senda, o parecer emitido conclui que, hodiernamente, "a luta contra o terrorismo requer novas, mais ágeis e tempestivas formas de cooperação transfronteiriça e internacional, tal como decorre da Estratégia Antiterrorista da União Europeia e da Estratégia da União Europeia do Combate à Radicalização e ao Recrutamento para o Terrorismo, no quadro da Estratégia de Segurança Interna da União Europeia e dos acordos internacionalmente assumidos pelo Estado Português", urgindo, nesse sentido a concretização e alocação de "recursos eficientes e de meios efetivos de acesso a informação e a dados".

O Parecer elaborado pela Comissão de Fiscalização de Dados do SIRP (2017), sobre o Projeto de Lei 480/XIII/2.ª (CDS-PP), demonstra a "fundamental importância para a localização e acompanhamento das deslocações de eventuais suspeitos, por território europeu, o acesso a um determinado conjunto de dados por parte dos Serviços de Informações europeus, nos quais os Serviços de Informações portugueses se integram, designadamente dados de tráfego relativos a comunicações em que intervenham".

Cumpre acautelar, contudo, conforme consideram H. CURADO & P. VELOSO GOMES (2012), "a partilha e integração da informação e do conhecimento é essencial na interconexão entre as diferentes forças de defesa e segurança, é uma necessidade com riscos associados, quer na segurança da informação, quer na salvaguarda da privacidade e liberdade individual".

5. A Lei Orgânica n.º 4/2017, de 25 de agosto

A propósito do Parecer emitido pelo Gabinete do Secretário-Geral do SIRP sobre a Proposta de Lei n.º 79/XIII/2.ª (GOV) é referido que a "luta contra o terrorismo, bem como contra a espionagem, requer, atualmente, novas, mais ágeis e tempestivas formas de cooperação transfronteiriça e internacional, tal como decorre da Estratégia Antiterrorista da União Europeia e da Estratégia da União Europeia de Combate à Radicalização e ao Recrutamento para o Terrorismo, no quadro da Estratégia de Segurança Interna da União Europeia e dos acordos internacionalmente assumidos pelo Estado Português". O Parecer salienta ainda que o meio operacional pesquisa através do acesso a dados de comunicações e Internet consubstancia um método "compatível" com "o grau de sofisticação da ameaça", num Estado de Direito Democrático, permitindo também o alinhamento da cooperação internacional do Estado Português.

Nos termos da alínea q) do artigo 164.º da Constituição da República Portuguesa, é de competência exclusiva da Assembleia da República legislar sobre o "regime do sistema de informações da República Portuguesa e do segredo de Estado"[155].

A Constituição não trata de forma explícita sob qualquer norma a atividade dos Serviços de Informações. Desta forma, através do Art. 164.º, alínea q) aloca a competência legislativa de forma exclusiva ao Parlamento, pelo que podemos desta forma "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"[156]. Na verdade, a alteração legislativa introduzida em 1997 acarretou "uma notória diminuição dos poderes que o Governo

[155] Assim, tal como preconizam J.J. GOMES CANOTILHO & VITAL MOREIRA (2007), a competência legislativa atribuída por este preceito atribui uma reserva absoluta da Assembleia da República em matéria de organização, atribuições legais e meios de atuação dos Serviços de Informações - levando a que o sentido e alcance da reserva absoluta de lei parlamentar considere: "(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".

[156] v. a Declaração de Voto do Juiz Conselheiro José António Teles Pereira, a propósito do Ac. do TC n.º 403/2015.

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)"[157].

Com antecedentes parlamentares, o acesso a novos meios operacionais foi alvo da proposta de Lei n.º 345/XII/4.ª, apresentada na XII Legislatura, a qual visava aprovar o regime do Sistema de Informações da República Portuguesa. Esta proposta viria a dar origem ao Decreto da Assembleia da República n.º 426/XII, vetado pelo Presidente da República na decorrência do Ac. do TC n.º 403/2015, que se pronunciou, em sede de fiscalização preventiva, pela inconstitucionalidade da norma presente no n.º 2 do artigo 78.º do referido Decreto, por violação do n.º 4 do artigo 34.º da CRP[158].

A criação da Lei Orgânica n.º 4/2017, de 25 de agosto veio aprovar e regular o procedimento especial de acesso a dados de telecomunicações e Internet pelos Oficiais de informações do Serviço de Informações de Segurança (SIS) e do Serviço de Informações Estratégicas de Defesa (SIED). Esta Lei, que procedeu à segunda alteração da Lei n.º 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário) e visou, deste modo, regular o acesso a dados previamente armazenados pelos prestadores de comunicações eletrónicas.

Relativamente ao Art. 1.º, importa desde logo fazer referência ao regime de acesso. Assim, a lei visa "regular o procedimento especial" de acesso aos dados, ou seja, este acesso assume desde logo um carácter de especialidade (n.º 1).

Os dados cujo o acesso de prevê, deverão ter sido "previamente armazenados pelos prestadores de comunicações eletrónicas". Neste sentido, importa realçar que o Art. 6.º, n.º 2 proíbe a "interconexão em tempo real com as bases de dados dos operadores de telecomunicações e Internet para o acesso direto em linha aos dados

[157] Cf. JOSÉ MAGALHÃES, *Dicionário da Revisão Constitucional*, Mem Martins, 1989, p. 57 cit. In *Diário da República*, 1.ª série – N.º 182 – 17 de setembro de 2015 (p. 8268).

[158] Cumpre ainda, referir outras iniciativas da mesma legislatura, tais como o Projeto de Lei n.º 286/XII, que altera a LQSIRP em matéria de acesso a documentos; o Projeto de Lei n.º 287/XII que altera a LQSIRP, reforçando as competências da Comissão de Fiscalização de Dados do SIRP nos caos de recolha ilegítima de informação por parte dos Serviços de Informações; e o Projeto de Lei n.º 302/XII – que cria a Comissão da Assembleia da República para a Fiscalização do SIRP.

requeridos". Ou seja, em situação alguma poderá existir o acesso a dados à medida que estes se geram - esta proibição é retomada no n.º 3 do Art. 9.º ("não admitindo a aquisição de informação em larga escala, por transferência integral dos registos existentes, nem a ligação em tempo real às redes de comunicações eletrónicas").

Ainda em referência ao n.º 1 do Art. 1.º, importa destacar o *princípio de necessidade* das medidas previstas, já que o acesso a dados deve justamente acontecer quando estes se mostrem "estritamente necessários para a prossecução da atividade de produção de informações" pelo SIRP. Já o n.º 3 do Art. 2.º acresce na medida em que "A conservação e transmissão pelos prestadores de serviços de comunicações eletrónicas dos dados tipificados nos números anteriores obedecem exclusivamente às finalidades previstas no n.º 1 do artigo 1.º e nos artigos 3.º e 4.º".

A atividade de produção de informações a partir deste meio de atuação à disposição dos Serviços de Informações deve estar diretamente relacionada com a "segurança interna, a defesa, a segurança do Estado e a prevenção da espionagem e do terrorismo" sob escrutínio do Ministério Público e do controlo judicial.

Quanto às definições atendidas no Art. 2.º, constituem *Dados de telecomunicações* "os registos ou informação constantes de bancos de dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas relativos à prestação de serviços telefónicos acessíveis ao público e à rede de suporte à transferência, entre pontos terminais da rede, de comunicações vocais, serviços de mensagens e multimédia e de outras formas de comunicação" (cf. alínea a); e constituem *Dados de Internet* "os registos ou informação constantes de bancos de dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, relativos a sistemas de transmissão e a equipamentos de comutação ou encaminhamento que permitem o envio de sinais ou dados, quando não deem suporte a uma concreta comunicação" (cf. alínea b).

Saliente-se que a transmissão e conservação dos dados pelos prestadores de serviços de comunicações eletrónicas dos dados às autoridades competentes de

ambos os Serviços de Informações[159] só poderá acontecer quando *autorizada e ordenada* através de "despacho judicial fundamentado".

De acordo com o Art. 3.º, o acesso a *dados de base*[160] e *de localização de equipamento*[161] acontece quando este seja necessário à produção de informações relacionadas com a "salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada e no seu exclusivo âmbito".

Por outro lado, o acesso a *dados de tráfego*, conforme previsto no Art. 4.º, tem lugar "para efeitos de produção de informações necessárias à prevenção de atos de espionagem e do terrorismo". Obviamente, a apreciação judicial da necessidade, adequação e proporcionalidade do pedido de acesso dos Oficiais de informações do SIS e do SIED a este tipo de dados tem igualmente em consideração a circunscrição ao mesmo quadro de ameaças, nos termos no n.º 2 do Art. 10.º. Sempre que os dados obtidos indiciem a prática de crimes de espionagem e terrorismo, a lei garante a comunicação imediata dos mesmos ao Procurador-Geral da República, para a devida atuação em conformidade (Art. 13.º).

Podemos constatar que o legislador procurou diferenciar o acesso a determinado tipo de dados de telecomunicações e Internet mediante o tipo de ameaça a combater. A propósito, tal como refere JORGE BACELAR GOUVEIA (2018, p. 751), esta diferenciação da caracterização dos dados assume não só relevância no sentido da "delimitação dos procedimentos", mas também no sentido em que "é igualmente útil em vista do propósito de lhe aceder, porquanto há uma gradação a considerar". Ou seja, um acesso mais alargado aos dados de base e de localização de equipamento, quando de trate da necessidade de produzir informações no "exclusivo âmbito" da

[159] Nos termos da alínea d) do n.º 2 do Art. 2, constituem *Autoridades competentes* os dirigentes superiores e intermédios do SIS e do SIED.

[160] Para efeitos da Lei em análise, constituem "produção de informações necessárias à salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada e no seu exclusivo âmbito" (cf. alínea a), n.º 2 do Art. 2.º.

[161] Ou seja, "os registos ou informação constantes de bancos de dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas, relativos a sistemas de transmissão e a equipamentos de comutação ou encaminhamento que permitem o envio de sinais ou dados, quando não deem suporte a uma concreta comunicação" (cf. alínea b) do n.º 2 do Art. 2.º).

salvaguarda da defesa nacional, da segurança interna e da prevenção de atos de sabotagem, espionagem, terrorismo, proliferação de armas de destruição maciça e criminalidade altamente organizada. Por outro lado, prevê-se um acesso mais limitado aos dados de tráfego, uma vez que esta possibilidade apenas existe quando visem a produção de informações com vista à prevenção de atos de espionagem e do terrorismo.

O acesso dos oficias de informações do SIS e do SIED aos dados que acabamos de discorrer depende de autorização judicial com carácter prévio e obrigatório (Art. 5.º). Esta autorização é concedida por uma formação das secções criminais do Supremo Tribunal de Justiça - constituída pelos presidentes das secções do Supremo Tribunal de Justiça e por um juiz indicado pelo Conselho Superior da Magistratura, de entre os mais antigos destas secções - conforme previsto nos Art.ºs 8.º e 17.º.

De acordo com o Art. 6.º, o pedido é sujeito a um juízo de admissibilidade, pelo o acesso aos dados só poderá ser autorizado quando a referida formação considerar que se trata de uma diligência "necessária, adequada e proporcional". A informação que se pretende obter deverá estar relacionada com "um alvo ou um intermediário determinado" (cf. alínea a) do n.º 1) ou por se entender que existem razões para crer que a informação que se pretende obter "seria muito difícil ou impossível de obter de outra forma ou em tempo útil para responder a situação de urgência"– considerando, por isso, uma medida de *ultima ratio*.

O acesso a dados de telecomunicações e Internet deverá ter na sua génese um requerimento escrito, devidamente fundamentado, detalhado e circunstanciado, elaborado pelos diretores do SIS ou do SIED[162] acerca das "medidas pontuais de acesso"[163] em consideração. Este pedido é posteriormente enviado pelo Secretário-Geral do Sistema de Informações da República Portuguesa ao Presidente do Supremo Tribunal de Justiça, dando conhecimento ao Ministério Público, na pessoa do Procurador-Geral da República.

[162] Em alternativa, quem os substitua em caso de ausência ou impedimento, nos temos do n.º 1 do Art. 9.º.
[163] De acordo com o n.º 3 do Art. 9.º ".

O n.º 2 do Art. 9.º estabelece conjuntamente os elementos que devem constar no pedido, nomeadamente: a "Indicação da ação operacional concreta a realizar e das medidas pontuais de acesso requeridas"; os "Factos que suportam o pedido, finalidades que o fundamentam e razões que aconselham a adoção das medidas pontuais de acesso"; e a "Identificação da pessoa ou pessoas, caso sejam conhecidas, envolvidas dos factos (…) e afetadas pelas medidas pontuais de acesso requeridas".

Destaca-se o estabelecimento de um limite temporal do acesso, já que deve existir no pedido a indicação da duração das medidas pontuais de acesso, "que não pode exceder o prazo máximo de três meses". Este prazo é eventualmente prorrogável por "um único período sujeito ao mesmo limite, mediante autorização expressa, desde que se verifiquem os respetivos requisitos de admissibilidade", nos termos da alínea d) do n.º 2 do Art. 9.º.

Interessa elencar as considerações que são tomadas sobre as "medidas pontuais de acesso" (cf. n.º 3 do Art. 9.º). Neste sentido, tratam-se de "providências de recolha de dados", na medida em que:

a) São sujeitas a uma transferência previamente autorizada;

b) Existe um controlo casuístico;

c) Encontram-se relacionadas com uma "suspeita concreta e individualizada";

d) Existe circunscrição da sua duração ("que não se prolongam no tempo");

e) Há uma limitação da quantidade de dados a recolher, já que "não se estendem à totalidade dos dados (…), não admitindo a aquisição de informação em larga escala, por transferência integral dos registos existentes".

A apreciação judicial da necessidade, adequação e proporcionalidade do pedido é acautelada nos termos do Art. 10.º, que comporta, designadamente a "justa medida" não só da espécie e da escala da informação obtida, como a "definição das categorias de dados de telecomunicações e Internet a fornecer pelos operadores". Assim, verifica-se necessário "um juízo restritivo de proibição do excesso" mediante a interdição do acesso indiscriminado a todos os dados de determinado cidadão. A

decisão de concessão ou denegação da autorização deve ser informada sob a forma de despacho, no prazo máximo de 48 horas[164] – devidamente "fundamentado com base em informações claras e completas", com ênfase nos objetivos de processamento (n.º 3).

Atente-se igualmente o "princípio da necessidade de conhecer" disposto no n.º 2 do Art. 11.º, na medida em que apenas é concedido acesso do pessoal do SIRP a dados e informações conservados em arquivo nos centros de dados do SIS e do SIED através de autorização superior – considerando "o bom exercício das funções" incumbidas aos serviços que representam.

Da apreciação judicial parte-se para o processamento do "Acesso aos dados autorizados" (Art. 11.º). Neste caso, quando o pedido de acesso a dados de telecomunicações e Internet é deferido, a transmissão dos mesmos é feita com o conhecimento da formação das secções criminais do STJ e do PGR, mediante comunicação eletrónica[165]. A transmissão deve compreender as "condições técnicas e de segurança fixadas em portaria do Primeiro-Ministro e dos membros responsáveis pelas áreas das comunicações da cibersegurança", pela observação de "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, sem prejuízo da observação dos princípios e do cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados" (n.º 1), verificando-se nesta fase a fiscalização e controlo da Comissão de Fiscalização de Dados do SIRP.

[164] Em determinadas situações de urgência devidamente fundamentadas no pedido, a decisão judicial é dada a conhecer no prazo mais breve possível (cf. n.º 4 do Art. 10.º).

[165] De acordo com a Portaria 237-A/2018, após receberem o formulário autorizado, os operadores de telecomunicações têm 36 horas para dar uma resposta aos pedidos dos Serviços de Informações (através da aplicação informática SAPDOC), ainda que, "em situações de urgência devidamente fundamentadas" e "validadas no despacho de autorização judicial prévia, o envio do ficheiro de resposta com os dados recolhidos é efetuado no mais breve prazo possível" (cf. Art. 4.º). Importa relembrar que de acordo com a Lei Orgânica n.º 4/2017, "a decisão judicial de concessão ou de denegação da autorização consta de despacho proferido no prazo máximo de 48 horas", ou seja, o acesso pelos Oficiais de informações pode estar pendente de um período de 84 horas.

Recentemente, ao abrigo da Portaria n.º 237-A/2018, de 28 de agosto[166], é dado seguimento à definição das condições técnicas e de segurança da comunicação eletrónica para efeito de transmissão entretanto diferida dos dados de telecomunicações e Internet. Assim, prevê-se que os tramites processuais relacionados com a comunicação eletrónica dos referidos dados pelos prestadores de serviços de comunicação eletrónicas sejam "praticados por via de um serviço informático, baseado na Internet, especificamente disponibilizado para o efeito no denominado «Sistema de Acesso ou Pedido de Dados aos Prestadores de Serviços de Comunicações Eletrónicas», abreviadamente designado por SAPDOC[167]" (cf. Art.º 2.º da Portaria).

Após este processamento, é colocada em evidência a importância do respeito pelos direitos, liberdades e garantias e do princípio da legalidade da recolha pela vigência do Art. 12.º, n.º 1 da Lei Orgânica em análise. Assim, o controlo judicial pelas secções criminais do STJ deve garantir que os dados são, em primeiro lugar, "Recolhidos para finalidades determinadas, explícitas e legítimas" (alínea a), e que são "Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos" (alínea b).

A manutenção deste controlo judicial durante o acesso aos dados de telecomunicações e Internet visa garantir que a formação das secções criminais do STJ pode, "a todo o momento", cancelar os procedimentos que estejam em curso, bem como "ordenar a destruição imediata de todos os dados obtidos de forma ilegal ou abusiva, ou que violem o âmbito da autorização judicial prévia", assim como os que se estimem "manifestamente estranhos ao processo, nomeadamente quando não tenham relação com o objeto ou finalidades do pedido ou cujo tratamento possa afetar gravemente direitos, liberdades e garantias" (cf. n.º 3 do Art. 12.º)[168]. Se

[166] De acordo com o Art. 1.º da Portaria, são estabelecidos "os termos das condições técnicas e de segurança em que, mediante procedimento obrigatório e vinculado de autorização judicial prévia, se processa a comunicação eletrónica para efeitos da transmissão diferida de dados de telecomunicações e Internet…".

[167] O SAPDOC é desenvolvido e gerido pelo Instituto de Gestão Financeira e Equipamentos da Justiça, I. P. (cf. n.º 2 do Art. 2.º da Portaria). Pela salvaguarda do Art.º 6.º da Portaria n.º 237-A/2018, a aplicação informática "é rastreável e auditável de acordo com o estado da técnica ao momento da transmissão, conferindo as máximas garantias de segurança neste domínio" (n.º 1 do Art. 2.º).

[168] De acordo com o Art. 5.º da Portaria 237-A/2018, "1 – O despacho de cancelamento em curso de acesso a dados de comunicações e Internet e de destruição de dados (…) é comunicado, de imediato, pela formação das

eventualmente esta formação verificar alguma destas situações, deve notificar o Procurador-Geral da República acerca das decisões de cancelamento de acesso e destruição dos dados, de forma a serem instituídos os devidos procedimentos legais no exercício das suas competências (n.º 4 do mesmo artigo). Perante a mesma situação, a Comissão de Fiscalização de Dados do SIRP é alertada para o exercício das suas competências legais em matéria de proteção dos dados pessoais (n.º 5).

No que respeita ao tratamento dos dados obtidos importa considerar o Art. 14.º. Após a recolha dos dados de telecomunicações e Internet, a Lei prevê o seu devido processamento e conservação através dos centros de dados do SIS e do SIED[169] (n.º 1). O responsável pelo tratamento dos dados recolhidos deve assegurar a sua inserção no centro de dados do Serviço de Informações respetivo, garantido que os mesmos são tratados: "a) De forma lícita e com respeito pelo princípio da boa -fé; b) De forma compatível com as finalidades que determinaram a sua recolha; c) De modo a assegurar que sejam apagados ou retificados os dados inexatos ou incompletos, tendo em conta as finalidades da recolha e tratamento; d) De modo a que a conservação seja sempre fundamentada e restrita ao período necessário para a prossecução das finalidades da recolha ou do tratamento posterior" (n.º 2)[170].

Cabe referir que o procedimento que discorremos é coberto pelo regime do segredo de Estado aplicável ao SIRP, nos termos do n.º 5 do Art. 14.º da Lei.

A atuação da Comissão de Fiscalização de Dados do SIRP no âmbito da Lei Orgânica em análise é prevista no Art. 15.º. De acordo com o procedimento obrigatório previsto, esta Comissão constitui a autoridade pública incumbida da fiscalização do respeito pelos princípios e cumprimento das regras atinentes à qualidade e salvaguarda da confidencialidade, bem como da segurança dos dados obtidos (n.º 1). Também os centros de dados do SIS e do SIED estão sujeitos aos

secções criminais do Supremo Tribunal de Justiça aos prestadores de serviços de comunicações eletrónicas, às autoridades competentes do SIS e do SIED, ao/à Procurador/a-Geral da República e à Comissão de Fiscalização de Dados do SIRP, através da aplicação informática SAPDOC".

[169] O diretor de cada centro de dados é responsável pelo seu tratamento nos termos do regime de proteção de dados pessoais (n. º1).

[170] O n.º 3 do mesmo artigo vem ressalvar a implicação do regime especial de proteção de dados pessoais do SIRP aplicável aos centros de dados do SIS e do SIED, nomeadamente ao nível dos prazos de conservação, eliminação e destruição definidos em regulamento.

poderes de fiscalização oficiosa da Comissão de Fiscalização de Dados do SIRP, sendo que os dados de telecomunicações e Internet são verificados através de referência nominativa (n.º 2). Nos termos do n.º 3, cabe à formação das secções criminais do STJ comunicar à Comissão as autorizações concedidas com referência nominativa, que é apoiada pelos diretores dos centros de dados do SIS e do SIED (n.º 4).

A Comissão de Fiscalização de Dados do SIRP deve elaborar um relatório ao Conselho de Fiscalização do SIRP sempre que verifique irregularidades ou violações dos dados obtidos de acordo com o procedimento da Lei Orgânica em análise (n.º 5). Importa referir que a Comissão de Fiscalização de Dados do SIRP é igualmente responsável por garantir o direito de acesso dos cidadãos aos dados processados ou conservados nos centros de dados do SIS e do SIED, mediante a apresentação de participação (n.º 6). Importa destacar a salvaguarda que é feita no n.º 7, quando ocorra a violação dos direitos, liberdades e garantias previstos da Constituição e na Lei, a Comissão de Fiscalização que analisamos é responsável por ordenar o cancelamento ou a retificação dos dados, devendo exercer a respetiva ação penal.

O Conselho de Fiscalização do SIRP é igualmente responsável por exercer os seus poderes de fiscalização sobre o procedimento de acesso, bem como sobre os dados de telecomunicações e Internet propriamente ditos (n.º 1 do Art. 16.º). Neste sentido, o Secretário-Geral é responsável por entregar ao Conselho de Fiscalização do SIRP, uma listagem dos pedidos de autorização, com regularidade mínima bimensal, onde constem os pedidos de autorização de acesso a dados de telecomunicações e Internet submetidos à análise da formação do STJ. É permitido ao Conselho de Fiscalização do SIRP solicitar e obter os esclarecimentos que considere necessários e adequados ao exercício das suas funções de fiscalização (n.º 2).

Devemos observar que foi feito um esforço na minimização das preocupações de constitucionalidade que ressaltaram do Ac. do TC n.º 403/2015 - reforçando um conjunto de garantias procedimentais: desde logo, verificou-se a necessidade da existência de uma autorização prévia do acesso, através da formação das secções

criminais do STJ, bem como o controlo judicial dos acessos; as medidas pontuais de acesso apenas ocorrem quando exitir concreta necessidade, adequação e proporcionalidade da sua utilização; importa considerar igualmente que o pedido de acesso deve ser devidamente fundamentado, desde logo elencando as circunstâncias que motivam determinado acesso e com que finalidade; existe ainda um prazo fixado na lei sobre a duração das medidas pontuais de acesso ("que não pode exceder o prazo máximo de três meses); é prevista a proibição da interconexão com as bases de dados dos prestadores de serviços de telecomunicações, evitando-se a aquisição de informação em larga escala e a transferência integral dos registos existentes, nos termos do n.º 2 do Art. 6 e n.º 3 do Art. 9.º; a crucial graduação do acesso a dados de tráfego, exclusivamente para finalidades de "produção de informações necessários à prevenção de atos de espionagem e do terrorismo"; A previsão de sanções para funcionários do SIRP que cometam ilegalidades e abusos (Art. 7.º e Art. 11, n.º 3); a clarificação de um regime de cumprimento das regras relativas ao tratamento dos dados acedidos; promoção da fiscalização da atividade por meio dos Diretores do Centros de Dados do SIS e do SIED, bem como pela fiscalização exclusiva por entidades independentes como a Comissão de Fiscalização de Dados do SIRP, da Procuradoria-Geral da República e o Conselho de Fiscalização do SIRP; as garantias promovidas no âmbito do Art. 12.º, mormente a determinação do "cancelamento de procedimentos em curso de acesso a dados de telecomunicações e Internet*"* ou "a destruição imediata de todos os dados obtidos de forma ilegal ou abusiva, ou que violem o âmbito da autorização judicial prévia, bem como os dados que sejam manifestamente estranhos ao processo".

Lembremo-nos que o Ac. do TC n.º 403/2015 havia concluído que não poderia uma lei ordinária reconhecer ao SIRP legitimidade suficiente para aceder a dados que a CRP exigiu uma condição necessária que não inclui perentoriamente o campo de atuação do SIRP dessa possibilidade. Pela Lei Orgânica aprovada, esta inibição é ultrapassada, tendo em consideração os esforços dos mecanismos de controlo instituídos. Consideramos igualmente que o SIS e o SIED dispõem agora de capacidade de acompanhar as metodologias de produção de informações de outros países europeus - conforme discorremos no Capítulo II.

Assim, ultrapassamos uma garantia desmesurada de separação entre a produção de informações e investigação criminal, no nosso entendimento, maioritariamente suportada por um antepassado histórico ditatorial[171]. Se por um lado é necessário distinguir e dissociar ambas as atividades, também é necessário clarificar os instrumentos utilizados no desempenho do papel de cada uma das figuras competentes, bem como explicitar transparentemente a necessidade de adotar instrumentos adequados à prossecução das finalidades adstritas a diferentes organismos. Este meio de atuação previsto à disposição dos Serviços de Informações irá aumentar a capacidade de resposta do Estado a determinadas ameaças que esteja sujeito, através de uma atuação a montante do processo penal.

Considerando o panorama proporcionado pela Lei Orgânica n.º 4/2017, de 25 de agosto, entendemos que tem em consideração a recente jurisprudência do Tribunal de Justiça da União Europeia, na medida do Acórdão *Digital Rights Ireland*, de 8 de abril de 2014, bem como do Acórdão *Tele 2,* de 21 de dezembro de 2016, no reforço da sujeição a limites claros sob condições previamente estipuladas e objetivas da ingerência nas comunicações eletrónicas.

Mais recentemente, nos termos do disposto da alínea a), do n.º 1 e da alínea f) do Art. 281.º da CRP e nos Art.os 51.º e 62.º, n.º 3 da Lei n.º 28/82, de 15 de novembro, um número superior a um décimo dos deputados da Assembleia da República requereram ao Tribunal Constitucional a declaração de inconstitucionalidade com força obrigatória geral de normas constantes da Lei Orgânica 4/2017, de 25 de agosto. Por via da fiscalização abstrata sucessiva da constitucionalidade, "A questão relevante a apreciar é a de saber quais os tipos de dados que se encontram sob a proteção estabelecida no n.º 4 do artigo 34.º da Constituição…", importando aferir

[171] Acompanhando o entendimento demonstrado por JORGE SILVA CARVALHO (2007) na medida em que "Países que no século XX, período da autonomização e definição do conceito de serviços de informações, na sua acepção moderna, foram protagonistas principais de conflitos e guerras ou que se viram, ao longo desse período, sujeitos a alterações violentas da ordem constitucional ou interna, guerras civis, ou a violência terrorista, enquadram a actividade de informações de uma forma mais natural e convicta da sua necessidade. Por outro lado, países que tiveram em períodos da sua história regimes repressivos, que tradicionalmente recorrem a "polícias políticas", ou países que se mantiveram afastados de conflitos, internos e internacionais, mantendo uma situação de continuada tranquilidade, terão, certamente, perspectivas muito diferentes sobre a necessidade ou mesmo a bondade da actividade de informações". Desta forma, "os serviços de informações são o produto de uma cultura e de uma história".

"se o acesso a dados de tráfego previsto nos artigos 3.º e 4,º da LO [Lei Orgânica 4/2017] por parte de oficiais de informações se conforma com a exceção constante da segunda parte do n.º 4 do artigo 34.º da CRP que permite o acesso a dados dessa natureza nos casos previstos na lei em matéria de processo criminal" (ponto n.º 15). O pedido de fiscalização faz referência a uma série de jurisprudência do Tribunal Constitucional (Acórdãos n.os 241/02, 195/85, 407/97, 486/2009 e 699/2013), admitindo que " O TC considera, pois, que, fora do processo penal, vigora uma proibição absoluta de ingerência das autoridades públicas nos meios de comunicação, incluindo em matéria de dados de tráfego" (pontos n.º 19 e n.º 20). De acordo com o pedido formulado, interessa saber se o acesso de oficiais de informações a dados de tráfego, incluindo os dados de localização, se pode considerar como uma atividade "em matéria de processo criminal". O pedido de fiscalização admite que apesar dos desenvolvimentos que foram produzidos na Lei Orgânica agora em análise, nomeadamente ao nível do controlo judicial e a autorização prévia do acesso, bem como a superior "intensidade do controlo", "não afastam as decisivas razões que levaram à declaração da inconstitucionalidade do Decreto n.º 426/XII" (ponto n.º 34). No entendimento dos requerentes, apesar das secções criminais do Supremo Tribunal de Justiça serem inequivocamente um órgão de natureza jurisdicional, "não é menos certo que as funções que a LO lhes atribui – em tudo estranhas às funções que até agora este Tribunal foi chamado legalmente a desempenhar – não constituem matéria de processo criminal"[172] (ponto n.º 35).

6. Da Fiscalização e do Controlo da atividade de produção de informações

A par da preocupação da adoção de ferramentas que permitam a eficácia e eficiência da atuação do SIRP, devemos encarar a necessidade da existência de

[172] Segundo o pedido de fiscalização o que está em causa "não é tanto a natureza administrativa ou judicial da entidade de controlo (embora tal natureza não seja irrelevante) mas a questão de saber se o controlo judicial efetuado se insere, ou não, no âmbito do processo penal" (ponto n.º 37).

estruturas direcionadas à fiscalização das suas atividades, garantido a legalidade da sua atuação dos respetivos Serviços de Informações[173].

Tal como refere JÚLIO PEREIRA (2012[2], p. 1) "Pelas missões que competem aos Serviços não podemos também deixar de fazer alusão à sua dimensão ética de serviço público, que remete para imperativos muito exigentes no que diz respeito aos Direitos, Liberdades e Garantias dos Cidadãos e para a necessidade de encontrar mecanismos eficazes e adequados que assegurem a transparência[174], a responsabilização e a sua fiscalização, sem prejuízo da necessidade de manter elevados níveis de sigilo nas suas atividades".

A propósito do exercício da atividade prosseguida pela administração pública da segurança dever ser aliado a um quadro de ética e responsabilidade dos seus órgãos e agentes, ALICE FEITEIRA (2015, p. 17) adverte que "os mecanismos de interacção entre administradores e administrados pressupõem também a efectivação dos deveres de transparência, de actuação conforme ao direito e de boa gestão dos meios disponíveis, – humanos, materiais e jurídicos – de acordo com um modelo de *accountability*, destinado à promoção do bem comum e do interesse público. O modelo de *accountability* compreende o estabelecimento de modos de controlo e fiscalização dos poderes públicos, preferencialmente de dimensão alternativa – judiciais, parlamentares, administrativos e particulares –, o reforço do modelo democrático do exercício da administração, o aprofundamento do controlo político e o apuramento dos níveis de responsabilidade decorrentes da acção pública".

Importa acompanhar o ensinamento de D. VITKAUSKAS (1999, p. 28) sobre a adequação e proporcionalidade dos meios ao dispor Serviços de Informações, já que:

[173] "…não fazendo cair sobre esta melindrosa atividade administrativa do Estado qualquer sombra ou obscuridade antidemocrática", atuando os organismos de fiscalização como "o contrapeso da autorização democrática para a intensificação das respetivas estruturas", conforme ensina JORGE BACELAR GOUVEIA - *Os Serviços de Informações…,* p. 76.

[174] Assim, nas palavras do Ex-Secretário-Geral do SIRP "… tem de vir a público o que pode vir a público e mantido reservado o que se refere às atividades operacionais, sem confundir nunca estes dois níveis". Tornando-se o desafio fundamental "definir claramente os limites entre ambos", já que "precisamos de saber o que precisamos de partilhar" (p. 8).

> "*The potential for invasions by a security intelligence service into privacy, misuse of data and other types of problems will increase as telecommunications and computer technologies become more sophisticated. Therefore, a clear statutory basis and a tight executive or judicial control is necessary to prevent an abuse of individual's rights. In addition, methods of security investigation must be proportionate to the threat involved; a security intelligence service must focus its attention only on those individuals or groups who really pose a threat*".

É certo que a maioria do trabalho dos Serviços de Informações deva realizar-se em segredo, uma vez que a revelação de fontes, metodologias de atuação e recursos poderia comprometer a eficácia dos mesmos. Neste sentido, de alguma forma a sua atuação não poderá ser tão transparente como outras entidades do governo. Assim, no seguimento da argumentação de M.ª VILLALOBOS (2008, p. 4), sobre o contraste necessário adverte: "*pero que no pueda utilizarse esta transparencia no significa que estén fuera de los sistemas de control democráticos"*.

Cabe referir a importância da Lei n.º 15/96, de 30 de abril, tratando-se da segunda alteração à LQSIRP na qual se fortaleceram as competências atribuídas ao Conselho de Fiscalização dos Serviços de Informações, regulando também o procedimento de nomeação dos Diretores dos Serviços de Informações. Através da LQSIRP, o Conselho de Fiscalização passou a poder efetuar visitas de inspeção direta aos Serviços e obter dos mesmos os elementos que necessite para a prossecução das suas funções.

Assim, JORGE BACELAR GOUVEIA (2013), entende que a fiscalização da atividade do SIRP está, "numa perspetiva específica", atribuída a dois órgãos, são eles o Conselho de Fiscalização do Sistema de Informações da República Portuguesa (CFSIRP) e à Comissão de Fiscalização de Dados do Sistema de Informações da República Portuguesa (CFDSIRP). A fiscalização externa do SIRP está distribuída pela fiscalização político-parlamentar[175] e por uma fiscalização jurisdicionalizada,

[175] Conferida pelo Art. 36.º, n.º 1 da LQSIRP. Levada a cabo pelo CFSIRP, "Não integrando propriamente o SIRP, este órgão exerce as suas competências sobre a totalidade do sistema português de informações, não havendo espaços imunes à respetiva intervenção fiscalizadora, o que quer dizer que o SGSIRP, e o seu

apoiada pelo Ministério Público, nos termos do n.º 2 do Art. 26.º da LQSIRP. Soma-se igualmente uma fiscalização mais intrínseca, "através do autocontrolo a que a atividade de informações se submete dentro da organização do SIRP, com as suas estruturas superior de direção e de disciplina", junta ao controlo exercido pelo Governo e Primeiro-Ministro ("fiscalização interna"); e, também, por uma "fiscalização externa geral", pela Assembleia da República e do Governo (política), e pelos tribunais (judicial), quando exista a violação de direitos.

Como afere o Relatório da Comissão de Veneza (2015, p. 35),

> "*Signals intelligence has a very large potential for infringing privacy and certain other human rights. Understanding strategic surveillance merely through the lens of the right to privacy may not completely capture its potential harm. Unlike the situation for rendition, where the harm is clear, immediate and individualised, the damage insufficiently regulated and controlled signals intelligence can do to society is more diffuse and long term. (…). Agreement on minimum international standards on privacy protection thus appears to be necessary. (…) Only strong independent control and oversight mechanisms can assuage public concern that signals intelligence is not being abused*".

Assim, ALICE FEITEIRA (2015, p.33) informa que a estrutura normativa no sector da administração pública da segurança, em particular, no quadro dos Serviços de Informações "possibilita a conformação dos conteúdos vinculativos de forma directa e *in casu* por órgãos hetero-vinculados, mas suscita interrogações relativas à dimensão da tutela das garantias dos particulares. No entanto, o reconhecimento de direitos de defesa dos cidadãos só são eficazes se estiverem consagrados mecanismos que permitam que estes se possam dirigir a uma entidade competente para iniciar, prosseguir e concluir o procedimento de defesa dos seus direitos fundamentais".

Gabinete, bem como o SIED e o SIS se lhe submetem sob o ponto de vista da atividade de fiscalização que empreendem", assim, a "profundidade da efetivação da fiscalização político-parlamentar é ainda evidente pelo facto de o CFSIRP poder atuar mesmo através de uma atividade de inspeção nas próprias instalações dos serviços informações, que lhe devem facultar o acesso livre, sempre que o requeira, jamais se limitando a cuidados meramente administrativos ou burocráticos" (p. 84).

6.1. Do Conselho de Fiscalização do SIRP

O Conselho de Fiscalização do Sistema de Informações da República Portuguesa (CFSIRP) consta do Capítulo II da LQSIRP, adstrito à Fiscalização. Segundo SÓNIA REIS & BOTELHO DA SILVA (2007, p. 11) a LQSIRP cuida especialmente do estabelecimento de limites à atividade dos Serviços de Informações, daí não ser de estranhar que preveja um órgão "específico e exclusivamente vocacionado para a fiscalização da atividade". Para esse efeito, o CFSIRP, nos termos do Art. 9.º, n.º 1, acompanha e fiscaliza a atividade do Secretário-Geral e dos Serviços de Informações, zelando pelo cumprimento da Constituição e da lei, particularmente do regime de direitos, liberdades e garantias fundamentais dos cidadãos. Acrescem ainda nos termos do Art. 34.º, n.º 2 da Lei Orgânica n.º 4/2004, de 6 de novembro, os poderes de acompanhamento e de fiscalização sobre as atividades de produção de informações das Forças Armadas, da competência da CISMIL.

O Conselho de Fiscalização é composto por três cidadãos de reconhecida idoneidade e no pleno gozo dos seus direitos civis e políticos, eleitos pela Assembleia da República (Art. 8.º da LQSIRP). De forma a exercer as suas funções em plena imparcialidade e discrição, resulta claro que se trata de um órgão exterior à organização hierárquica de comando dos Serviços de Informações. As competências específicas do CFSIRP estão previstas no Art. 9.º, n.º 2.º da LQSIRP, competindo-lhe nomeadamente efetuar visitas inspetivas, com ou sem aviso prévio, com vista à recolha de elementos sobre o modo de funcionamento e a atividade do Secretário-Geral e dos Serviços de Informações (alínea d); solicitar os elementos dos centros de dados que entenda necessários à persecução das suas competências, ou, relativamente ao conhecimento de eventuais irregularidades ou violação da lei (alínea e); verificar a efetivação e adequação de mecanismos de controlo instituídos internamente relacionados com o pessoal, com vista a identificar situações de incompatibilidade, inadequação de perfil ou conflito de interesses que possam por em causa o funcionamento regular dos Serviços (alínea h); emitir pareceres com regularidade mínima semestral sobre o funcionamento do SIRP e apresentá-los à Assembleia da República (alínea j).

Realçamos ainda a competência geral de assegurar o acompanhamento e conhecimento das modalidades admitidas de permuta de informações entre Serviços, bem como os tipos de relacionamento dos Serviços com outras entidades, em especial de polícia, incumbidos de garantir a legalidade e sujeitos ao dever de cooperação, conforme consta do n.º 3 do Art. 9.º da LQSIRP.

De uma forma geral, a atividade do CFSIRP desenvolve-se "através de reuniões com os responsáveis institucionais e visitas de trabalho às instalações para contacto e verificação das tarefas desenvolvidas pelas estruturas integradas no Sistema de Informações da República Portuguesa e ainda através da análise de documentação que lhe é facultada diretamente, ou por solicitação própria junto das entidades competentes". O CFSIRP deverá procurar um acompanhamento permanente das atividades dos Serviços "que por decurso das suas competências diretas, quer na busca de esclarecimento de questões de dimensão pública que possam afetar o funcionamento do sistema de informações ou que derivam de matéria que exigem atenção mais particular" – tal como transmitido no Parecer do 1.º semestre de 2017 do CFSIRP.

Reveja-se o facto do CFSIRP, no seu Parecer relativo ao 1.º Semestre de 2017, ter registado a relevância da atuação do SIS no âmbito do gabinete do Coordenador de Segurança (resultante do Art. 21.º da Lei n.º 53/2008), verificando-se um "papel central e produtivo", a partir do qual a cooperação entre Serviços de Informações e serviços de segurança promoveu esforços no âmbito da segurança interna, "com participação do SIS em grupos de trabalho para tratamento de temáticas especificas neste domínio".

Como informa JORGE BACELAR GOUVEIA (2013, p.79) "As finalidades da atuação do CFSIRP são de natureza geral, tanto de uma perspetiva de eficiência organizativa como sobretudo de respeito pela juridicidade, sendo esta peculiarmente sinalizada pela alusão que se faz ao cumprimento dos direitos fundamentais dos cidadãos". Ressalva-se assim que o "alcance da atividade fiscalizadora do CFSIRP não se resume finalmente a ser meramente informativo, dado que na presença de situações de violação dos direitos fundamentais ou em face de anomalias de

funcionamento dos serviços tem a *possibilidade de fazer acionar os mecanismos próprios de aplicação de sanções* – pedindo inquéritos e sindicâncias – ou *propor medidas legislativas apropriadas* – dando sugestões aos órgãos legislativos competentes" (p.85).

Relembremos que o procedimento de acesso e os dados de telecomunicações e Internet obtidos dos termos da Lei Orgânica 4/2015, de 25 de agosto, estão sujeitos aos poderes de fiscalização do CFSIRP (cf. n.º 1 do Art. 16.º), competindo igualmente ao CFSIRP receber (com regularidade mínima bimensal) do SGSIRP, uma listagem dos pedidos de autorização de acesso aos dados de telecomunicações e Internet submetidos à formação das secções criminais – estando possibilitado de solicitar os demais esclarecimentos e informações complementares que entenda necessários e adequados ao exercício das suas funções de fiscalização (n.º 2 do Art. 16.º).

6.2. Da Comissão de Fiscalização de Dados do SIRP

A Comissão de Fiscalização de Dados do Sistema de Informações da República Portuguesa (CFDSIRP) trata-se de outro organismo de fiscalização específico do SIRP, contudo, comparativamente ao CFSIRP, estão incumbidos de menos competências[176].

É certo que a atividade de produção de informações acarreta uma intensa recolha e processamento e armazenamento de dados. Assim, o n.º 1 do artigo 23.º da LQSIRP prevê que os Serviços de Informações possam dispor de Centros de Dados compatíveis com a natureza do serviço prestado, competindo-lhes, nomeadamente, o processamento e conservação em arquivo magnético os dados e informações recolhidos na prossecução da sua atividade, daqui decorre a intervenção da CFDSIRP.

A Lei n.º 67/98, de 26 de outubro, ao estabelecer o regime de proteção de dados pessoais, prevê no seu n.º 7 do Art. 4.º que a "Lei aplica-se ao tratamento de dados pessoais que tenha por objeto a segurança pública, a defesa nacional e a Segurança

[176] Cf. JORGE BACELAR GOUVEIA – *Direito da Segurança*, 2018, p. 770.

do Estado, sem prejuízo do disposto em normas especiais constantes de instrumentos de direito internacional a que Portugal se vincule e da legislação específica atinente ao respetivos setores". Neste sentido, verifica-se que o regime de fiscalização de dados que decorre da LQSIRP e da LOSIRP derroga a Lei de Proteção de Dados Pessoais e as competências da Comissão Nacional de Proteção de Dados (CNPD) de fiscalizarem as bases de dados dos Serviços de Informações.

Assim, nos termos do n.º 1 do Art. 26.º da LQSIRP decorre que a "atividade dos centros de dados é exclusivamente fiscalizada pela Comissão de Fiscalização de Dados". A Comissão com sede da Procuradoria-Geral da República e constituída por três magistrados do Ministério Público (fiscalização jurisdicionalizada), exerce a sua função através de verificações periódicas dos programas, dados e informações por amostragem, fornecidos sem referência nominativa (n.º 4), sendo certo que no caso de a Comissão atuar perante uma denúncia ou suspeita fundamentada poderá aceder a dados e informações com referência nominativa (n.º 5). De acordo com o n.º 6 do mesmo artigo, a Comissão de Fiscalização de Dados "deve ordenar o cancelamento ou retificação de dados recolhidos que envolvam violação dos direitos, liberdades e garantias consignados na Constituição e na lei e, se for caso disso, exercer a correspondente ação penal"[177].

No que concerne à vigência da Lei Orgânica 4/2017, de 25 agosto é preponderante o papel da CFDSIRP, a quem compreende, nomeadamente:

a) Ser notificada das decisões de cancelamento de acesso e de destruição dos dados, para efeitos do exercício das suas competências legais em matéria de proteção dos dados pessoais (cf. n.º 5 do Art. 12.º);
b) Aprovar o regulamento inerente à aplicação de prazos de conservação, eliminação e destruição dos dados de telecomunicações e Internet constantes dos centros de dados do SIS e do SIED (cf. n.º 4 do Art. 14.º);
c) Fiscalizar o respeito pelos princípios e cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados

[177] O cancelamento e retificação de dados está previsto no Art. 27.º da Lei-Quadro do SIRP.

obtidos de acordo com o procedimento obrigatório e vinculativo da Lei Orgânica 4/2017, de 25 de agosto (nos termos do n.º 1 do Art. 15.º);

d) Fiscalizar oficiosamente, por referência nominativa, os dados de telecomunicações e Internet obtidos (cf. n.º 2 do Art. 15.º);
e) Ser notificada das autorizações concedidas pela formação das secções criminais do STJ (n.º 3 do Art. 15.º);
f) Receber especial apoio dos diretores dos centros de dados do SIS e do SIED (n.º 4 do Art. 15.º);
g) Dar conhecimento ao CFSIRP das irregularidades ou violações detetadas no exercício das suas funções (cf. n.º 5 do Art 15.º);
h) Exercer o direito de acesso dos cidadãos aos dados processados ou conservados nos centros de dados do SIS e do SIED (n.º 6 do Art. 15.º);
i) Ordenar o cancelamento ou retificação dos dados de telecomunicações e Internet recolhidos que envolvam a violação dos direitos, liberdades e garantias consignados na CRP e na lei, exercendo a correspondente ação penal, quando aplicável (n.º 7 do Art. 15.º).

6.3. Da Comissão de Controlo Prévio à Autorização e Controlo Judicial previsto Lei Orgânica n.º 4/2017, de 25 de agosto

O Ac. do TC n.º 403/2015 concluiu que a proposta da criação de uma Comissão de Controlo Prévio, tal como prevista pelo Decreto 426/XII, não iria substituir a intervenção de uma autoridade judiciária exigida nos termos constitucionais (cf. n.º 20 do aresto):

> "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 [(cfr. 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".

Continua o Acórdão referindo que "… 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 já 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 o acesso e manutenção dos dados de tráfego se poderia equiparar ao controlo existente num processo penal".

Diferencia-se no arresto ainda a atuação da entidade de controlo num processo penal – que assegura as garantias de acesso aos dados, bem como o tratamento, manutenção e destruição ou cancelamento dos mesmos (pelas garantias do Código de Processo Penal e pela Lei n.º 32/2008, de 17 de julho) – da competência levada a cabo pela 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 acessos aos dados em causa".

O assunto foi revisto pela Lei Orgânica n.º 4/2017, de 25 de agosto[178], em que a natureza jurisdicional prévia decorrente do acesso aos dados de tráfego é constituída por um procedimento faseado, conforme concretiza o Professor JORGE BACELAR GOUVEIA (2018, p. 751ss):

- a *iniciativa*: desde logo, o "procedimento obrigatório e vinculado de autorização judicial prévia do acesso dos oficiais de informações do SIS e do SIED a dados de telecomunicações e Internet inicia-se com o pedido elaborado pelos diretores do SIS ou do SIED, ou de quem os substitua em caso de ausência ou impedimento, enviado pelo Secretário-Geral do Sistema de Informações da

[178] "A tramitação da autorização do acesso a estes dados [dados de tráfego] foi profundamente remodelada por este diploma [Lei Orgânica] e tem uma natureza jurisdicional prévia", conforme JORGE BACELAR GOUVEIA (2018).

República Portuguesa ao Presidente do Supremo Tribunal de Justiça, com conhecimento ao Procurador-Geral da República" (Art. 9.º, n.º1);

- a *decisão*: "A decisão judicial de concessão ou de denegação da autorização consta de despacho proferido no prazo máximo de 48 horas, fundamentado com base em informações claras e completas, nomeadamente quanto aos objetivos do processamento" (Art. 10.º, n.º 3);

- a *execução*: "A transmissão diferida dos dados de telecomunicações e Internet obtidos de acordo com o regime consagrado na presente lei processa-se mediante comunicação eletrónica, com conhecimento da formação das secções criminais do Supremo Tribunal de Justiça prevista no artigo 8.º e ao Procurador-Geral da República, nos termos das condições técnicas e de segurança fixadas em portaria do Primeiro-Ministro e dos membros do governo responsáveis pelas áreas das comunicações e da cibersegurança, 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" (Art. 11, n.º 1);

- o *acompanhamento*: "Após a comunicação prevista no n.º 1 do artigo anterior, a formação das secções criminais do Supremo Tribunal de Justiça valida o tratamento pelo SIS ou pelo SIED dos dados de telecomunicações e Internet considerados em conformidade com o disposto no número anterior" (Art. 12, n.º 2);

- a *fiscalização*: por um lado pelo CFDSIRP – na medida em que "A Comissão de Fiscalização de Dados do SIRP é a autoridade pública competente para a fiscalização do respeito pelos princípios e cumprimento das regras relativos à qualidade e à salvaguarda da confidencialidade e da segurança dos dados obtidos de acordo com o procedimento obrigatório e vinculado previsto na presente lei", por outro pelo CFSIRP – visto que "Compete ao Conselho de Fiscalização do SIRP receber do Secretário-Geral, com regularidade mínima bimensal, uma lista dos pedidos de autorização de acesso a dados de telecomunicações e Internet submetidos à formação das secções criminais referida no artigo 12.º podendo solicitar e obter os

esclarecimentos e informações complementares que considere necessários e adequados ao exercício das suas funções de fiscalização" (Art. 16.º, n.º 2).

Conforme interpreta JORGE BACELAR GOUVEIA (2018, p.753), "São várias as questões que aqui se levantam, se bem que esta versão do acesso aos metadados [decorrente da Lei Orgânica n.º 4/2017], por força da intervenção do Supremo Tribunal de Justiça, possa ter afastado boa parte dessas dúvidas, para não dizer todas elas sob o prisma de não se tratar de aceder a dados protegidos pela inviolabilidade das comunicações privadas, envolvendo o risco de inconstitucionalidade"[179].

Tal como explana o Parecer 2/2017 da CFDSIRP, a propósito da Proposta de Lei n.º 79/XIII/2.ª (GOV), "a intervenção prévia dos Serviços de Informações, no âmbito do combate a terrorismo, tem essencialmente em vista, (…), habilitar as autoridades judiciárias com a informação necessária para poderem levar a cabo, mais eficazmente, as funções de repressão e julgamento dos crimes que vierem eventualmente a ser cometidos". Por este motivo, para a CFDSIRP revela-se mais adequado desta forma "prever uma tal intervenção de apoio, (…), às autoridades judiciárias, no combate a formas particularmente graves de criminalidade, através de uma lei extravagante de natureza penal, que consagre, até por isso mesmo, adequadas formas de controlo judicial em todo o processo da referida intervenção" (p. 9).

7. Meios adequados às finalidades pretendidas?

Tal como aponta JORGE BACELAR GOUVEIA (2018, p. 695), "O setor mais controverso e decerto incompreendido da Segurança Nacional é o da Produção de Informações de Segurança do Estado, através dos serviços de inteligência".

Não podemos olvidar que "atendendo à sua natureza os serviços de informações partilham os problemas de outras entidades públicas: previnem uma acção disruptiva da normalidade da vida em sociedade e essa acção preventiva é silenciosa em relação

[179] Conforme continua o Professor Catedrático: "Note-se que, se é verdade que a CRP, quanto a este direito, liberdade e garantia, refere a sua eventual quebra no quadro da investigação criminal que nunca foi atribuída à produção de informações, não é menos firme que os termos em que está prevista a recolha dos dados jamais se pode colocar nessa perspetiva, com o que se protegem os valores subjacentes à inviolabilidade das comunicações privadas" (2018, p. 754).

ao custo-benefício para a comunidade de cidadãos, considerando que só é aferido o benefício da prevenção quando há uma acção"[180]. Nesta senda, ALICE FEITEIRA (2015,p. 8), a propósito da Segurança como um dos fins do Estado[181], apela que a "determinação do conceito de segurança, num Estado de direito democrático resulta necessariamente de uma permanente dialéctica entre as necessidades humanas, historicamente condicionadas, a protecção dos valores essenciais da sociedade e o poder e legitimação da administração do Estado", para o efeito o domínio da administração pública da segurança é decomposto numa dimensão legal e operativa que resulta da delegação de competências a determinadas entidades públicas que se traduzem em tarefas de segurança.

Conforme JÚLIO PEREIRA (2016) revela "A ação terrorista, até se manifestar por qualquer das suas formas, tem um longo percurso preparatório a que muitas vezes está vedada a intervenção policial. Uma célula terrorista necessita para os seus membros de casas seguras, transportes, dinheiro, documentos de identificação e de viagem, armas, explosivos, comunicações, etc. E a montante de tudo isto há outras circunstâncias a ter em conta como métodos, ambientes e causas de radicalização, processos de recrutamento, disseminação de propaganda, padrões de comportamento e muitos outros fatores, cujo conhecimento é indispensável para a definição de uma estratégia de prevenção e repressão, e cujo conhecimento compete aos serviços de informações, sem prejuízo das competências policiais quando os referidos atos só por si constituam crime ou atos preparatórios criminalmente puníveis". Desta forma, compreende-se por isso que as informações sejam a "primeira linha de prevenção e combate às ameaças", no sentido em que a ação policial sem elas será predominantemente reativa. Não esquecendo que "os elementos fornecidos pelos serviços, não podendo constituir prova, servem no entanto como radar para a ação policial, potenciado o sucesso das ações de prevenção e de investigação"[182].

[180] ALICE FEITEIRA - *A Administração Pública da Segurança e Cidadania*, 2015 p. 20
[181] Para a autora "o Estado não é um dado da natureza, nem um fim em si mesmo, mas antes uma realidade histórica e instrumental ao serviço dos fins comuns às pessoas que integram essa comunidade política" (2015, p. 8).
[182] *Op. Cit. Liber Amicorum Manuel Simas Santos*, p. 811.

Acompanhamos ALICE FEITEIRA (2015, p. 12), quando refere que "Num Estado de matriz liberal, a relação comunicacional entre a administração e os cidadãos, bem como a eficiência das atividades públicas, deve espelhar uma visão integrada da sociedade quanto à natureza dessas actividades, dos meios afectos e da sua necessidade, de forma a garantir um consenso social quanto ao exercício dessas competências".

Ainda segundo o Parecer elaborado pelo Gabinete do Secretário-Geral do SIRP, a propósito da Proposta de Lei n.º 79/XIII/2.ª (GOV), o "acesso aos dados de comunicações e internet, constitui um meio operacional de pesquisa compatível, num Estado de Direito democrático, com o grau de sofisticação da ameaça, bem como um vetor essencial da cooperação internacional do Estado Português com sistemas e alianças de segurança de que é membro fundador e parte ativa".

Neste sentido, importa realçar a advertência feita pelo RASI 2017, na medida em que "O agravamento da ameaça terrorista que a Europa conheceu nos últimos anos determinou o fortalecimento dos mecanismos de prevenção dos serviços de informações de segurança europeus, sobressaindo a cooperação internacional como uma pedra angular desse fortalecimento" (p. 75). Desta forma, constitui orientação estratégica para 2018 o "Reforço da articulação e da partilha de informações entre todos os órgãos de polícia criminal, serviços de informações e entidades públicas e privadas, tendo em vista a prevenção do recrutamento, radicalização e financiamento do terrorismo" (p. 232).

Trata-se desta forma de situação contrária ao referindo o Acórdão de 21/12/2016, *Tele 2* (processos n.º C-203/15 e C-698/15) no que concerne à Lei n.º 32/2008, de 17 de julho[183], que ao analisar a legislação de transposição da Suécia e do Reino Unido conclui que "uma regulamentação deste tipo não exige nenhuma relação entre os dados cuja conservação se encontra prevista e uma ameaça para a

[183] Que transpôs para o ordenamento jurídico português a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março e que veio regular "a conservação e a transmissão dos dados de tráfego e de localização relativos a pessoas singulares e a pessoas coletivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes".

segurança pública. Nomeadamente, não está limitada a uma conservação que tenha por objeto dados relativos a um período temporal e/ou uma zona geográfica e/ou a um círculo de pessoas que possam estar envolvidas de uma maneira ou de outra numa infração grave, nem a pessoas que, por outros motivos, mediante a conservação dos seus dados, podiam contribuir para a luta contra a criminalidade…"[184].

No parecer do CFSIRP, de julho de 2015 a propósito da Proposta de Lei n.º 345/XII/4, foram apontadas limitações ao Serviços de Informações portugueses, no sentido em que seriam os únicos que, no contexto atual, não dispunham de qualquer possibilidade legal de prosseguir os seus objetivos através da recolha de informações previstas na norma discutida da referida proposta, sendo que "essa limitação se reflete, naturalmente, na sua atividade, quer quanto à possibilidade de colaboração com serviços congéneres no quadro dos compromissos internacionais do Estado (e mesmo da luta internacional contra o terrorismo), quer quanto às possibilidades de deteção de ameaças em território nacional". Desta feita, não podemos limitar a ação dos Serviços de Informações portugueses à deriva da possibilidade de cedência de informações por serviços congéneres, à dependência exclusiva da disponibilidade de cooperação destes últimos.

O Relatório da Agência da União Europeia para os Direitos Fundamentais (2015, p. 77) adverte que "*Clear and accessible legislation, strong oversight mechanisms, proper control mechanisms, as well as effective remedies are only some of the elements essential for the kind of accountability that encourages the level of trust society should have vis-à-vis its intelligence service. Achieving this may undeniably be difficult*". Daí que "*The difficulty in producing clear and accessible*

[184] Parágrafo 106 do Acórdão de 21/12/16, *Tele 2*. Nestes termos, concluiu que "O artigo 15.º, n.º 1, da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), conforme alterada pela Diretiva 2009/136/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, lido à luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia, deve ser interpretado no sentido de que se opõe a uma regulamentação nacional que prevê, para efeitos de luta contra a criminalidade, uma conservação generalizada e indiferenciada de todos os dados de tráfego e de todos os dados de localização de todos os assinantes e utilizadores registados em relação a todos os meios de comunicação eletrónica".

legislation, which is merely the first step in attaining a transparent system, is therefore an obstacle"[185].

Em 2007, SÓNIA REIS & MANUEL BOTELHO DA SILVA previam que o futuro das estruturas de *intelligence* correspondesse mais a uma ampliação dos meios de atuação, com limites claramente disciplinados, do que à modificação das atribuições dos Serviços de Informações - no sentido em que continuariam a centrar-se no plano estritamente preventivo e de produção de informações, sem desempenho de quaisquer funções policiais ou de investigação criminal (p. 17) – verificamos que estas projeções foram cumpridas, acreditando que continue a ser este o caminho a prosseguir.

[185] O relatório refere ainda a importância da partilha de metodologias entre sistemas congéneres, assim "*Exchanges on practices between actors help clarify and enhance relevant control standards. Despite the great diversity and the predominantly national competences of oversight bodies, exchanges can help promote promising practices. When it comes to exchanges between oversight bodies, already existing networks, such as the European Network of National Intelligence Reviewers (ENNIR), can be fostered. Such exchanges and cooperation should, however, not be limited to oversight bodies. Similar exchanges on the manner in which intelligence services uphold fundamental rights in their work could also be beneficial*" (p. 77). A propósito, é interessante consultar a informação transmitida pela "*European network of national Intelligence Reviewers* (ENNIR)", através de sítio disponível online: www.ennir.be/ [última consulta a 15/08/2018].

CONCLUSÕES

A propósito do significado da história e da reconstrução do sistema internacional como "o derradeiro desafio da diplomacia dos nossos tempos", na procura do equilíbrio entre a estabilidade e a defesa de princípios universais, HENRY KISSINGER (2018, p. 428) admite que se trata de "uma questão a que temos de responder da melhor forma possível, na certeza, porém, de que o debate estará sempre em aberto, de que cada geração será julgada pela forma como lidou com as questões maiores e mais prenhes de consequências, e que as decisões que os estadistas tomam para enfrentar esses desafios têm de ser tomadas antes de se saber qual vai ser o seu resultado". Urge, por isso, debater e estudar a área da segurança do ponto de vista académico, para que as políticas públicas sejam cada vez mais baseadas em conhecimento científico, principalmente, pelo incremento de um relacionamento próximo entre as matérias da Segurança e do Direito.

Neste trabalho procurámos colocar a par matérias tão sensíveis como a Liberdade, a Segurança e a Democracia, numa sociedade altamente instável. Entendemos que o combate das ameaças ao contexto securitário alicerçado no uso das tecnologias da comunicação constitui um desafio complexo dos Estados democráticos, pelo que não devemos ignorar o facto do avanço legislativo alcançado pela Lei Orgânica n.º 4/2017, de 25 de agosto, se tratar de um importante passo ancorado na neutralização de ameaças.

Acreditamos, contudo, que a potencialidade desta ferramenta de *intelligence* deva ser ponderada e acautelada por meio de sérios critérios de adequação, proporcionalidade e necessidade ao longo de todo o processo de utilização e assente em finalidades claras e objetivas - numa perspetiva protetora dos direitos fundamentais envolvidos, mormente a liberdade, a privacidade e a segurança. Assim, devemos apreciar esta medida no panorama do esforço e reforço constante do SIS e do SIED, com vista ao sucesso da sua honrosa missão, num contexto em que as exigências de acompanhamento dos serviços congéneres são elevadas, e quando assumir distinta posição não auguraria melhores resultados.

A decisão explanada no Acórdão n.º 403/2015 não foi surpreendente, já que foi ao encontro de uma metodologia de interpretação restritiva da norma da Constituição, contudo é certo que a decisão do Tribunal Constitucional se traduziu indiretamente na manutenção de uma debilidade há muito visível dos Serviços de Informações. Notamos, igualmente, a dificuldade de o Tribunal Constitucional se afastar daquilo que seria a necessidade de abordar de forma integrada as missões e necessidades do SIRP.

A recolha de informações pessoais através da utilização das tecnologias da comunicação pode levar a diferentes consequências para a privacidade das pessoas, bem como violar princípios fundamentais afins, como a autodeterminação informacional e o direito de acesso aos dados pelo seu titular. De forma a dirimir nefastas consequências, a utilização do meio técnico previso na Lei Orgânica n.º 4/2017, de 25 de agosto, é eficazmente controlado, devendo ser ponderado como uma medida de *ultima ratio,* ou seja, quando algum meio de produção de informações menos intrusivo (por exemplo, utilização de fontes abertas) não seja capaz de alcançar o mesmo objetivo.

Ao analisarmos as pretensões do progresso veiculado pela Lei Orgânica n.º 4/2017, de 25 de agosto aferimos a existência de uma maior cautela e controlo da atuação do SIS e do SIED. Nesta senda, aferimos que o previsto acesso pontual a dados de telecomunicações e Internet deve ser concedido quando existirem garantias mínimas que se traduza num benefício superior na produção de informações atinentes à prossecução de um objetivo previamente delimitado, com vista à neutralização de uma ameaça concreta, temporalmente demarcada.

Importa reforçar que o que se pretende através do acesso a estes dados não é um acesso a conteúdos das comunicações (sejam escritas ou de voz), pela intrusão ou ingerência nas comunicações (conforme prevista no n.º 4 do artigo 34.º da CRP) nem uma vigilância em massa, mas antes o acesso a dados destas comunicações (quer sejam de base, de localização do equipamento ou de tráfego) através da sua solicitação às entidades legitimamente incumbidas pelo seu tratamento - após

autorização e ordem por despacho judicial fundamentado de acordo com o procedimento estatuído também na Lei Orgânica n.º 4/2017, de 25 de agosto.

Verificamos igualmente que este avanço operacional é subordinado a um concertado, exigente e fiável mecanismo de controlo e fiscalização – algo vislumbrado por uma *natureza jurisdicional prévia* ao acesso, conforme pretendemos explanar no capítulo IV (especialmente nas secções 5. e 6.3). Entendemos que a atuação do SIS e do SIED esta sujeita a um intensivo escrutínio pelos órgãos de controlo e fiscalização de indiscutível competência e capacidade. Contudo, importa aqui deixar algumas questões para futuros estudos, nomeadamente: como se irão articular todos os mecanismos de controlo e fiscalização do SIRP? Existirá coordenação entre eles? Possuirá a secção do STJ competência técnica suficiente para averiguar as operações em curso?

Concluímos que não estamos perante uma abdicação desmesurável de Liberdade e Privacidade em benefício da nossa Segurança. Devemos caminhar no sentido em que a *intelligence* seja capaz de prever, com a maior antecedência possível, as ameaças concretas aos cidadãos e defender os princípios e valores do Estado de Direito democrático. Não devemos, de forma alguma, limitar a produção de informações por meio de *open source intelligence* ou *human intelligence*, quando é gritante a necessidade de recolher informações por via de *communications intelligence*, sob a forma de *signals intelligence (SIGINT).* Acrescem as finalidades que auguram alcançar, na medida em que se tratam do combate a ameaças cujo a seu carácter e implicações são vulgarmente debatidos da sociedade civil. Entendemos, por isso, tratar-se de um meio de *intelligence* que os serviços devem dispor face às necessidades securitárias discutidas ao nível do quadro político e social atual.

Na nossa opinião, assistimos paralelamente a uma falta de cultura de segurança e de informações em Portugal. Se não vemos ou sentimos a ameaça não sentimos a necessidade de antecipá-la e preveni-la, falhando a ideologia de que as decisões que tomamos hodiernamente terão um forte impacto no nosso futuro. Urge discutirmos constantemente as medidas securitárias que devemos ou não adotar e aferir o seu

impacto no sentimento de (in)segurança da sociedade[186]. Entendemos, por isso, que devemos continuar a desenvolver uma cultura de segurança e de informações em Portugal, não comercializável por frações político-partidárias. Antes, se requer uma maior mobilização em prol da discussão pública, bem como o incremento da sensibilização e entendimento da sociedade civil destas matérias – principalmente, acerca da intervenção do SIRP e da sua importância no panorama da segurança, já que do seu desempenho escassa a devida valorização, reconhecimento e interesse pela comunidade. Assiste-se, por isso, à necessidade de combater o facto de que se a sociedade não sente a necessidade de antecipar e prevenir uma ameaça, simplesmente por que não a presencia, não se interessa por discutir determinada medida securitária nem exercer a sua cidadania na área da segurança.

Procurámos demonstrar a manifesta necessidade de adotar esta metodologia de atuação na adaptação ao combate às novas ameaças, já que se traduz numa maior capacidade e aperfeiçoamento da atividade de *intelligence*, cujas informações obtidas se podem verificar cruciais ao desempenho do decisor político ou dos órgãos de polícia criminal. Entendemos que as medidas pontuais de acesso aos dados de telecomunicações e Internet constitui um vetor de cooperação internacional do Estado Português com Serviços de Informações congéneres (destacando-se o papel relevante a considerar no seio da UE e da OTAN), através da sua atuação numa lógica eminentemente preventiva e proativa - não limitando as suas capacidades de forma a permeabilizar ameaças ao Estado democrático. Revela-se igualmente importante fomentar o diálogo e a reflexão crítica desta matéria entre as várias estruturas incumbidas da Segurança.

Propomos a criação de relatórios anuais de conhecimento público, descritivos não só da quantidade de acessos pontuais concedidos aos Serviços de Informações, como também indicativo da qualidade destes dados para atingir as finalidades que se

[186] O Professor NELSON LOURENÇO adverte, quanto ao sentimento de insegurança, que "é corretamente definido como um conjunto de representações e de manifestações, quer individuais quer coletivas, de inquietação, de perturbação ou de medo e de preocupação pela ordem social. Surge associado a um clima generalizado de ansiedade, cujo origem assenta no complexo e muito rápido processo de mudanças sociais que caracteriza a sociedade moderna e em que o aumento da criminalidade é uma das consequências mais visíveis" (*Enciclopédia de Direito e Segurança*, p. 443).

pretendiam alcançar - por exemplo, pelo sucesso ou insucesso de atingir os objetivos a que se destinavam e face a que ameaça. Esta medida corresponderia a uma maior transparência, na medida do possível, da Administração Pública e incrementaria a abertura à discussão da sociedade civil.

Urge repensarmos o desenvolvimento operacional do SIRP na próxima revisão da CRP, compensado o défice constitucional regulatório da produção de informações. Até então, não consideramos que deva existir um entendimento radicalizado do Art. 34.º, n.º 4 da CRP, sendo que não podemos ficar presos a crenças do passado quando existe a necessidade de adotar uma visão atualista da Constituição. Numa próxima revisão constitucional é premente a necessidade de atualizar matérias relacionadas com a segurança numa perspetiva generalizada, transformando ideologias mais militarizadas próprias do tempo da sua redação, concedendo maior relevância à constitucionalização da segurança interna e dos Serviços de Informações.

BIBLIOGRAFIA

- AGÊNCIA DA UNIÃO EUROPEIA PARA OS DIREITOS FUNDAMENTAIS
  ____ *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU: Mapping Member State's legal frameworks – V.1*, novembro de 2015. Disponível em http://fra.europa.eu/en/publication/2015/surveillance-intelligence-services, acedido a 16/06/2018.
  ____ *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU – V. II*, maio 2018. Disponível em http://fra.europa.eu/en/publication/2018/surveillance-intelligence-services-fundamental-rights-safeguards-and-remedies, acedido a 16/06/2018.
- ANES, José Manuel - *Organizações Criminais: Uma Introdução ao Crime Organizado*. Lisboa: Universidade Lusíada, 2010
- BECK, Ulrich – *Sociedade de Risco Mundial: em busca da segurança perdida*, 1.ª Ed., Lisboa: Edições 70, 2015. ISBN: 978-972-44-1857-5.
- BORAZ, S. & BRUNEAU, T. – "Reforming Intelligence: Democracy and Effectiveness", In *Journal of Democracy*, Vol. 17, N. º 3, California: National Endowment for Democracy and The Johns Hopkins University Press, julho de 2006. Disponível em http://hdl.handle.net/10945/43134, acedido a 03/04/2018.
- CANOTILHO, J. J. Gomes – *Direito Constitucional e Teoria da Constituição*, 7.ª Edição, Lisboa: Almedina, 2007, p. 514.
- CANOTILHO, J. J. Gomes & MOREIRA, V. – *Constituição da República Portuguesa Anotada*, Vol. I, 4.ª ed., Coimbra: Coimbra Editora, 2007.
- CARVALHO, Jorge Silva – "Segurança Nacional, Serviços de Informações e as Forças Armadas", In *Revista de Segurança e Defesa*, N.º 11, set./nov. 2009.
- CASTRO, Catarina Sarmento e - *O Direito à Autodeterminação Informativa e os Novos Desafios Gerados pelo Direito à Liberdade e à Segurança no pós 11 de Setembro*, 2005. Disponível em: http://egov.ufsc.br/portal/conteudo/o-direito-%C3%A0-autodetermina%C3%A7%C3%A3o-informativa-e-os-novos-desafios-gerados-pelo-direito-%C3%A0-liberda, acedido a 15/02/2018.

- COMISSÃO DE VENEZA – *Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies: Adopted by the Venice Commission at its 102nd Plenary Session*. Strasbourg, 01/04/2015. Disponível em: http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e, acedido a 02/07/2018.

- COMISSÃO EUROPEIA – *Agenda Europeia para a Segurança*, COM(2015) 185 final. Estrasburgo, 28/04/2015. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0185&from=EN, acedido a 17/06/2018.
- COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS
  ____ Parecer N.º 24/2017
  ____ Parecer N.º 29/98
  ____ Parecer N.º 38/2017
  ____ Parecer N.º 2/2017
- CONSEIL DES MINISTRES RÉPUBLIQUE FRANÇAISE – "Projet de Loi Renseignement: «Protéger les Français dans le respect des libertés»", In *Dossier de Presse*, 19/03/2015. Disponível em: https://www.gouvernement.fr/sites/default/files/document/document/2015/03/dp-loi-renseignement_v3-bat.pdf, acedido a 22/07/2018.
- CONSELHO DE FISCALIZAÇÃO DO SISTEMA DE INFORMAÇÕES DA REPÚBLICA PORTUGUESA – Parecer do Conselho De Fiscalização Do Sistema De Informações Da República Portuguesa (1 de janeiro a 30 de junho de 2016), Lisboa, 31/01/2017. Disponível em: http://www.cfsirp.pt/Geral/parecer-1-semestre-de-2016.html, acedido a 17/07/2018

- CONVENÇÃO SOBRE O CIBERCRIME, Budapeste, 23/11/2001. Disponível em https://www.cicdr.pt/documents/57891/128776/Conven%C3%A7%C3%A3o+Cibercrime.pdf/3c7fa1b1-b08e-4f66-9553-f4470f502b9c, acedido a 17/07/2018.

- CRUZ, Adélio Neiva da - *Ameaças Assimétricas e Planeamento Estratégico* (12/12/2017), Reitoria da Universidade Nova de Lisboa. Disponível em https://www.sis.pt/pagina/88/discurso-do-diretor-do-sis, acedido a 01/06/2018.
- CURADO, Henrique & GOMES, Paulo Veloso – "Os sistemas de inteligência num contexto de homeland defence e a tutela da privacidade", In *Segurança e Defesa*, N.º 21, Loures, maio-agosto de 2012, p. 28-32, ISSN 1646-6071.
- DEIBERT, R. – "The Geopolitics of Cyberspace after Snowden", In *Current History*, Nova Iorque, janeiro de 2015. Disponível em http://www.currenthistory.com/Deibert_CurrentHistory.pdf, acedido a 03/04/2018.
- DOUTRIAUX, Me Cécile – *Données personnelles et cybersurveillance*, in *Revue défense nationale*, N.º 775, Paris, dezembro de 2014. ISSN 2105-7508. Disponível em: https://www.chaire-cyber.fr/IMG/pdf/article_3_17-_chaire_cyberdefense.pdf, acedido a 10/06/2018.
- ESTRATÉGIA NACIONAL DE COMBATE AO TERRORISMO, aprovada pela Resolução do Conselho de Ministros n.º 7 -A/2015, de 20 de fevereiro.
- FEITEIRA, Alice – "A Administração Pública da Segurança e Cidadania", In *Revista de Direito e Segurança*, Ano III, N.º 5, jan-jun, 2015.
- FELTEN, Edward W. – *Committee on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act*, United States Senate: EUA, 02/10/2013. Disponível em https://www.judiciary.senate.gov/download/testimony-of-felten-pdf, acedido a 16/06/2018.
- FERREIRA, Arménio Marques – "O Sistema de Informações da República Portuguesa" In *Estudos de Direito e Segurança* (coordenação JORGE BACELAR GOUVEIA e RUI PEREIRA), Coimbra: Edições Almedina, 2007, p. 69. ISBN: 9789724030531
- FONTES, José. – "A Constituição e os Serviços de Informações", In *Segurança e Defesa*, n.º 15, outubro-dezembro 2010.

- GOUVEIA, Jorge Bacelar

____ *Direito da Segurança: Cidadania, Soberania e Cosmopolitismo*, Lisboa: Edições Almedina, 2018. ISBN: 978972407492.

____ "Os direitos fundamentais à proteção dos dados pessoais informatizados", In *Revista da Ordem dos Advogados*, Ano 51, 1991-III, pp. 699 e ss..

____ "Os serviços de informações de Portugal: organização e fiscalização", In *Estudos de Direito e Segurança* (coordenação JORGE BACELAR GOUVEIA e RUI PEREIRA), Coimbra: Edições Almedina, 2007, pp. 171ss. ISBN 978-972-40-3053-1.

____ "Os serviços de informações de Portugal: organização e fiscalização", In *Revista de Direito e Segurança*, n.º 1, jan./jun de 2013: 63-85

- GREENWALD, Glenn – *Edward Snowden: Sem Esconderijo*, 1.ª Edição, Lisboa: Bertrand Editora, 2014. ISBN: 978-972-25-2847-4.
- HOME OFFICE – *Acquisition and Disclosure of Communications Data: Code of Practise*, março de 2015, Londres. ISBN 9780113413805. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf, acedido a 01/07/2018.
- HOUSE OF COMMONS – *Daily Hansard*: *Statement on G20 and the Paris attacks (*17/11/2015). Disponível em https://publications.parliament.uk/pa/cm201516/cmhansrd/cm151117/debtext/151117-0001.htm#15111751000004, acedido a 01/07/2018.
- INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT - *ISC Annual Report 2016-2017*. Disponível em: http://isc.independent.gov.uk/committee-reports/annual-reports, acedido a 17/07/2018.
- KISSINGER, Henry – *A Ordem Mundial*, Lisboa: Publicações D. Quixote, 2018. ISBN: 978-972-206476-7

- LOURENÇO, Nelson – "Sentimento de Insegurança", In *Enciclopédia de Direito e Segurança* (coordenação JORGE BACELAR GOUVEIA e SOFIA SANTOS), Coimbra: Almedina, pp. 443-444, 2015.
- LUCENA, José N. Sousa – "Tipologia e Hierarquização das Ameaças, A importância das informações. Tipos de Sistemas de Informações", In *Revista Nação e Defesa*, Ano XVII, N.º 61, p. 129, janeiro-março 1991. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/1749/1/NeD61_JoseNSousaLucena.pdf, acedido a 17/07/2018.
- LYON, David – *Surveillance Power and Everyday Life: The Oxford Handbook of Information and Communication Technologies*, 2007. Obtido a 12/04/2018 disponível em: https://www.researchgate.net/publication/239850589_Surveillance_Power_and_Everyday_Life.
- MARTINS, Fernando M. C. – "Inteligência", In *Revista Lusíada*: *Política Internacional e Segurança*, n.º 3, p. 144, 2010. Disponível em http://repositorio.ulusiada.pt/bitstream/11067/1012/1/LPIS_n3_7.pdf, acedido a 22/08/2018.
- MASSENO, Manuel David

____ *A Proteção dos dados pessoais enquanto limite à investigação do cibercrime: Que fazer, na UE, depois do Acórdão Digital Rights Ireland?*, V Simpósio da Segurança Informática e Cibercrime, 8 de maio 2014, auditório do Instituto Politécnico de Beja. Disponível em: https://ipbeja.academia.edu/ManuelDavidMasseno, acedido a 28/02/2018.

____ *Será constitucional o regime de acesso aos "Dados de Tráfego?"*. SimSIC' 10, Beja, 19 de maio 2010. Disponível em: https://ipbeja.academia.edu/ManuelDavidMasseno, acedido a 28/02/2018.

- MIGUEL, Carlos Ruiz – "Problemas actuales del derecho de los servicios de inteligencia", In *Inteligencia y Securidad* 1, 2006. Disponível em:

https://www.academia.edu/10234274/_Problemas_actuales_del_Derecho_de_los_servicios_de_inteligencia_, acedido a 14/10/2017.

- MIRANDA, J. – *Constituição e Cidadania: Terrorismo e Direitos Fundamentais*, 2003, pp. 317-323. ISBN 972-32-1167-X
- OMAND, D.; BARTLETT, J.; MILLER, C. – "A balance between security and privacy online must be struck…", In *Demos*, Londres, 2012. Disponível em https://www.demos.co.uk/wp-content/uploads/2017/03/intelligence-Report.pdf, acedido a 10/10/2017.
- PEREIRA, Júlio

____ "Os Serviços de Informações e a Prevenção e Investigação Criminais", In *Liber Amicorum: Manuel Simas Santos* (coordenação ANDRÉ PITON e ANA CARNEIRO), Lisboa: Rei dos Livros, 2016. ISBN: 978-989-8823-20-5

____ "Segurança Interna: o mesmo conceito novas exigências", In *Segurança e Defesa*, N.º 3, pág. 97ss., maio-julho 2007.

____ Conferência "Informações Estratégicas e Segurança". *O SIRP*, Instituto de Defesa Nacional, Pós-Graduação em Estudos Estratégicos e de Segurança, 28/03/2012[1]. Disponível em https://www.sirp.pt/media/2018/05/informacoes-estrategicas-e-seguranca.pdf, acedido a 15/06/2018.

____ Seminário Internacional: "A Segurança Global e os Sistemas Democráticos: desafios e perspetivas", IV Painel Temático - *Desafios do Futuro: Os Vetores Estratégicos das Informações em Portugal*, Reitoria da Universidade NOVA de Lisboa, 06/12/2012[2]. Disponível em https://www.sirp.pt/media/2018/06/seminario.pdf, acedido a 15/06/2018

- PEREIRA, R, & FEITEIRA, A. – "Serviços de Informações", In *Enciclopédia de Direito e Segurança* (coordenação JORGE BACELAR GOUVEIA e SOFIA SANTOS), Coimbra: Almedina, pp. 448-450, 2015.
- PRESIDÊNCIA DE CONSELHO DE MINISTROS - Parecer do Gabinete do Secretário-Geral do Sistema de Informações da República Portuguesa sobre o Projeto de Lei n.º 480/XIII-2.ª.

- RAMALHO, David Silva & COIMBRA, José Duarte – "A declaração de invalidade da diretiva 2006/241CE: presente e futuro da regulação sobre conservação de dados de tráfego para fins de investigação, deteção e repressão de crimes graves", In *Liber Amicorum: Manuel Simas Santos* (coordenação ANDRÉ PITON e ANA CARNEIRO), Lisboa: Rei dos Livros, 2016. ISBN: 978-989-8823-20-5.
- REIS, Sónia & BOTELHO DA SILVA, Manuel – "O Sistema de Informações da República Portuguesa", In *Revista da Ordem dos Advogados*, Ano 67, III – Lisboa, dezembro 2007.
- RODRIGUES, Joaquim Chito – "Os Sistemas de Informações e a Saúde da Democracia", In *Nova Cidadania: Liberdade e Responsabilidade Pessoal*, Ano 12, N.º 46, Lisboa, 2011, ISNN 0874-5307.
- SANTOS, Sofia – "Segurança Cooperativa", In *Enciclopédia de Direito e Segurança* (coordenação JORGE BACELAR GOUVEIA e SOFIA SANTOS), Coimbra: Almedina, pp. 408-409, 2015.
- SCHUSTER, S.; BERG, M.; LARRUCEA, X.; SLEWE, T.; IDE-KOSTIC, P. – *Mass surveillance and technological policy options: Improving security of private communications*, in *Computer Standards & Interfaces*, V. 50, ELSEVIER, pp. 76-82, fevereiro de 2017. Disponível em: https://www.sciencedirect.com/science/article/pii/S0920548916300988?via%3Dihub, acedido a 21/03/2018.
- SISTEMA DE SEGURANÇA INTERNA – *Relatório Anual de Segurança Interna (RASI)*, 2017.
- VALENTE, Manuel Guedes – *Escutas telefónicas: Da excecionalidade à vulgaridade*, 2-ª Edição, Coimbra: Almedina, 2008, ISBN 978-972-40-3583-3.
- VILLALOBOS, M.ª - *El Control de los Servicios de Inteligencia en los Estados Democraticos, I Congreso Nacional de Inteligencia*, Madrid, 23/10/2008. Disponível em: http://digibug.ugr.es/bitstream/10481/27872/1/El%20control%20democr%C3%

A1tico%20de%20los%20servicios%20de%20inteligencia.pdf, acedido a 10/10/2017.

- VITKAUSKAS, Dovydas – *The Role of a Security Intelligence Service in a Democracy*, NATO: Democratic Institutions Fellowship Programme 1997-1999, junho de 1999. Disponível em: http://www.nato.int/acad/fellow/97-99/vitkauskas.pdf, acedido a 14/05/2018.
- WOOD, David Murakami & BALL K. – "A Report on the Surveillance Society: Public Discussion Document", In *Surveillance Studies Network*, setembro de 2006. Disponível em https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf, acedido a 13/10/2017.

LEGISLAÇÃO NACIONAL

- Código Civil
- Constituição da República Portuguesa
- Decreto n.º 426/XII da Assembleia da República - Regime jurídico do Sistema de Informações da República Portuguesa (revoga 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).
- Decreto-Lei n.º 188/81, de 2 de julho
- Decreto-Lei n.º 224/85, de 4 de julho - Estabelece a orgânica do Serviço de Informações Estratégicas de Defesa, criado pela Lei n.º 30/84, de 5 de setembro que aprova a Lei Quadro do Sistema de Informações da República Portuguesa.
- Decreto-Lei n.º 225/85, de 4 de julho - Estabelece a orgânica do Serviço de Informações de Segurança, criado pela Lei n.º 30/84, de 5 de setembro (Lei Quadro do Sistema de Informações da República Portuguesa).
- Decreto-Lei n.º 226/85, de 4 de julho - Reestrutura o Serviço de Informações Militares, integrando-o no Sistema de Informações da República Portuguesa, ao abrigo da Lei n.º 30/84, de 5 de setembro (Lei Quadro do Sistema de Informações da República Portuguesa).

- Decreto-Lei n.º 254/95, de 30 de julho - Estabelece a orgânica de Serviço de Informações Estratégicas de Defesa e Militares (SIEDM)
- Decreto-Lei n.º 290-A/99, de 30 de julho - Estabelece as condições gerais a que obedece a exploração de redes públicas de telecomunicações no território nacional tendo em vista a oferta de rede aberta, incluindo a oferta de circuitos alugados.
- Decreto-Lei n.º 290-B/99 de 30 de julho - Aprova o Regulamento de Exploração dos Serviços de Telecomunicações de Uso Público.
- Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12/07/2002 - relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas).
- Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15/03/2006 - 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.
- Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 - Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
- Lei n.º 109/2009, de 15 de setembro - Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.
- Lei n.º 32/2008, de 17 de julho - Transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.
- Lei n.º 41/2004, de 18 de agosto - Transpõe para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de Julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas.

- Lei n.º 49/2008, de 27 de agosto - Aprova a Lei de Organização da Investigação Criminal.
- Lei n.º 67/98, de 26 de outubro - Transpõe para a ordem jurídica interna a Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
- Lei n.º 69/98, de 28 de outubro - Regula o tratamento dos dados pessoais e a proteção da privacidade no sector das telecomunicações (transpõe a Diretiva n.º 97/66/CE, do Parlamento Europeu e do Conselho, de 15 de dezembro de 1997)
- Lei n.º 88/89, de 11 de setembro - Define a Lei de Bases do Estabelecimento, Gestão e Exploração das Infra-Estruturas e Serviços de Telecomunicações.
- Lei n.º 9/2007, de 19 de fevereiro - Estabelece a orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa, do Serviço de Informações Estratégicas de Defesa e do Serviço de Informações de Segurança e revoga os Decretos-Leis n.os 225/85, de 4 de Julho, e 254/95, de 30 de Setembro.
- Lei n.º 91/97, de 1 de agosto - Define as bases gerais a que obedece o Estabelecimento, gestão e exploração de redes de telecomunicações e a prestação de serviços de telecomunicações.
- Lei Orgânica n.º 4/2004, de 6 de novembro - Altera a Lei Quadro do Sistema de Informações da República Portuguesa.
- Lei Orgânica n.º 4/2017, de 25 de agosto - Aprova e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa e procede à segunda alteração à Lei n.º 62/2013, de 26 de agosto (Lei da Organização do Sistema Judiciário).
- Portaria n.º 237-A/2018, 27 de agosto de 2018 - Define as condições técnicas e de segurança da comunicação eletrónica para efeito de transmissão diferida dos dados de telecomunicações e Internet pelos oficiais de informações do Serviço de Informações de Segurança e do Serviço de Informações Estratégicas de Defesa.
- Proposta de Lei n.º 345/XII/4.ª (GOV).

- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 - Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).
- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril - Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

OUTRA LEGISLAÇÃO

- Tratado da União Europeia
- Tratado de Funcionamento da União Europeia

LEGISLAÇÃO ESTRANGEIRA

Brasil:

- Resolução n.º 164, de 28 de maio de 2013

Reino Unido:

- *Intelligence Services Act (ISA)*
- *Human Rights Act*
- *Regulation of Investigatory Powers Act (RIPA)*

França

- *LOI n° 2015-912 du 24 juillet 2015 relative au renseignement*
- *Code de la sécurité intérieure*
- *LOI n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales*

Alemanha

- *Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz* (Lei Federal de Proteção Constitucional – BverfSchG)
- *Gesetz über den militärischen Abschirmdienst (*Lei do Serviço de Proteção Militar)

- *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (*Lei sobre a limitação do sigilo postal e de telecomunicações)
- *Telekommunikationsgesetz* (Lei das Telecomunicações)
- *Gesetz über den Bundesnachrichtendienst* (Ato do Serviço Federal de Inteligência)

JURISPRUDÊNCIA CONSULTADA

- Acórdão n.º 403/2015 do Tribunal Constitucional, de 27/08/2017 (Processo n.º 773/15)
- Acórdão n.º 486/2009 do Tribunal Constitucional (Processo n.º 4/09)
- Acórdão *Weber Saravia* v. *Germany*, de 29/06/2006
- Acórdão de 08/04/2014 do Tribunal de Justiça, *Digital Rights Ireland e Seitlinger* (Processos C-293/12 e C-594/12)
- Acórdão de 06/10/2015, Caso *Schrems* (Processo C-362/14)
- Acórdão de 22/10/2001, *Roquette Frèrres* (Processo n.º C-94/00)
- Acórdão de 09/11/2010, *Volkerund Markus Schecke* (Processos C-92/09 e C-93/09)
- Acórdão de 02/08/1984, *Malone v. Reino Unido*

ÍNDICE