DEPARTAMENTO DE DIREITO

MESTRADO EM DIREITO

ESPECIALIDADE EM CIÊNCIAS JURÍDICO-CRIMINAIS

UNIVERSIDADE AUTÓNOMA DE LISBOA

"LUÍS DE CAMÕES"

DIREITO DE INGERÊNCIA NAS COMUNICAÇÕES. O ESPECIAL ACESSO A DADOS DE TRÁFEGO, DE BASE E DE LOCALIZAÇÃO NA PRODUÇÃO DE INFORMAÇÃO E PREVENÇÃO CRIMINAL

Dissertação para a obtenção do grau de Mestre em Direito

Autor: Ivan Soeiro Rodrigues

Orientador: Professor Doutor Armando Reis Dias Ramos

Coorientador: Professor Doutor Pedro Gonçalo Tavares Trovão do Rosário

Número do candidato: 20150508

22 Julho de 2022

Lisboa

AGRADECIMENTOS

As minhas palavras iniciais nunca poderiam deixar de ser para o Doutor Reginaldo Rodrigues de Almeida que não só facilitou o meu processo de acesso ao ensino superior, como sempre se mostrou disposto a ajudar-me nos momentos mais difíceis ao longo de todo o meu percurso académico, a ele, o meu muito obrigado sincero, nunca esquecerei os seus gestos as suas palavras, o seu apoio incomensurável… não só pela ajuda que me deu, estou grato, mas por o meu caminho um dia ter cruzado com o seu… obrigado, bem-haja.

A todos os professores, sem exceção, o meu muito obrigado foi uma honra, ter sido vosso aluno, ter partilhado momentos de reflexão e conhecimento, sem eles não conseguiria chegar até aqui.

A todos os meus familiares, pelo apoio incondicional que sempre demonstraram ao longo desta fase académica. Em especial à minha mulher que sacrificou horas de sono na revisão desta investigação, para além de não ter sido possível chegar aqui sem esse apoio.

A todos os colegas que me acompanharam neste desafio, e amigos que permitiram-me enriquecer enquanto pessoa. A todos aqueles com quem me cruzei e não tive oportunidade de agradecer pelos seus contributos nas conversas de circunstância e debates de ocasião.

Um especial sentimento de apreço e gratidão ao meu orientador, Professor Armando Ramos, que foi sem dúvida, "o" elemento-chave na elaboração e conclusão desta investigação, demostrando sempre disponibilidade e apoio bem como ao Professor Trovão do Rosário, cujas aulas foram sempre memoráveis, não só pela dedicação aos alunos e aos conteúdos, mas porque sei, que daqui a muitos anos ainda as recordarei como pilares no meu percurso.

RESUMO

O acesso aos metadados pelos serviços de inteligência revela-se imprescindível na produção de informação e na prevenção criminal, num mundo cada vez mais digitalizado. Para que os Estados possam efetivar as suas capacidades e maximizar os instrumentos necessários a garantir a segurança nacional, a salvaguarda do Estado de Direito Democrático e a defesa dos cidadãos, deverão estes, atribuir aos organismos responsáveis de segurança as ferramentas adequadas de modo que, perante as ameaças mais heterogéneas que afetam os mais diversos campos da sociedade, possam responder da forma mais eficiente possível.

Assim, independentemente da controvérsia do tema a que nos propomos, no que respeita à ingerência nas comunicações e acesso aos metadados pelos Serviços de Informações, na deteção e prevenção de crimes como espionagem, terrorismo e criminalidade altamente organizada transnacional, é necessário que a legislação relativa aos Serviços de Informações acompanhe a evolução tecnológica e o cibercrime. Face aos desafios impostos pelo ordenamento jurídico português, mormente a Constituição da República Portuguesa, torna-se necessário uma análise circunscrita aos aspetos mais relevantes no que aos Serviços respeita, sem olvidar o controlo e fiscalização, os princípios norteadores da atividade de inteligência, as diferenças entre inteligência policial e inteligência estratégica e os ordenamentos jurídicos dos serviços de informações congéneres face á proteção da convenção dos direitos fundamentais.

Palavras-chave: Ingerência nas comunicações, metadados, inteligência, serviços de informações, produção de informações e prevenção criminal.

ABSTRACT

The access to metadata by intelligence services is essential in the generation of information and crime prevention in an increasingly digitized world. In order for States to carry out their capabilities and maximize the instruments necessary to guarantee national security, safeguard the Democratic Rule of Law and defend citizens, they must provide the responsible security bodies with the appropriate tools so that, facing the most heterogeneous threats that affect the most diverse fields of society, they can respond in the most efficient way possible.

Thus, regardless of the controversy of the subject we are proposing from, with regard to interference in communications and access to metadata by the Intelligence Services, in the detection and prevention of crimes such as espionage, terrorism and highly organized transnational crime, it is necessary that the related legislation Information Services keep up with technological developments and cybercrime. Given the challenges imposed by the Portuguese legal system, especially the Portuguese Constitution, it is necessary to review the most relevant aspects regarding the Services, without forgetting the control and supervision, the guiding principles of intelligence activity, the differences between intelligence police and strategic intelligence and the legal systems of similar information services in view of the protection of the fundamental rights convention.

Key words: communication interference, metadata, intelligence, intelligence services, generation of information and crime prevention.

Índice

SIGLAS E ABREVIATURAS

ABIN	Agência Brasileira de Inteligência
Ac.	Acórdão
AJ	Autoridade Judiciária
AMN	Autoridade Marítima Nacional
Art.,arts	Artigo, artigos
BND	*Bundesnachrichtendienst* (Serviço de Inteligência Federal Alemão)
CDFUE	Carta dos Direitos Fundamentais da União Europeia
CE	Comunidade Europeia
CEDH	Convenção para a Proteção dos Direitos Humanos
CEDHLF	Convenção Europeia dos Direitos Humanos e Liberdades Fundamentais
CF-SIRP	Conselho de Fiscalização do SIRP
CIA	*Central Intelligence Agency* (USA)
Cf.	Confira, Conforme
Consult.	Consultado
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
CSM	Conselho Superior da Magistratura
CSNU	Conselho de Segurança das Nações Unidas
DL	Decreto Lei
DNI	*Digital Network Intelligence* (Inteligência de rede digital)
EM	Estado Membro
EMGFA	Estado Maior General das Forças Armadas
EMP	Estatuto do Ministério Público
ENINT	Estratégia Nacional de Inteligência (Brasileira)
EU INTCEN	Centro de Análise de Inteligência da União Europeia
FA	Forças Armadas
FRA	Agência da União Europeia dos Direitos Fundamentais

GPS	*Global Positioning System* (Sistema de Posicionamento Global)
HUMINT	*Human Intelligence* (fontes humanas)
IA	Inteligência Artificial
IMINT	*Imagery Intelligence* (fontes de inteligência através de imagens fotográficas)
LAI	Lei de Acesso à Infromação (Brasileira)
LCCCEF	Lei de Combate à Corrupção e Criminalidade Económica e Financeira
LCT	Lei de Combate ao Terrorismo
LOIC	Lei de Organização da Investigação Criminal
LOSIRP	Lei Orgânica dos Serviços de Informações da República Portuguesa
LQPC	Lei Quadro da Politica Criminal
LQSIRP	Lei Quadro dos Serviços de Informações da República Portuguesa
LSI	Lei de Segurança Interna
MP	Ministério Público
n.º, n.ºs	número, números
NSA	*National Security Agency* (USA)
OPC	Órgãos de Polícia Criminal
Org.	Organização
OSINT	*Open Sources Intelligence* (fontes abertas)
OSS	*Office of Strategic Services*
PE	Parlamento Europeu
PIDCP	Pacto Internacional sobre os Direitos Civis e Políticos
PGR	Procuradoria Geral da República
PNI	Politica Nacional de Inteligência (Brasileira)
p. , pp.	página, páginas
Proc.	Processo
PSP	Polícia de Segurança Pública
RASI	Relatório Anual de Segurança Interna

RCD	Regulamento do Centro de Dados (do SIRP – engloba o SIS e SIED)
RCM	Resolução do Conselho de Ministros
RGPD	Regulamento Geral de Proteção de Dados
SGSIRP	Secretário-Geral do Serviço de Informações da República Portuguesa
SIRP	Serviços de Informações da República Portuguesa
SIED	Serviços de Informações Estratégicas de Defesa
SIM	Serviço de Informações Militares
SIS	Serviço de Informações de Segurança
SNI	Serviço Nacional de Informações (Brasileiro)
SISBIN	Sistema Brasileiro de Informações
TC	Tribunal Constitucional
UE/EU	União Europeia/ *European Union*
USA	*United States of America* (Estados Unidos da América)

INTRODUÇÃO

"A razão por que um soberano esclarecido e um general sensato vencem o inimigo sempre que se movem, e os seus feitos ultrapassam os dos homens vulgares, é a presciência. A chamada "presciência" ou "previsão" não pode ser deduzida dos espíritos nem dos deuses, nem por analogia com os conhecimentos passados, nem por cálculos. Ela deve ser obtida por homens que conhecem a situação do "inimigo"[1].

"E, portanto, somente um soberano iluminado e um general valoroso é que são capazes de empregar as pessoas mais inteligentes como agentes e estarem certos de alcançarem grandes resultados"[2].

Os ensaios de *Sun Tzu* sobre «A Arte da Guerra» constituem os primeiros "tratados" conhecidos sobre o assunto, defendendo alguns autores que nunca foram ultrapassados em termos de alcance e profundidade de conhecimento, considerando a essência concentrada da sabedoria da conduta da guerra. São diversas, as áreas do conhecimento, que tomam como referência esta obra milenar. Desde as relações internacionais à história, das ciências militares à gestão de empresas, da simples gestão de equipas às mais complexas teorias de emprego de "forças". De facto, considerava-se mesmo que a guerra representava sempre uma perda, destacando-se permanentemente o vital conhecimento das intenções do inimigo, assim como as suas capacidades.

Não obstante deste prelúdio, importa realçar que esta investigação circunscrever-se-á na análise jurídica, sobre o direito de acesso aos metadados pelos serviços de informações portugueses, e, no contributo imprescindível destes na prevenção criminal.

Apesar de não ser nosso intuito fazer esta abordagem, nesta perspetiva não deixa de estar diretamente relacionado com o tema proposto contribuindo apenas como breve introdução e relação de interdisciplinaridade face ao objeto que pretendemos explorar. Portanto, a fim de evitar uma dispersão do objeto de investigação, faremos de seguida a abordagem pertinente relativo ao tema na ótica jurídica.

Esta compreensão desde cedo fomentou a mais ampla troca de impressões sobre o "papel" dos serviços de informações nas sociedades democráticas aquando da prossecução de uma vantagem estratégica. A sociedade num Estado de Direito Democrático sob os alicerces dos

[1] *Sun Tzu*, «A Arte da Guerra», *Evergreen, Taschen GmbH Hohenzollerning* 53, D-50672 Köln, 2007, Cap XIII, 3 e 4, p.232

[2] General Pedro Cardoso – As Informações em Portugal. Gradiva – Publicações, Lda/Instituto da Defesa Nacional, Março 2004, p.15, *apud*, *Sun Tzu*, «A Arte da Guerra», Editorial Futura, Lisboa, Junho 1974, Cap.XIII, 23, p.301

princípios da transparência e da liberdade jamais poderá dar-se ao luxo de prescindir de serviços de inteligência, pois "estes contribuem indiretamente para o bem-estar dos cidadãos, fazendo chegar aos decisores políticos, estudos e análises prospetivas de curto, médio e longo prazo que ajudam os governos a programar e a planear ajustamentos em relação às previsões, quer no âmbito interno, quer no âmbito externo[3]".

É neste sentido que reconhecemos a necessidade de enquadrar os serviços de informações como garante do Estado Democrático, da independência nacional e manutenção da segurança interna e externa, agindo no respeito pela Constituição e pela lei.

Como refere Joanisval Gonçalves, "o grande dilema sobre o papel da inteligência em regimes democráticos é o de conciliar a tensão entre a necessidade premente do segredo (sigilo) na atividade de inteligência e a transparência das atividades estatais, essencial em uma democracia". Associada a esta questão, outra preocupação surge, particularmente nas sociedades democráticas que viveram, em passado recente, períodos autoritários: como garantir que os órgãos de inteligência desenvolvam as suas atividades de maneira consentânea com os princípios democráticos, evitando abusos e arbitrariedades contra essa ordem democrática e contra os direitos e garantias fundamentais dos cidadãos? A maneira com que determinada sociedade lida com o dilema transparência versus sigilo, em termos de procedimentos e atribuições dos serviços de inteligência, é um indicador do grau de desenvolvimento da democracia nessa sociedade. Em países com modelos democráticos consolidados, como EUA, Reino Unido (…), a dicotomia é resolvida por meio de mecanismos eficientes e efetivos de fiscalização e controle interno e, especialmente, de controlo externo, exercido pelo Poder Legislativo[4].

Neste segmento que acima se transcreveu, revela-se o prelúdio de uma mudança de paradigma na forma como o público (em geral) deverá "olhar" para os serviços de informações, as ameaças descentralizadas e de caráter difuso, a disrupção tecnológica, a dependência cada vez maior das novas tecnologias e o que a nova realidade incrementou (em particular da IA, da Robótica e dos Drones) "bem como a expansão da liberdade de movimentos através das fronteiras (sem controlo na travessia) reivindica a antecipação, por parte dos Estados, do

[3] *Op.cit.* Pedro Simões, "Os serviços secretos em Portugal: os serviços de informação e a comunicação social", 2002, p.39, *apud* Pedro Cardoso – A visão das Informações (…) até ao SIRP.
[4] *Op.cit.* Joanisval Brito Gonçalves, Políticos e Espiões. O Controle da Atividade de Inteligência. 2ª Ed. 2019, p.11 e 12.

patamar que reputam de necessário para a mobilização do seu poder punitivo, que, em determinadas matérias, fazem retroagir ao estádio da investigação preventiva[5]".

No primeiro capítulo pretendemos então realizar um breve contexto da evolução histórica das Informações desde a extinção do regime totalitário até as últimas alterações que se registaram no âmbito da Lei-Quadro do SIRP e demais diplomas legais relacionadas com a atividade de informações, bem como reforçar a imprescindibilidade de tão importante corpo de Estado.

Atentos à norma Constitucional que restringe o acesso nas comunicações, será analisado a norma relacionada com a ingerência nas comunicações, presumindo-se uma preocupação com as restrições que resultam da lei fundamental e que paralelamente faremos acompanhar à luz da análise de dois acórdãos do Tribunal Constitucional.

Não menos importante serão enunciados os princípios fundamentais e penais (relevantes), por forma a contextualizar as objeções impostas pelos Doutos Acórdãos do Tribunal Constitucional. Não obstante da controvérsia que este tema tem gerado em trabalhos científicos no mundo académico, e que alguns autores têm sucessivamente suscitado divergências, á contrário das decisões proferidas nos referidos acórdãos, faremos uma breve alusão à (in)viabilidade de uma revisão constitucional sustentada nas circunstâncias e impedimentos legais.

A análise do tema leva-nos ainda a uma reflexão de cariz político-criminal, nomeadamente na relevância das políticas criminais adotadas face as prioridades e orientações definidas pelo (s) governo (s), tendo em conta a dignidade dos bens jurídicos tutelados e se de facto existe uma verdadeira e real ameaça. Qual ou quais as prioridades de políticas criminais devemos ter em consideração em pleno século XXI perante as novas ameaças nesta "Era digital"?

No segundo capítulo abordaremos alguns conceitos básicos sobre os metadados, que aparentemente ainda suscitam alguma controvérsia.

Sobre o Projeto de Lei n.º 480/XIII/2ª – acesso aos dados de tráfego, de localização ou outros dados conexos de comunicações – e sobre a proposta de Lei n.º 79/XII – acesso a dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas pelo SIRP – com vista a estabelecer competência e o procedimento de acesso por funcionários e agentes dos serviços de informações da República Portuguesa, faremos uma análise na perspetiva da fiscalização e controlo judicial para cumprimento das atribuições legais daqueles serviços. Aqui daremos particular ênfase aos projetos propostos até à data, uma vez que se carecia de ausência

[5] Mariana Machado, O acesso aos metadados pelo SIRP à Luz da Lei e da Constituição, Almedina, 2019, *op.cit.*, p.21

de iniciativas legislativas no segmento normativo relativo ao acesso aos metadados fundamentando-se a premência de dotar o SIRP e de reforçá-lo com instrumentos legais. Assim, por forma, a assegurar a cooperação com os seus congéneres e demais organismos nacionais no combate ao terrorismo e sua proliferação, espionagem e criminalidade altamente organizada de natureza transnacional.

Ainda neste capítulo daremos uma perspetiva diferenciada da «inteligência policial» (investigação criminal), e da «inteligência estratégica» (*intelligence*), no sentido de frisar a importância de um serviço de inteligência que sem o acesso às comunicações, ver-se á diminuída na sua capacidade operacional, se não mesmo incapacitado de prosseguir as atribuições a que está incumbido. Daqui decorre talvez um dos grandes problemas na operacionalidade dos serviços que, como referem alguns autores, "sem acesso aos metadados os serviços ficariam reduzidos a um gabinete de estudo[6]", permitindo brechas no sistema de segurança interna.

No último capítulo á luz da Convenção dos direitos fundamentais faremos uma alusão do acesso aos metadados pelos serviços congéneres, permitindo desta forma uma comparação com os seus sistemas jurídicos.

Após uma leitura exaustiva, quer doutrinária, quer obras «não jurídicas» e jurisprudência relacionadas com o tema proposto, foi nos suscitado ao longo desta investigação várias questões que faremos os possíveis para responder de forma sucinta e objetiva, aproveitando esta interdisciplinaridade para enriquecer (mas não esvaziando) a abordagem jurídica.

Estando atentos à economia de espaço e objetividade do tema, não nos foi alheio o facto de notarmos frequentemente alguma dispersão, contudo tentámos manter a "bussola" orientada no caminho que julgamos ser o mais coerente e assertivo academicamente. Neste sentido deparámo-nos com as seguintes questões: i) Que instrumentos e organismos o Estado tem à disposição na investigação à "nova criminalidade"? ii) Que alternativas existem a esta "nova criminalidade" sem recorrermos ao acesso aos metadados?; iii) Justifica-se o acesso aos metadados por parte dos serviços de informações, ou seja, a montante de uma investigação criminal, o contributo necessário a esta "nova criminalidade"?; iv) Que tipo de crimes se justificaria tal ingerência? v) Que funções estão incumbidas aos nossos serviços de informações? vi) Que papel podia desempenhar o "dito" quarto poder (dos jornalistas) face à operabilidade dos serviços de informações? e; vii) À luz do princípio da cooperação

[6] *Op.cit*. Pedo Simões, "Os serviços secretos em Portugal: os serviços de informação e a comunicação social", 2002, pp.57 e 81. *apud* Daniel Sanches.

internacional (na UE) que instrumentos temos atualmente em vigor (oficiais/informais)? viii) Quais os sistemas jurídicos dos serviços de inteligência congéneres?

Questões que através de uma análise sistemática, face ao sistema jurídico atual tender-se-á procurar alternativas com base nos conceitos jurídico-penais, abandonando uma posição intrasistémica e se pondere uma nova posição jurídico-dogmática que permita não só ultrapassar as questões suscitadas nos recentes acórdãos como adotar uma postura proactiva em vez de reativa perante as novas ameaças e face à evolução dos instrumentos que a nova criminalidade recorre.

CAPÍTULO I – PRINCÍPIOS FUNDAMENTAIS E LIMITES CONSTITUCIONAIS. A (IN) VIABILIDADE DE UMA REVISÃO CONSTITUCIONAL. E AS PRIORIDADES POLITICO CRIMINAIS.

1. Enquadramento histórico e constitucional face à evolução dos serviços de informações

Durante o período compreendido entre 1926 e 1974, prevaleceu em Portugal um regime de cariz autoritário marcado por uma forte inspiração nacionalista, o período do Estado-Novo. Com características repressoras e limitadoras de direitos e liberdades dos cidadãos. A PVDE (1933)[7], PIDE (1945)[8] e mesmo a DGS (1969)[9] conotadas como "polícias políticas", ou como serviços de informações, eram vistos como uma expressão de autoridade do Estado.

Em mais de 40 anos de Estado de Direito Democrático, Portugal registou um avanço significativo nas suas estruturas políticas, económicas, sociais e culturais. Não menos relevante, o caminho seguido para a criação legislativa e institucional da atividade de informações do Estado, foi-se desenvolvendo com dificuldades, incompreensões, recuos e avanços, muitas das vezes suscitando dúvidas sobre o modelo institucional a seguir[10].

Pedro Cardoso expressa de uma forma clara e evidente a necessidade de um Governo manter-se informado: "Onde o governante tem de ser hábil, dominante e objetivo é nas análises, previsões e estudos prospetivos, para reduzir ao mínimo a surpresa e a impreparação do aparelho do estado para fazer face aos acontecimentos"[11].

Este autor refere ainda que para tanto, os homens de Estado sentiram a necessidade de dispor de serviços de informações[12] com estruturas próprias, missões definidas e enquadramento no

---

[7] Cf. Pedro Cardoso, As informações em Portugal, p.96.
[8] Cf. *Idem*. p.110.
[9] *Idem*. p.138.
[10] Cf. Bacelar Gouveia, Direito da Segurança. Cidadania, Soberania e Cosmopolitismo, pp.685 e ss
[11] Cf. Pedro Cardoso, As informações em Portugal, p.146.
[12] Cf. Joanisval Brito Gonçalves, Atividade de inteligência e legislação correlata, p. 6ª ed. Impetus, 2018 – a diferença entre "informações" e "inteligência" prende-se essencialmente com o âmbito de aplicação. A terminologia "informações", mais adequada em Portugal utilizada e associada mais no âmbito militar; FERREIRA, Arménio Marques - in Estudos de Direito e Segurança (coordenação de Jorge Bacelar Gouveia e Rui Pereira), p.74 a 76. No decurso das várias alterações das estruturas orgânicas do sistema de informações em Portugal, e dos desígnios que adotaram nas diversas ditaduras, e que degradaram o "Instituto" com a perversão policial desde a criação da Polícia de Defesa Política e Social e da Polícia de Vigilância e Defesa do Estado, à Polícia Internacional de Defesa do Estado e a sua transformação em Direção-Geral de Segurança, apesar das vicissitudes e a sua reestruturação, que o Decreto Lei nº 226/85 efetivamente operou, veio definir como seu objeto as informações de natureza estratégico-militar, organizacional, tática e logística, com interesse para a segurança e atuação das Forças Armadas. Por "inteligência" Joanisval Brito comenta a diferença, através de Olivier Forcade e Sébastien Laurent, assinalando o caráter elaborado desta. Explica o ciclo de inteligência, no qual há a reunião da inteligência bruta (raw intelligence), que é enriquecida por um estudo, e que posteriormente é produzindo um documento de inteligência- recorrendo a técnicas de dados negados - para os tomadores de decisão. Em conclusão o termo

aparelho de Estado. Acima de tudo urgia inevitavelmente uma regulamentação própria, enquadrada no segmento constitucional e salvaguardando os princípios estruturantes de um Estado de Direito.

Só a partir da década de 80 é que se revelou uma vontade política da criação de um serviço de informações - primeiro o SIS e mais tarde a criação do SIED). Como elucida Bacelar Gouveia, o caminho sinuoso e a evolução daqueles Serviços poder-se-á distinguir em vários períodos: "o 1º período (1974-1984): ocupado pela 2ª Divisão do EMGFA[13]; um 2º período (1984-1995): na criação do SIRP[14] (apoiado em três organismos, apesar de estarem a funcionar efetivamente apenas dois (o SIS e o SIM); 3º período (1995-2004: estabilizando apenas através de um serviço "interno" e de natureza "externa" no domínio das informações militares; 4º período (2004-2007): distinguiu-se pela criação do cargo do SGSIRP e note-se a aproximação dos dois serviços de informações (o SIS e o SIED); e um 5º período (2007- …): com a criação de infraestruturas administrativas comuns e a aprovação da Lei n.º 9/2007, 19 de fevereiro"[15].

A questão colocada por Mariana Machado[16] destaca-se de modo bastante elucidativo não obstante controvertido pelo juízo constitucional na ordem jurídica nacional[17]. Designadamente confronta duas abordagens, por um lado, o arquétipo do SIRP – os seus antecedentes, a sua evolução histórica, o seu escopo, atribuições e competências, a natureza jurídica dos serviços de informações – face ao exercício do *ius puniendi* e *ius imperium*, encetado através de um processo penal e conformado com as autoridades judiciárias[18]. Por outro lado e numa abordagem jusfundamental, traz à colação diplomas legislativos - como a LOIC e a Lei de

"informações" utilizado em Portugal poder-se-á dizer que tem o mesmo sentido e equivalência de acordo com o termo utilizado por outros países "inteligência".

[13] Cf. Pedro Cardoso, As informações em Portugal, *op.cit.*, pp.141 – 143. «reforçada com pessoal dos três ramos (Marinha, Exército e Força Aérea) e com pessoal civil de outros ministérios, acionou o serviço de informações nacional na dependência direta do CEMGFA e do qual foi dirigida pelo próprio autor.

[14] Tendo este diploma entrado em vigor pela Lei n.º 30/84, de 5 de setembro sujeito a várias alterações ao longo dos anos

[15] Cf. Bacelar Gouveia, Direito da Segurança. Cidadania, Soberania e Cosmopolitismo, *op.cit.*, p.688.

[16] Cf. Mariana Machado, O acesso aos metadados pelo SIRP à Luz da Lei e da Constituição, *op.cit.*, p.20 a p.22. No segmento dos desenvolvimentos conceptuais de segurança transnacional e de redes intergovernamentais por meio de cooperação transnacional iniciada pelos governos e a comunidade dos serviços de inteligência e as autoridades policiais, gizou projetar uma proposta: ´´é constitucionalmente admissível o acesso aos (…) metadados (isto é, dados dos dados) por parte dos oficiais do SIRP, no âmbito da sua atividade de produção de informações, para efeitos de prevenção e combate ao terrorismo? Ou (…) apenas por via de uma revisão constitucional pode tal acesso ser objeto de um juízo de conformidade constitucional?

[17] No Ac. n.º 464/2019, do TC, resultou um pedido de apreciação e declaração da inconstitucionalidade das normas constantes dos artigos 3.º e 4.º da Lei Orgânica n.º4/2017, de 25 de Agosto, que aprovou e regula o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais do SIS e do SIED, procedendo á segunda alteração á Lei n.º 62/2013, de 26 de Agosto (Lei da Organização do Sistema Judiciário).

[18] Cf. Mariana Machado, O acesso aos metadados pelo SIRP à Luz da Lei e da Constituição, *op.cit.*, p.22.

Combate à Corrupção e Criminalidade Económica e Financeira[19] - na circunstância de (re)emergir conceitos como a investigação preventiva[20] ou como alguns autores descrevem, "investigações pró-ativas"[21].

Recorde-se que o SIRP (doravante designado também por Serviços) de acordo com a génese de um organismo de inteligência[22] a sua intervenção situa-se tendencialmente numa fase precedente à notícia de um crime[23]. De acordo com o n.º 2 do artigo 2.º da LQSIRP, "incube aos serviços assegurar, no respeito da Constituição e da lei, a produção de informações necessárias à preservação da segurança interna e externa, bem como à independência e interesses nacionais e à unidade e integridade do Estado". Em concatenação com o disposto do n.º1 do artigo 219.º da CRP, "ao ministério público compete representar o Estado e defender os interesses que a lei determinar, bem como (…), participar na execução de política criminal (…) exercer a ação penal orientada pelo princípio da legalidade e defender a legalidade democrática", em conformidade com o primado processual do MP que decorre do artigo 48.º do CPP em conjugação com a tarefa de investigação e repressão penal.

"As operações dos serviços devem manter-se secretas, mas os princípios que norteiam a direção e controlo desses serviços devem ser cuidadosamente considerados, discutidos e compreendidos por aqueles que a nível governamental são responsáveis pelo controlo dos

[19] Podíamos fazer uma reflexão exaustiva, ainda que não seja objeto de investigação e análise deste estudo, a abordagem unitária que foi inicialmente transposta para o direito português através da Lei n.º 25/2008 de 5 de junho (alterada pela Lei n.º 83/2017 de 18 de agosto que procedeu a revogação e atualização) que previa um regime preventivo de combate ao branqueamento de capitais e ao financiamento do terrorismo; António Manuel Abrantes descreve no seu artigo – Anatomia de um crime: O financiamento do terrorismo no ordenamento jurídico-penal português. Revista Anatomia do Crime (2017) pp.95-125 - que o diploma em conformidade com o regime previsto no direito europeu, centra-se na previsão de vários deveres nomeadamente; o de controlo, de identificação e diligência, de comunicação, de abstenção, de recusa, de conservação, de exame, de colaboração, de não-divulgação e de formação a cargo das entidades financeiras e certas entidades não-financeiras, cujo cumprimento tem como finalidade a deteção e a prevenção de possíveis situações de branqueamento de capitais e de financiamento do terrorismo.

[20] Cf. Mariana Machado, O acesso aos metadados pelo SIRP à Luz da Lei e da Constituição, *op.cit*., p.22.

[21] Cf. Augusto Dias e Rui Pereira, Sobre a validade de procedimentos administrativos prévios ao inquérito e de fases administrativas preliminares no processo penal, p.41. Os autores esclarecem a tendência atual de confusão entre prevenção criminal, investigação criminal e repressão criminal. Reiterando a proibição no sistema penal vigente de pré-inquéritos, inquéritos preliminares, investigações policiais, investigações pró-ativas ou afins, não obstante, esta conclusão não ser afastada pela circunstância de no passado existir e ainda se consagrar alguns processos de averiguações, de averiguações preliminares ou de atividade de recolha de informações de segurança.

[22] Cf. Mariana Machado, *op.cit.,* p.60. Quando comparamos com serviços congéneres e com os respetivos diplomas legais que regulamentam a atividade daqueles, encontramos implícito a "marginalidade" com que atuam face a um processo penal. Veja-se por exemplo no regime atual do Reino Unido, «A RIPA – *Regulation of Investigatory Powers Act* - é a lei que define os poderes cometidos aos serviços, especificamente ao MI5 (BBS British Security Service) ao MI6 (SIS *Secret Intelligence Service*) e o serviço militar (*Difence Intelligence* – que contempla interceções telefónicas, denominadas, *bulk interception* (interceção em massa, sem alvo concreto, para antecipar e investigar planos terroristas e ataques à cibersegurança, suscetíveis de colocar em perigo a segurança nacional). Não obstante de em 2016 ter sido introduzido a exigência de confirmação judicial das decisões emanadas pelo órgão executivo. Disponível no site de internet [em linha: https://www.legislation.gov.uk/ukpga/2000/23/contents]

[23] *Idem*, p.54.

serviços"[24]. O indispensável controlo dos Serviços é levado a cabo pelos próprios órgãos de soberania, contudo não se esgota apenas através das diretivas, da promulgação de legislação corretiva ou preventiva no decurso das atividades abertas ou encobertas, imputáveis a alguém.

Apesar de todas as medidas constitucionais, legais e regulamentares de controlo, é sabido "que o controlo mais eficaz é a existência de órgãos de comunicação social que prossigam verdadeira e inteiramente livres e esclarecidos para criticar a atuação daqueles serviços e dos seus elementos, mantendo assim uma potencial capacidade e desafio permanente que contribui grandemente para condução das atividades dos serviços dentro da legalidade e do respeito pelos direitos fundamentais"[25].

Questiona-se não raras vezes: "Mas para que é que temos afinal Serviços de Informações?" Muitos países talvez passariam muito melhor sem eles, mas temos de aceitar que fazem parte da vida moderna nacional e internacional, num mundo que há muito deixou de ser regido por "negociações entre cavalheiros", mas por conjuras, cabalas, conspirações, assassinatos, golpes de estado e violências de todos os tipos[26].

Os Serviços (SIS e SIED) no exercício das suas missões e competências, prosseguem as atividades de produção de informações atinentes à manutenção das condições de respeito pela legalidade e pelos princípios do Estado de Direito Democrático. No estrito cumprimento da Constituição e da Lei e em regime de exclusividade, asseguram a produção de informações necessárias à salvaguarda dos interesses nacionais, da independência nacional e da segurança interna.

A evolução legal e constitucional, no pós 25 de Abril, revelou-se lenta e marcada pela "indiferença constitucional ou até de proibição constitucional[27]. Contudo, não foi desprezada de todo, evidenciando orientações em relação aos serviços de informações na revisão constitucional de 1989, introduzindo nas competências de reserva relativa da Lei da Assembleia

[24] Cf. Pedro Cardoso, As informações em Portugal, op.cit., p.155. Numa conferência, cujo o tema central foi o citado e que teve por título «The Relationship Between Secret Services and Governments in Modern States» no ambiente do Royal United Services Institute for Defense Studies (cuja sigla se designa – RUSI)

[25] *Idem*, p.155.

[26] *Ibidem. Apud*. Sir John B. Lockhart em determinada passagem da sua conferência que teve como título «The Relationship Between Secret Services and Governements in Modern States», realizada em 21 de Novembro de 1973 e publicada no «Journal of the RUSI», Junho de 2974, Vol 119, n.º2. Publicada em Português com a introdução do Almirante Silva Horta, nos «Anais do Club Militar Naval», n.ºs 1 a 3, janeiro-Março de 1976, pp.21 a 31.

[27]Cf. Bacelar Gouveia, Direito da Segurança. Cidadania, Soberania e Cosmopolitismo, 1ª ed., Almedina, 2018, cit. p.683

da República, a definição do regime dos serviços de informações e subsequentemente na revisão constitucional de 1997 transferiu a matéria para a reserva, de competência absoluta, da AR[28].

O consenso de alguns autores, na reflexão do estatuto constitucional dos serviços de informações revelou-se *tardio*, bem como *minimalista*. *Tardio* porque ainda se vivia na sombra de um regime de polícia de estado (PVDE, PIDE e DGS) e com a lembrança sempre presente de um Estado capaz de violar as mais diversas dimensões dos direitos fundamentais. Está em todos, ainda muito presente, casos em que os "polícias de estado" cometiam as maiores das atrocidades, hoje censuradas – mantinham por seis meses presos preventivamente quaisquer cidadãos recorrendo a técnicas desumanas de interrogatório. Observava-se o uso sistematizado da tortura e chantagem como principal método de atuação policial, bem como espancamentos, tortura do sono, isolamento e ameaças – que julgamos não preconizar a ideologia que ergue o princípio do governo limitado, indispensável à garantia dos direitos em dimensão estruturante da organização político-social de uma comunidade[29]. *Minimalista* talvez porque apesar dos esforços empreendidos no sentido de regular e dar uma forma mais robusta ao seu regime jurídico, o que se verifica num plano material, como nos esclarece Bacelar Gouveia, são várias as opções que o texto constitucional não versa sobre determinadas matérias optando por um "silêncio", de um entendimento negativo a respeito da sua possibilidade, como por exemplo: na arquitetura estrutural do SIRP. Os poderes que dispõem os serviços de informações, designadamente na sua relação como os direitos fundamentais dos cidadãos, as atribuições dos serviços, nas tarefas que se colocam aos organismos da Segurança Nacional e como devem correlacionar-se. Na salvaguarda dos interesses nacionais, prevenindo ameaças internas e externas (contrainteligência), com o intuito de prosseguir verdadeiramente as finalidades de um serviço de inteligência, protegendo os valores essenciais do poder público estadual, sejam estes de interesse estratégico, político, económico, social, ou cultural[30].

Concordamos com José Fontes[31] e António Abrantes[32] quando reforçam a ideia de necessidade de uma maior «intervenção» constitucional, propondo uma revisão da Lei

---

[28] *Ibidem.* Ver também, Mariana Gomes Machado, O acesso aos metadados pelos serviçõe de informações da Republica Portuguesa á luz da Lei e da Constituição, Almedina, 2019, cit. p.30 e 31. p.31, *apud* José Fontes, A constituição e os serviços de informações, in Segurança e Defesa, n.º15, Outubro-Dezembro de 2010, p.48

[29] Cf. José J. Gomes Canotilho – Direito Constitucional e Teoria da Constituição. 7ª ed. 17ª (reimp). Coimbra, *op.cit*., p.51.

[30] Cf. Bacelar Gouveia, Direito da Segurança – Cidadania, Soberania e Cosmopolitismo, Ed. Almedina, p.685; Mariana Gomes Machado, O acesso aos metadados pelo SIRP à Luz da Lei e da Constituição, p. 31.

[31] Cf. José Fontes, A Constituição e os Serviços de Informações "Segurança e Defesa" [Em linha]. Nº 15 (Out.-Dez. 2010), p. 1-7. [Consult. 25 Jan.2021]. Repositório aberto. Universidade Aberta. Disponível em https://repositorioaberto.uab.pt/handle/10400.2/1788.

[32] Cf. António Abrantes, Academia Edu [em linha]. Revista do Ministério Público 156 (Out. – Dez. 2018). P. 157-208- [25 Jan. 2021]. O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à

Fundamental. Não afastando as eventuais preocupações no que diz respeito aos direitos, liberdades e garantias constitucionalmente tutelados, a necessidade de um reforço, visível e eficaz num sistema de fiscalização de amplas garantias constitucionais que assegurem o cumprimento da CRP e da Lei.

A propósito da fiscalização, não menos relevante, contemplado no Decreto n.º 426/XII no seu artigo 35.º, a previsão de uma Comissão de Controlo Prévio composta por três magistrados judiciais, designados pelo Conselho Superior da Magistratura, de entre Juízes conselheiros do STJ, o Tribunal Constitucional pronunciou-se no Ac.464/2019 no sentido de "suscitar" uma certa "desconfiança" deste órgão jurisdicional (apesar de constituída por magistrados de um tribunal judicial superior, revelam-se como uma autoridade administrativa independente)[33]. Não obstante esta última observação, a qual se reserva um espaço de aprofundamento mais adiante.

Não pode o Estado prescindir tão importante corpo de Estado e não integrar no seu normativo constitucional uma referência menos discreta, objetiva e reconhecida.

Nas palavras de alguns autores, a ideia da Constituição funda-se na prossecução de vários desideratos, nomeadamente: ordenar e limitar o poder político, por um lado e, garantir os direitos e liberdades do indivíduo por outro[34].

A função dos serviços de informações é vital no Estado de Direito Democrático - destina-se a municiar os decisores políticos de informação elaborada, de conhecimento que permite reduzir o nível de incerteza, "*Free societies as well as closed ones need to have secret services; otherwise the closed ones will take them over*"[35]. Joanisval Gonçalves alude impreterivelmente na necessidade da atividade de inteligência ser imprescindível em qualquer democracia, não fazendo sentido falar-se em poder sem inteligência, "conhecimento é poder, e sem conhecimento os homens, organizações ou mesmo Estados tornam-se não mais que uma folha lançada ao vento, sem qualquer controle sobre o seu destino"[36]. Articulado a esta imprescindibilidade da atividade de inteligência não podemos menosprezar a grande discussão

inviolabilidade das comunicações. Disponível em https://arquitectura-ucp.academia.edu/Ant%C3%B3nioManuelAbrantes.

[33] Conforme mencionado no referido acórdão (Ac.464/2019, TC, p.16), o TJUE pronunciou-se igualmente sobre a matéria do acesso a dados pessoais, no Acórdão Tele2, entre outras questões, que o artigo 15º, nº1, da Diretiva 2002/58, lido á luz dos artigos 7.º, 8.º e 11.º, bem como do artigo 52.º, n.º1, da CDFUE, deve ser interpretado no sentido de que uma regulamentação nacional que incida sobre o acesso das autoridades nacionais competentes aos dados conservados, deve obedecer aos seguintes requisitos (…); o referido acesso deve estar submetido a um controlo prévio por parte de um órgão jurisdicional ou de uma autoridade administrativa independente (…)

[34] Cf. Mariana Machado, O acesso aos metadados pelo SIRP à Luz da Lei e da Constituição, *op.cit.*, p.101.

[35] Cf. Joanisval Gonçalves, Atividade de inteligência e legislação correlata, *op.cit.*, p.135 «The Economist, 15/03/1980» e p.135.

[36] *Ibidem.*

relacionada com a atividade de inteligência em regimes democráticos, como é o caso de Portugal.

Teme-se o risco e o desvirtuar dos fins a que se destina um serviço de inteligência, como é o caso do uso da inteligência para propósitos político-partidários e ainda, o excesso de poder dos órgãos de inteligência por lidarem com informações sigilosas[37].

Diante desta dicotomia "*necessidade*" versus "*risco*" da atividade de inteligência para a democracia, tem-se no controle público destes, grande relevância. É pois, através do controlo eficiente e eficaz que garantirá que os serviços operem dentro de princípios democráticos e realizem uma atividade verdadeiramente em benefício do Estado e da Sociedade[38].

Os serviços de inteligência num Estado de Direito Democrático inscrevem-se fundamentalmente nos limites da instrumentação jurídica propriamente dita e oferecem-se, neutros à tutela do poder estabelecido, tendo em consideração a visão de que as informações, ao darem significado, emancipam da conjuntura e, ao criarem conhecimento com exclusão de terceiros, conferem poder. Poder esse como referimos anteriormente, poderá ser utilizado com propósitos político-partidários pelos Governos, descredibilizando a atividade dos órgãos de inteligência, tornando-os vulneráveis e fragilizados. Sendo este um retrocesso ao paradigma de um organismo de vital importância vinculado ao arbítrio político vigente.

Será suficiente uma mera positivação de uma norma constitucional a fim de conferir ao indivíduo um direito fundamental, tornando-o uma realidade jurídica efetiva?

Esta questão foi colocada por alguns autores nomeadamente Mariana Machado, e que nas palavras de Bacelar Gouveia se torna clarividente e por nós acompanhada, descrevendo que os direitos fundamentais representam a atribuição às pessoas de uma posição subjetiva de vantagem, positivadas na constituição, exercidas por contraposição ao Estado-Poder[39]. Como afirma a autora: "há direitos fundamentais que, em especial, quando considerados como um todo tutelam diferentes bens jurídicos e, inversamente, bens jurídicos cuja proteção se encontra repartida por mais de um direito, se não mesmo disseminada por categorias mais ou menos dilatadas de direitos fundamentais"[40].

[37] Cf. Bacelar Gouveia, in Direito da Segurança – Cidadania, Soberania e Cosmopolitismo, p.698.
[38] Cf. Joanisval Gonçalves, Atividade de inteligência e legislação correlata, *Op.cit.*, p.136. O autor refere por último sem reservas que, «não se deve de temer os serviços "secretos". Conhecendo-os, é possível controlá-los e orientar essa atividade tão preciosa e tão mítica a serviço da sociedade, do Estado e da Democracia»
[39] Cf. Mariana Machado, O acesso aos metadados pelo SIRP à Luz da Lei e da Constituição, *op.cit.*, p.102.
[40] Cf. Mariana Machado, *op.cit.*, p.103, *apud* Jorge Pereira da Silva, in Direitos Fundamentais – Teoria Geral, p.171.

2. Interpretação e alcance do n.º 4 do artigo 34.º da CRP, na legitimação de acesso aos metadados.

Vejamos agora o alcance e interpretação do n.º 4 do artigo 34.º da Constituição[41].

Com o desenvolvimento e gestão de programas de vigilância das comunicações que abrangem indiscriminadamente os cidadãos, quer em contexto de guerra quer de paz, estes são desenvolvidos sob o argumento de garantir a segurança dos Estados e em particular combater o terrorismo. Programas esses que violam diretamente diplomas legais nacionais, regionais e internacionais, que consagram o respeito pela privacidade e a proteção de dados pessoais[42], nomeadamente os artigos 26.º, 34.º e 35.º da CRP, os artigos 7.º, 8.º e 11.º da CFDUE e o artigo 12.º da DUDH. Entendemos que estes direitos podem ser restringidos, de acordo com o princípio da proporcionalidade (*latu sensu*) e seus corolários da necessidade, adequação e proporcionalidade (*strito sensu*) para o respeito de interesses públicos relevantes e relacionados inclusive com a defesa e segurança do Estado. Contudo, essa restrição revela-se desproporcionada, "destruindo o próprio estado de Direito a abrir mão dos valores que muitas vezes esse terrorismo pretende desfazer"[43], abrangendo todas as pessoas, independentemente de estas constituírem ou não uma verdadeira ameaça, considerando ainda que a interceção das comunicações é realizada de forma indiscriminada.

[41] Neste contexto Sofia Casimiro, Liberdade e Segurança no Combate ao Terrorismo: Quis Custodiet Ipsos Custodes? Uma perspeiva Jurídica. Nação e Defesa – Terrorismo e Violência Política. Ed. Instituto de Defesa Nacional. N.º 152 (2019), [p.23-38], veja-se os exemplos de programas de vigilância, utilizados para combater o fenómeno do terrorismo, que geraram alguma controvérsia e forte reação do Parlamento Europeu, cujo o conhecimento resultou, entre outras fontes, das revelações de Edward Snowden (antigo funcionário da NSA/CIA), em 2014. "O programa ECHCELON que consiste num sistema de vigilância eletrónica desenvolvido pelo Reino Unido, Estados Unidos da América, Canadá, Austrália e Nova Zelândia, e que apresenta como caraterística a capacidade praticamente global de vigilância, recorrendo principalmente a estações recetoras via satélite e a satélites de espionagem. Outra caraterística é o facto de funcionar a nível mundial graças a uma cooperação entre vários países (…) representando uma vantagem comparado com sistemas nacionais". Outro programa utilizado é o PRISM, "que consiste num programa desenvolvido pelos estados Unidos da América de recolha e tratamento de dados de grande abrangência". A respeito deste programa «PRISM», veja-se também David Silva Ramalho, Métodos ocultos de investigação criminal em ambiente digital: Almedina. 2019, cit., p.150 e ss., sobre as medidas anti-forenses e a recolha de prova digital e ainda Paulo Nunes, Sociedade em rede, Ciberespaço e Guerra de Informação, 2.ª ed. – Publicações IDN, 2016, *cit.*, p.181. Por outro lado existe também o Carnivore, sistema de vigilância eletrónico utilizado pelo FBI para identificar e intercetar comunicações via Internet, possibilitando não só a análise de endereços visitados como também a análise de conteúdos.

[42] Como é o caso do RGPD (Regulamento Geral sobre Proteção de Dados), que feita uma análise mais cuidada revela que "este" não são aplicáveis a situações como as que se visa cobrir com aqueles programas de vigilância, excluindo a sua aplicação às atividades relacionadas com a defesa e segurança do Estado. Cf. Sofia Casimiro, Liberdade e Segurança no Combate ao Terrorismo: Quis Custodiet Ipsos Custodes? Uma perspeiva Jurídica. Nação e Defesa – Terrorismo e Violência Política. Ed. Instituto de Defesa Nacional. N.º 152 (2019), op.cit., p.34-35).

[43] Sofia Casimiro, Liberdade e Segurança no Combate ao Terrorismo: Quis Custodiet Ipsos Custodes? Uma perspeiva Jurídica. Nação e Defesa – Terrorismo e Violência Política. Ed. Instituto de Defesa Nacional. N.º 152 (2019), *op.cit.*, p.36.

Precedido pelos valores da segurança pública e da defesa dos interesses nacionais essenciais, reclama-se a adoção de medidas preventivas excecionais que, em princípio apenas seriam de admitir no âmbito de um processo penal, após a prática de um crime.

A versão atual do n.º 4 do artigo 34.º da Constituição ainda não reflete expressamente essa necessidade, colocando antes uma fronteira intransponível à atuação dos Serviços de Informações, de acordo com a lei e respetivo regime. Sendo que, se encontra expressamente vedado através de vários diplomas nomeadamente da Lei n.º 9/2007, de 19 de fevereiro que estabelece a orgânica do SGSIRP, do SIS e do SIED no artigo 6.º, n.º 1 e n.º 2 e na Lei Orgânica n.º 4/2014, de 13 de agosto (procedeu à 5.ª alteração da Lei Quadro do SIRP, Lei n.º30/84) no artigo 3.º, n.º1 e 2, e artigo 4.º, n.º1. Reitere-se o facto de os limites da atividade dos Serviços não poderem desenvolver atividades de pesquisa, processamento e difusão de informações que envolvam a ameaça ou ofensa aos direitos, liberdades e garantias consignados na CRP e na Lei, ficando sujeitos a todas as restrições legalmente estabelecidas em matéria de defesa de direitos, liberdades e garantias perante a informática.

Como nos refere Manuel Abrantes[44], o legislador constitucional ao introduzir a norma constante no artigo 34.º, n.º4, "não previu que existiria um dia a necessidade de combater determinadas ameaças logo num plano preventivo, com recurso a medidas restritivas que tradicionalmente, apenas seriam de admitir no âmbito de um processo penal em curso", levando-nos a refletir na solução de uma atualização do texto constitucional. Podemos constatar igualmente aqui neste domínio específico, que as Constituições vigentes nalguns dos Estados-Membros da EU parecem encontrar-se preparadas para admitir a interceção de comunicações privadas como finalidades exclusivamente preventivas. Vejam-se, por exemplo, a Constituição Espanhola no seu artigo 18.º, n.º3, quando determina que "é garantido o segredo das comunicações e, em especial, das postais, telegráficas e telefónicas, salvo resolução judicial". A Constituição Italiana estabelece no seu artigo 15.º "a liberdade e o segredo da correspondência e de qualquer outra forma de comunicação são invioláveis. A sua limitação pode ocorrer somente por determinação judiciária, sendo mantidas as garantias estabelecidas pela lei". Já a Lei Fundamental da República Federal Alemã é ainda mais permissiva prevendo no seu artigo 10.º, n.º1 "que o sigilo das comunicações, assim como das comunicações postais e da telecomunicação são invioláveis" e no mesmo articulado no seu n.º2 "as limitações só

[44] Manuel Abrantes, Academia Edu [em linha]. Revista do Ministério Público 156 (Out. – Dez. 2018). p. 157-208-[Consult.25 Jan. 2021]. O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações, p.195. Disponível em https://arquitectura-ucp.academia.edu/Ant%C3%B3nioManuelAbrantes.

podem ser ordenadas em virtude da lei. Se a limitação tiver por finalidade proteger a ordem fundamental livre e democrática ou a existência e segurança da Federação e de um Estado federado, a lei pode determinar que a limitação não seja levada a conhecimento do indivíduo atingido e que, em vez de se seguir a via judiciária, o controle seja feito por órgãos principais e auxiliares, nomeados pelos representantes do povo".

Como é sabido, a Constituição Portuguesa mitiga o âmbito da autorização para a restrição do direito fundamental à inviolabilidade das comunicações "aos casos previstos na lei em matéria de processo criminal", que só se inicia após a receção da notícia de um crime e se destina à realização da justiça e à descoberta da verdade.

Querendo abordar a questão da possibilidade de uma revisão constitucional mais adiante, o facto é que, existem autores que consideram esta solução exagerada, pois o problema seria ultrapassado com uma interpretação atualista e adequada do n.º 4 do artigo 34.º da CRP, que tivesse em conta a intensidade da ameaça que a medida de acesso aos dados visa prevenir e os valores fundamentais que pretende preservar. Contudo, entendemos que é precisamente pelo facto de esta medida ser considerada de exceção que deveria estar recortada de forma precisa na Constituição. Ou seja, a sua fonte de legitimação deveria encontrar expressão numa norma Constitucional de forma expressa e inequívoca[45]. De acordo com Manuel Abrantes, "os riscos colocados por interpretações demasiado amplas das normas constitucionais poderá levar, a de que, um dia, se comece por fazer interpretações diferenciadas e tendenciosas, considerando que certas garantias só valem para os cidadãos e não para os inimigos que colocam um determinado tipo de ameaça, relativamente as quais já seria possível relativizar todos os direitos e garantias constitucionais"[46].

Entendemos ainda que na sequência da quinta Revisão Constitucional (2001), no n.º 3 do artigo 34.º foi aditada a possibilidade de passar a permitir excecionalmente a entrada durante a noite no domicílio de uma pessoa, sem o seu consentimento, na sequência de uma autorização judicial que só poderá ser concedida conforme o disposto e nos termos dos artigos 176.º, 177.º e al. c) n.º 1 do art.º 269.º, todos do CPP. Atendendo ainda à circunstância de os OPC poderem efetuar esta diligência, sem que seja necessário de uma autorização expressa por uma autoridade judiciária (JIC ou MP) nos casos: i) de terrorismo, criminalidade violente ou altamente organizada, quando haja igualmente fundados indícios de prática iminente de crime que ponha em grave risco a vida e integridade de terceiros; ii) em que os visados consintam (neste caso, na circunstância de não haver consentimento do visado e fora de flagrante delito, é, sob pena

[45] *Ibidem*, p.195
[46] *Ibidem*, p.196.

de nulidade, imediatamente comunicada ao juiz de instrução por forma a ser validada a diligência); iii) e aquando da detenção em flagrante delito por crime a que corresponda pena de prisão[47]. Não obstante, a Constituição estabelece ainda um regime excecional na extradição de nacionais portugueses, nos termos do n.º 3 do artigo 33.º e no n.º 1 do artigo 207.º na prática de crimes de terrorismo e de criminalidade altamente organizada.

Quando falamos na introdução de uma nova exceção ao n.º 4 do artigo 34.º da CRP, no âmbito da produção de informações, na prevenção dos crimes supra citados, julgamos que não seria estranho nem uma novidade que se procedesse a uma interpretação "ampla", do artigo, ora em análise. A este propósito recordamos as palavras de Jorge Miranda "as leis restritivas não podem diminuir a extensão e o alcance do conteúdo essencial do direitos, liberdades e garantias (cf. art. 18.º, n.º3, 2ª parte), devendo ainda essas restrições ater-se aos fins em nome dos quais são estabelecidas ou permitidas (cf. art.18.º da CEDH e o art. 30.º da Convenção Interamericana), só devendo ser adotadas se esses fins não puderem ser alcançados por meio de medidas menos gravosas; as restrições devem corresponder à medida exigida por esses fins, não devendo ultrapassar as suas justas exigências; devem limitar-se ao necessário para salvaguardar outros interesses constitucionalmente protegidos; e na dúvida, os direitos devem prevalecer sempre sobre as restrições (in dúbio pro libertate), devendo as leis restritivas ser interpretadas, senão restritivamente, pelo menos sem recurso à interpretação extensiva e à analogia"[48].

Contudo, paradoxalmente a esta tese refere-nos Manuel Abrantes[49], através da análise ao voto vencido do Juiz Conselheiro José Pereira no Ac. 403/2015, do TC "que embora o teor literal do n.º4 do artigo 34.º da Constituição parecesse restringir, à primeira vista, a possibilidade de acesso aos dados de tráfego ao domínio exclusivo do processo penal, isso não implicaria que a atividade dos Serviços se devesse desconsiderar, no âmbito naturalmente das suas atribuições. Para todos os efeitos julgo ser de consenso que os Serviços de Informações se inserem dentro de uma função de "Proteção Administrativa da Constituição", levada a cabo pelo SIRP relativamente a ameaças que podem evoluir para a prática de condutas penalmente

[47] Cf. Art.º 174.º, n.º5 e 6 e art.º 177.º, n.º 4, do CPP.
[48] Jorge Miranda, Manual de Direito Constitucional. Tomo IV. Direitos Fundamentais, 2014, p.20-21.
[49] Manuel Abrantes – Academia Edu [em linha]. Revista do Ministério Público 156 (Out. – Dez. 2018). P. 157-208- [Consult.25 Jan. 2021]. O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações, p.172. Disponível em https://arquitectura-ucp.academia.edu/Ant%C3%B3nioManuelAbrantes.

relevantes suscetíveis de colocar em causa os valores estruturantes do Estado de Direito Democrático"[50].

Assim, defendemos que a atividade desenvolvida pelos Serviços teria de ser tida em conta na relação de complementaridade com o processo penal, não tendo sido intenção do legislador constitucional, no nosso modesto entendimento, criar um corte radical entre o momento prévio de recolha de informações, em nome da prevenção criminal, e o processo penal[51].

Acompanhamos também, o entendimento do Juiz Conselheiro José Pereira no Ac. 403/2015, do TC quanto à questão da conformidade com o princípio da proporcionalidade, na medida em que, esta era "adequada face ao fim a que se destinava – a obtenção de informações relevantes para a prevenção de crimes com especial gravidade".

Por outro lado, "consideramos que a medida era necessária para que os Serviços pudessem atuar no âmbito da prevenção criminal, pois o acesso a este tipo de informações permitiria estabelecer conexões entre informações dispersas com vista à formação da convicção de elementos vitais na constituição de uma cadeia informacional coerente"[52].

Por último, sustentamos que "os efeitos restritivos deste acesso deveriam ser considerados uma justa medida tendo em conta os fins prosseguidos, devido essencialmente à espécie de informação obtida (limitada a dados de tráfego e não também a dados de conteúdo), à escala da informação obtida (limitada a um acesso pontual determinado, por circunstâncias concretas, sendo excluída a recolha em massa e dados) e a existência de um controle prévio composta por três magistrados"[53] designados pelo CSM, de entre juízes conselheiros do STJ, com pelo menos três anos de serviço nessa qualidade[54].

---

[50] Talvez esta tese seja demasiado utópica e merecesse maior reflecção quanto à aplicação prática dos "Serviços de Inteligência" ao serviço dos interesses nacionais, com efeito, no exemplo da concretização da defesa dos direitos, liberdades e garantias dos cidadãos. Mas baseamos esta visão com fundamento, não em leis, propriamente ditas, mas apelando a uma verdadeira Estratégia Nacional de Inteligência. Associamos naturalmente o "Conceito de Estratégia" para fins Militares. Apesar do conceito original de Estratégia ser compreendida num contexto Bélico, esta não deixa de ter uma variedade semântica e prática. Encontrando-se desenvolvido no trabalho exaustivo de Henrique M. Lages Ribeiro no contributo que realizou ao elaborar o "Dicionário de termos e citações de interesse político e estratégico. Gradiva, 2008, p.120-125". De entre os vários significados destacamos a "Grande Estratégia"(GE), "o verdadeiro objetivo da GE deve ser o de alcançar uma segura e duradoura paz". Como nota Lages Ribeiro, o papel desta GE é "coordenar e dirigir todas as respostas de uma Nação, ou de um conjunto de Nações, para a consecução do objetivo definido pela política fundamental". " A arte e a ciência de empregar o poder nacional sob todas as circunstâncias para exercer graus e tipos desejados de controlo sobre o oponente através de ameaças, força, pressões indiretas, diplomacia, subterfúgio e outros imaginativos meios e, consequentemente, alcançar os interesses e os objetivos nacionais de segurança", *apud* COLLINS, John M., the essence of Strategy, in Grand Strategy: Principles and Practices, US Naval Institute, 1973;Ref.ªC, p.3-1.

[51]Cf. Manuel Abrantes, p.173. Disponível em https://arquitecturaucp.academia.edu/Ant%C3%B3nioManuelAbrantes.

[52] *Ibidem.*

[53] *Ibidem.*

[54] Cf. Art.35.º do Decreto n.º 426/XII.

Consideramos a função dos Serviços de tal ordem importante para o desempenho das atribuições estaduais que deve prever-se um sistema de garantias seguro, amplo e visível. A CRP não pode deixar de consagrar garantias específicas aos Serviços devendo estes retribuir com devida lealdade e obediência à Lei Fundamental. Note-se que, esta previsão não afeta nem diminui o exercício das suas funções, a operacionalização das suas ações, a eficiência dos seus métodos, a eficácia da sua atividade, contribuindo antes, em realçar a importância e a dignidade constitucionais dos Serviços devendo, ainda, determinar garantias e restrições específicas, ampliar exceções no texto da Lei Fundamental e que não deveriam vincular a atuação daqueles[55].

A questão que se coloca não será tanto a interpretação ou restrição que a norma constitucional valora e legítima num quadro teleológico e axiológico, mas antes considerar-se a possibilidade de dotarmos os organismos do Estado - incumbidos de assegurar a segurança nacional, dos cidadãos e da própria estrutura democrática que se exige a um Estado de Direito Democrático - no âmbito preventivo de instrumentos e garantias legais na prossecução das suas atribuições. Nunca olvidando que estes são um garante da soberania do Estado, à semelhança dos seus congéneres europeus[56], e em relação aos quais não prevê a possibilidade de acesso aos metadados, o que deixa os mesmos serviços numa situação de particular vulnerabilidade, ainda

[55] Cf. José Fontes, "A Constituição e os Serviços de Informações. Segurança e Defesa" Nº 15 (Out.-Dez. 2010), p. 1-7. Disponível em https://repositorioaberto.uab.pt/handle/10400.2/1788

[56] Destaca-se o CdB (Clube de Berna) constituído pelos serviços de informações de segurança europeus (grupo informal), integrado por todos os países da União Europeia, a Noruega e a Suíça. Veja-se a este propósito a referência de Mariana Machado in "O acesso aos metadados pelos Serviços de Informações da República Portuguesa á luz da Lei e da Constituição, p.45.

comprometendo a eficácia de uma cooperação efetiva [57] aos restantes países europeus que poderá resultar num prejuízo majorado por tal limitação.[58]

Neste particular ponto ainda resta esclarecermos de que forma poderíamos solucionar ou ultrapassar a questão do n.º 4 do artigo 34.º da Constituição?

A discussão em redor do plano constitucional mereceu a apreciação como já foi referenciado, no Ac.403/2015, do TC, destaca-se o voto vencido do Juiz Conselheiro José Pereira, uma vez mais no sentido de reforçar a importância da atividade dos Serviços de Informações, no quadro de uma democracia constitucional, colocados em paralelo entre os valores democráticos e a adoção de políticas públicas promotoras de segurança. Trata-se neste domínio, afigurar o argumento que sustenta a relação de incindibilidade entre liberdade e segurança. Como afirma Gomes Canotilho e Vital Moreira, "o direito à liberdade não é um direito absoluto, admitindo restrições». Restrições que se traduzem em medidas de privação total ou parcial dela, (…) não pudendo a lei criar outras"[59]. A Constituição apesar de não determinar uma disposição de um direito à liberdade em geral, consagra as principais liberdades em que ela se analisa, englobando sub-direitos conforme o disposto no seu artigo 27.º (e.g: o direito de não ser detido ou preso pelas autoridades públicas, salvo nos casos e termos previstos neste artigo; o direito de não ser aprisionado ou fisicamente impedido ou constrangido por parte de outrem e ainda o direito á proteção do Estado contra os atentados de outrem á própria liberdade), estando sujeito às competentes regras do artigo 18.º, n.º2 e 3 da CRP.

---

[57] A respeito desta cooperação, a criação do EU INTCEN - ou Centro de Situação da UE (EU SITCEN), como era chamado até 2012 - está intimamente ligada ao estabelecimento da Política Europeia de Segurança e Defesa (PESD). O desenvolvimento das capacidades de gestão de crises da PESD e o envio de missões civis e militares tornaram claro que era necessária uma estrutura de análise de inteligência mais ampla. Os acontecimentos de 11 de setembro de 2001 e as crescentes ameaças do terrorismo global também realçaram a necessidade de uma análise de informações atempada e precisa para apoiar a formulação de políticas da UE. Em 2002, o EU SITCEN foi criado no Secretariado-Geral do Conselho, diretamente ligado ao gabinete do Alto Representante. No mesmo ano, pessoal dos serviços de informações dos Estados-Membros foi destacado para o SITCEN da UE. Em 2005, o SITCEN da UE foi reforçado com a chegada de uma equipa de peritos antiterroristas destacados dos serviços de segurança dos Estados-Membros. Isto permitiu ao SITCEN da UE fornecer ao Conselho avaliações estratégicas da ameaça do terrorismo com base em informações dos serviços nacionais. Em 2007, o SITCEN da UE reforçou a sua colaboração com a Direção de Informações do Estado-Maior Militar da UE (EUMS), concluindo um acordo funcional, a chamada Capacidade Única de Análise de Informações (SIAC). Todas as avaliações de inteligência emitidas para os Estados-Membros são produtos conjuntos preparados no âmbito do SIAC. Com a entrada em vigor do Tratado de Lisboa, o SITCEN da UE ficou sob a autoridade do Alto Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança / Vice-Presidente da Comissão. Em 2011, o SITCEN da UE foi transferido para o Serviço Europeu para a Ação Externa (SEAE). Na sequência das mudanças organizacionais no SEAE em março de 2012, o EU SITCEN foi renomeado para Centro de Análise de Inteligência da UE (EU INTCEN). Disponível em: https://www.statewatch.org/media/documents/news/2016/may/eu-intcen-factsheet.pdf [consult. 03 Março de 2021].

[58] Cf. Mariana Machado, O acesso aos metadados pelos serviços de informações da Republica Portuguesa á luz da Lei e da Constituição, Almedina, 2019, *op.cit*. p. 45.

[59] Cf. J.J Gomes Canotilho e Vital Moreira – Constituição da República Portuguesa Anotada Artigos 1º a 107º. Coimbra Editora, 2007, *op.cit.*, p.478 e ss.

Ainda no artigo 27.º da Constituição para além da liberdade, determina que todos têm direito à segurança confirmando um conceito fundamental que deve assistir a tudo o que se relacione na área da segurança, isto é, como elucida Pedro Simões "a liberdade sem segurança significa a vigência da lei do mais forte, e a segurança sem liberdade constituiria o único privilegio do escravo, o que seria inaceitável"[60].

Referente a este direito à segurança, dizem-nos Gomes Canotilho e Vital Moreira, que significa essencialmente uma garantia de exercício seguro e tranquilo dos direitos, liberto de ameaças ou agressões[61]. Por um lado, numa dimensão negativa, estritamente associada ao direito à liberdade, traduzindo-se num direito subjetivo à segurança (direito de defesa perante agressões dos poderes públicos); por outro lado, numa dimensão positiva, traduzindo-se num direito positivo à proteção através dos poderes públicos contra as agressões ou ameaças de outrem (segurança da pessoa, do domicílio, dos bens)[62]. Do exposto, conforme decorre da parte final do n.º 4 do artigo 34.º da CRP que consiste numa autorização constitucional expressa para a restrição do direito fundamental à inviolabilidade das comunicações, conjugado com os pressupostos exigidos no n.º 2 do artigo 18.º para que qualquer restrição a um direito, liberdade e garantia possa ocorrer reside na existência de uma autorização constitucional para esse efeito, pois essa restrição só será possível nos casos expressamente previstos na Constituição. Com efeito, esta norma constitucional parece-nos ser demasiado perentória quando prevê a proibição indubitável a toda e qualquer ingerência nas comunicações privadas "*salvo nos casos previstos na lei em matéria de processo criminal*". Sendo que à luz da versão vigente da constituição, a única forma de legitimar uma restrição àquele direito fundamental circunscreve-se na conexão no âmbito de um processo penal e, portanto, fora das fronteiras de atuação, alegadamente, da atividade e autorização a que os Serviços de Informações estão legalmente vinculados. Como refere António Abrantes "é aqui que deverá ser procurado o fundamento para legitimar uma

[60] Cf. Pedro Simões, Os Serviços Secretos em Portugal. Os serviços de informação e a comunicação social. Prefácio, 2002, *Op.cit*., p.55 e 56. Neste contexto aproveitaria para fazer referência a uma passagem de Beccaria parafraseando Montesquieu in "Dos Delitos e das Penas ", p.38: "Toda a pena que não deriva da absoluta necessidade é tirânica"…embora as penas produzam um bem, elas nem sempre são justas, porque, para isso, devem ser necessárias, e uma injustiça útil não pode ser tolerada pelo legislador que quer fechar todas as portas à vigilante tirania". Neste sentido e tomando em linha de raciocínio o exposto, julgamos que só as medidas, necessárias, à prevenção criminal adequadas num quadro de garantias e liberdades dos cidadãos realizará o bem comum e a atuação de organismos (Serviços de Informações) capazes de salvaguardar, não só, os interesses nacionais, como a proteção que o Governo deve dar a todos para poderem conservar os seus direitos pessoais.

[61]Cf. J.J Gomes Canotilho e Vital Moreira, Constituição da República Portuguesa Anotada Artigos 1º a 107º. Coimbra Editora, 2007, *Op.cit.*, pp.478 - 479.

[62] *Ibidem.*

restrição a esse direito fundamental"[63]. A este respeito chamamos à colação a declaração de voto da Juíza Conselheira Maria Amaral (Cf. Acórdão n.º 403/2015 do TC) que dissentiu da interpretação sufragada pela maioria no que diz respeito à "tensão" ou "colisão" entre dois valores constitucionais – por um lado, a liberdade individual expressa no direito à inviolabilidade das telecomunicações, por outro, a segurança e preservação da própria ordem constitucional, expressa na necessidade de prevenir a ocorrência de atos que contra ela atentem. Neste sentido, "concordamos com a posição de princípio de que as normas constitucionais que autorizam expressamente restrições a determinados direitos fundamentais não estão efetivamente a criar verdadeiras relações de regra/exceção entre o direito em questão e a possibilidade da sua restrição, mas sim simplesmente a antecipar uma possível ocorrência futura de conflitos entre esse direito fundamental e outros interesses constitucionalmente protegidos, devolvendo ao legislador ordinário a tarefa de os solucionar. O que o legislador constitucional não previu expressamente quando formulou o âmbito desta exceção é que a preservação desses valores comunitários fundamentais poderia ter de passar pela aplicação de medidas restritivas preventivas num momento prévio ao processo penal, de forma a evitar que determinados crimes sejam efetivamente cometidos e lesem de forma grave os valores comunitários fundamentais que os tipos legais de crime que os consagram visam, em primeira linha, salvaguardar"[64].

Na perspetiva de Manuel Abrantes e como refere o Ac.403/2015 do TC, pela Juíza Conselheira Maria Amaral, a existência de uma inegável afinidade *valorativa* ou *teleológica* entre as finalidades prosseguidas pelos Serviços de Informações e as finalidades prosseguidas no âmbito de um processo penal. Deste modo, esclarece-se que "a existência dos serviços justifica-se efetivamente para salvaguardar bens jurídicos constitucionais que possuem a importância semelhante face aos bens que são tutelados por normas penais incriminadoras"[65].

No caso de existir uma tensão ou colisão entre dois valores constitucionais de elevadíssima grandeza – o valor da liberdade individual e o valor da segurança e preservação da própria ordem constitucional, devendo esta questão ser constitucionalmente resolvida, não cabendo ao intérprete empreender, o facto é que o próprio legislador constituinte conferiu uma solução clara determinando de reserva absoluta do processo criminal (como se retira do n.º 4 do artigo 34.º da Constituição). A menos que, haja uma revisão constitucional prevendo uma autorização explícita aos Serviços de Informações, situando-se estes atualmente fora do âmbito do poder

[63] Cf. Manuel Abrantes, O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações, p.200. Disponível em https://arquitectura-ucp.academia.edu/Ant%C3%B3nioManuelAbrantes
[64] *Idem*, p.201 e 202.
[65] *Ibidem*

judicial e que atuam com outras finalidades que não as próprias de um processo penal, não podem em caso algum, intercetar os designados metadados.[66]

Na verdade, é com base nesta exceção à inviolabilidade das comunicações que o processo penal consagra meios de obtenção de provas como as apreensões de correspondência e escutas telefónicas. Seguindo naturalmente regras e requisitos apertados, havendo necessidade de uma consagração expressa, em nome do princípio da reserva de lei e das estritas barreiras de permissão.

Fruto do avanço tecnológico e da dependência de aparelhos tecnológicos, que se gerou em torno de uma massificação de busca de informação e constante atualização face ao desenvolvimento de "aplicações" levada a cabo pelas grandes corporações digitais tornou-se imperativo criar mecanismos, e um "ponto de equilíbrio já difícil de alcançar, na área da criminalidade grave e organizada, pois, por vezes, a invasão do agente ser a única forma de lograr o combate ao crime[67]".

Produto da globalização e do avanço constante desta nova "*era digital*" levou a que as grandes organizações criminosas também elas encontrassem novos instrumentos e passassem por debaixo dos radares dos Estados e das organizações no combate à criminalidade grave e organizada.

Os Estados viram-se obrigados a conjugar esforços, criando várias medidas de cooperação em matéria de criminalidade organizada, bem como ao terrorismo e criminalidade especialmente violenta[68].

Claro que não se circunscreve apenas a este tipo de crimes, hoje enfrentamos com uma maior transparência judicial e divulgação através dos *media* de alguns processos-crime, nomeadamente os crimes de corrupção e branqueamento de capitais que geram uma revolta popular contra o próprio sistema judiciário, comprometendo muitas das vezes o papel dos juízes que não se podem abster desta censura popular, vendo a sua vida pessoal mediatizada por comentadores e "bloggers"[69].

---

[66] Cf. refere a Juíza Conselheira Maria Amaral no Ac. 403/2015 do TC e que dissentiu desta interpretação.
[67] Cf. Rita Neves, As ingerências nas comunicações eletrónicas em processo penal. Coimbra editora, 2011, p.53.
[68] Cf. Diretiva (EU) 2017/541, do Parlamento Europeu e do Conselho de 15 de Março de 2017, da Lei de Branqueamento de capitais e ao financiamento do terrorismo, Lei n.º 83/2017, de 18 de agosto e ainda relativa à Decisão Europeia de Investigação (DEI) que decorre da Lei n.º88/2017, de 21 de agosto (transpõe a Diretiva (EU) 41/2014, do Parlamento Europeu e do Conselho de 3 de abril de 2014.
[69] Cf. Rita Neves apud Jorge Figueiredo Dias, sobre a revisão de 2007 do Código de Processo Penal Português", In Revista Portuguesa de Ciência Criminal, Ano 18, n.ºs 2 e 3, Abril-Setembro 2008, Coimbra Editora, p.384 – "a verdade que o direito serve há- de ser, não uma verdade obtida a todo o preço, mas uma verdade processualmente válida", p.54.

Já Figueiredo Dias[70], quando se reporta à tese de que a grande criminalidade "moderna" só pode combater-se com a plena admissibilidade da prova carreada através de escutas sistemáticas opõem-se igualmente á tese contrária, da total inadmissibilidade de princípio, seja qual for o tipo de criminalidade em causa. Por isso, defende que uma adequada solução de futuro se traduzirá na existência, político-criminalmente imposta, de uma consideração diferenciada e diversificada. No tema em apreço talvez pudéssemos incluir a regulamentação de uma política-criminal coadjuvada pela implementação de uma política de inteligência eficiente dotada de autonomia e controlo. Não obstante, esta última observação e as legislações empreenderem já uma regulamentação destas questões, embora com limites a certas situações e muitas vezes duvidosa ou mesmo contestável nas soluções preconizadas, outras omitem qualquer regulamentação, deixando que tudo se passe ao nível de provas ilícitas e de proibições de prova[71]. Como nos ensina Figueiredo Dias, o "ponto de equilíbrio dos interesses conflituantes deve ser um para a criminalidade "geral", mesmo quando deva reputar-se grave ou muito grave (…). Por outro lado, deverá ser diferente, para a grande e nova criminalidade, concretamente, para o terrorismo e a criminalidade organizada. Aqui, as "vítimas" reais e potenciais têm um direito indeclinável a uma proteção reforçada e, consequentemente, a uma intensificação do intervencionismo estadual. Com uma dupla e inultrapassável limitação, em todo e qualquer caso: a que resulta do respeito pelo núcleo irredutível da dignidade humana que pertence também ao criminoso mais brutal e empedernido; e a que deriva da exigência jurídico-constitucional de não diminuição, pela legislação ordinária e pela sua aplicação, "da extensão e do alcance do conteúdo essencial dos preceitos constitucionais" em matéria de direitos, liberdades e garantias"[72].

De volta à autorização constitucional que restringe o direito à inviolabilidade das telecomunicações, constante do n.º 4 do artigo 34.º da CRP, apesar de constituir uma exceção, e a mesma só comportar a matéria de processo criminal, que maioritariamente se encontra consensual no Tribunal Constitucional no sentido em que se encontra vedado a qualquer processo interpretativo que procure indagar da razão de ser dessa mesma exceção, a fim de saber se nela se poderá ou não incluir outra matéria que, não sendo a expressamente prevista, apresenta no entanto esta última afinidades valorativas constitucionalmente relevantes. Porém houve quem não entendesse o conceito constitucional de autorização para restringir [um direito

[70]Cf. Jorge Figueiredo Dias, "Sobre a revisão de 2007 do Código de Processo Penal Português", Revista Portuguesa de Ciência Criminal, Ano 18, n.ºs 2 e 3, Abril-Setembro 2008, Coimbra Editora, p.383
[71] *Ibidem*, p.383.
[72] *Idem*, p.384.

fundamental] deste modo. Verificamos que os fundamentos constitucionais que justificam a existência dos Serviços de Informações não foram abordados pelo Tribunal no Ac. n.º 403/2015 nem no Ac. n.º 464/2019. Contudo, não foi desprezado neste último, pela declaração de voto da Juiz Conselheira Maria Amaral, que apesar de citar: "numa ordem, como a nossa, de Estado de Direito Democrático, justifica-se pela necessidade de salvaguardar bens jurídicos, coletivos e individuais, que ocupam na axiologia constitucional um lugar não menor que os bens tutelados por normas penais incriminadoras. (…) Havendo uma afinidade valorativa ou teleológica entre as finalidades prosseguidas pelos serviços de informações e as normas incriminadoras, (…) poder-se-ia concluir, se tivesse sido outra posição conceptual e metódica de que partisse, que a autorização constitucional para restringir a inviolabilidade das telecomunicações em «matérias de processo criminal» se entenderia, por maioria de razão, aos Serviços de Informações"[73].

É claro que entendemos a excecionalidade deste meio de obtenção de prova assim como por analogia a outros regimes mais agressivos dos direitos, liberdades e garantias fundamentais que ofendem mais gravemente bens jurídicos dos cidadãos. Veja-se por exemplo o regime do agente infiltrado, consagrado em diploma autónomo, assim como o registo de voz (off) e de imagem.[74]

Como refere Manuel Valente, "lembramos que este meio ou técnica, sacralizada pela PJ, encontra-se sediada nas polícias. Não obstante de ser instrumentalizada por estas, impende o seu controlo da AJ competente, ou seja depende de autorização judicial e nunca pode funcionar como típica medida cautelar e de polícia, para além de realizarem-se apenas no inquérito (cfr. decorre do n.º 1 do art.º 187 do CPP) "[75]. Contudo, não podemos ignorar que estas interceções

[73] A este respeito, Pedro Simões – Os serviços secretos em Portugal. Prefácio: 2002, pp.81 e ss - aquando da indagação das escutas telefónicas como fonte de informação, menciona a opinião de alguns ex-dirigentes dos Serviços, e não só, divergindo na sua justificação. Assim, por um lado houve quem entendesse, talvez por necessidade e razões práticas, dadas as limitações e condicionamentos na obtenção de provas, perceber que sem escutas telefónicas os serviços ficam reduzidos a um gabinete de estudo. A inexistência deste meio pode condicionar qualquer tipo de investigação, inclusivamente poderão surgir «brechas» no sistema de segurança interna (…), adianta ainda que se torna impossível na área das informações darem-se elementos mais objetivos, mais concretos, nomeadamente quando se trata de informação veiculada através de serviços de informações congéneres, considerando grave porque esta área situar-se nas áreas do terrorismo e demais áreas que causam danos à sociedade portuguesa. Mais cauteloso, ainda que partilhe da mesma opinião e considerar-se defensor deste instrumento de investigação, defende que o que é decisivo é que haja uma fiscalização judicial e que fosse autorizado por um órgão de natureza jurisdicional (como previsto no Decreto n.º 426/XII no seu artigo 78.º e 35.º). Contrariamente a esta opinião existe quem não veja condições para que seja alargado os poderes existentes, e nomeadamente alterar a delimitação que existe hoje entre os Serviços e as entidades habilitadas a proceder à instrução de processos-crime, e não devendo por isso, ser posto em causa no ordenamento jurídico português. Não menos relevante das demais opiniões foi a de que durante muito tempo, a proibição constitucional de realizar «escutas», serviu para uma fação, que estava instalada nos serviços, explicar ou justificar a sua própria ineficácia e incompetência. Defendendo que já se fez prova que esse instrumento não é imprescindível, alegando que há múltiplos instrumentos que não estavam a ser utilizados e que agora estão a ser utilizados e produzem excelente informação, de qualidade, a qual é seguramente um meio bastante e adequado para que os serviços sejam competentes.

[74] Cf. Lei n.º 101/2001, de 25 de agosto e art.º 6 da Lei n.º 5/2002, de 11 de janeiro.

[75] Cf. Manuel Valente – Escutas Telefónicas. Da excecionalidade à vulgaridade. Almedina, 2008, pp.21 e ss.

bem como as gravações de conversação ou comunicações, não impedem que o OPC, que procede à investigação, tome previamente conhecimento do conteúdo da comunicação a fim de proceder aos atos cautelares necessários e urgentes que julgar pertinente para assegurar os meios de prova (cfr. n.º 1 do art.º 188 do CPP). Como decorre da Lei n.º 53/2008, de 29 de agosto (LSI), confere aos OPC e não só, medidas preventivas de polícia que têm vindo a ser consagradas amplamente na legislação da generalidade dos ordenamentos jurídicos dos Estados, como forma de prevenir atividades que possam colocar em causa a segurança pública.

Como supra mencionado, noutros ordenamentos jurídicos estas medidas preventivas de polícia têm vindo a revelar um impacto restritivo bastante mais forte, tendo evoluído (ou regredido, consoante a leitura que delas seja feita) para verdadeiras medidas de vigilância e de controlo individual sobre pessoas meramente suspeitas, com uma aplicação cada vez mais generalizada no âmbito da prevenção do terrorismo.[76]

Analisando também a questão da cadeia de custódia da prova, e não querendo aprofunda-lo em razão de recear um desvio ao tema em análise, levantamos um conjunto de questões que obrigariam a desenvolver outras tantas. Portanto circunscrevendo-nos a este elementar juízo alusivo à cadeia de custódia da prova com os princípios constitucionais da prova, nomeadamente, a nulidade e proibição das provas que decorre do n.º 8 do artigo 32.º da CRP em conjugação com o n.º 3 e 4 do artigo 126.º do CPP, que sob o escopo de uma matriz constitucional democrática garante-se a efetividade do princípio do devido processo legal dotado de todas as garantias processuais (v.g., n.º 4 e 5 do artigo 20.º da CRP). Reserva-se, assim, aos entes judiciários – Juiz, Ministério Público e OPC - que operacionalizem dentro do quadro da legalidade democrática e do *iter processualis a* verificação da veracidade, ou seja, a comprovação da verdade de todos os factos essenciais à descoberta da verdade[77]. Como refere Manuel Valente, impõe-se, por isso, uma atuação por parte dos operadores judiciários, geradora de confiança e que garantam este comportamento sistemático, coerente, consistente e íntegro na prossecução dos atos pré-processuais ou extra - processuais[78]. Paralelamente a este princípio de confiança encontramos também o princípio da boa-fé que se traduz num instrumento

[76] Cf. Manuel Abrantes no âmbito da aplicação de medidas preventivas de polícia à margem do processo penal. Manuel Abrantes, Academia Edu [em linha]. Revista do Ministério Público 156 (Out. – Dez. 2018). [Consult.25 Jan. 2021]. O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações. Disponível em https://arquitectura-ucp.academia.edu/Ant%C3%B3nioManuelAbrantes, *op.cit.* pp. 181 e ss.

[77] Sobre os "princípios da identidade e autenticidade na cadeia de custódia da prova" vide Manuel Valente, Cadeia de custódia da Prova. Almedina: 2019, p.45-48

[78] *Idem*, p.55 e 56.

garantístico das expetativas e da confiança dos particulares, geradas a partir de comportamentos dos operadores do Estado – *in casu*, dos OPC.

Segundo Manuel Valente, enquanto meio de obtenção de prova e tomando como exemplo a possibilidade da realização de escutas telefónica pelos Serviços, para além de estes estarem impedidos por imposição de comando constitucional, não são OPC nem APC, não podendo desempenhar e praticar atos processuais e pré-processuais, como resulta dos seus diplomas orgânicos[79].

Por mais que queiramos negar a utilidade da aplicação a montante de medidas preventivas, revela-se necessariamente um conflito de direitos a salvaguardar. Não sendo possível neutralizar determinadas ameaças, no caso de existirem pessoas classificadas como perigosas pelas autoridades, através da aplicação de sanções penais, porque as mesmas não cometeram ainda qualquer infração penal concreta, procura-se deste modo, o controlo destas pessoas de forma a assegurar que não vêm a fazê-lo.

Como referimos, aquando da declaração de voto da Juiz Conselheira Maria Amaral, por maioria de razão e da necessidade de fornecer os instrumentos adequados a todos os operadores do Estado, frente às novas ameaças emergentes desta "era digital", ou como muitos a descrevem, de "quarta revolução industrial"[80], o reforço das competências dos serviços de inteligência para a produção de informações à margem do processo penal no âmbito dos crimes considerados mais graves ou que afetem grandemente a estabilidade social, económica e os interesses estratégicos nacionais, revela-se necessária e vital.

Recordamos que a adoção destas medidas – acesso aos metadados – foi reconhecido pelo próprio TEDH, ainda em 1978, relevando que, "dados os perigos colocados às sociedades democráticas por formas cada vez mais sofisticadas de terrorismo e de espionagem, seria legítimo que os Estados restringissem o direito ao respeito pela vida privada e familiar consagrado no artigo 8.º da CEDH através de procedimentos de vigilância secreta da correspondência e das comunicações privadas, como forma de garantir a segurança nacional e de prevenir a comissão de infrações penais"[81].

[79] Cf. Manuel Valente – Escutas Telefónicas. Da excecionalidade à vulgaridade. Almedina, 2008, p.26-28.
[80] Ver WEF (World Economic Forum). Disponível em https://www.weforum.org/reports [consult. 04 maio de 2021].
[81] Cf. Manuel Abrantes, O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações, p.192, e relativo ao trecho da decisão ver: Klass and Others v. Germany, Application n.º 5029/71, Judjement, 6 September 1978, disponível em https://hudoc.echr.coe.int/rus#{%22itemid%22:[%22001-57510%22]}

Exposta a temática sobre a interpretação e o alcance do n.º 4 do artigo 34.º da CRP cabe-nos a análise de alguns princípios e limites constitucionais que os Serviços de Informações não se podem arredar.

3. Princípios fundamentais e processuais-penais (relevantes)

3.1 O artigo 18.º da Constituição e o princípio da concordância prática.

Cabe-nos então enunciar alguns princípios fundamentais que servem de âncora à concretização e salvaguarda das normas constitucionais, uma vez que estas dão suporte à inviolabilidade das comunicações e do acesso aos metadados.

Comecemos pelo n.º 2 do artigo 18.º da CRP, que impõe a observância do princípio da proporcionalidade em matéria de intervenções restritivas de direitos fundamentais, estabelecendo que a lei deve limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos. Posto isto, não podemos deixar de ter em conta a necessidade da concordância prática entre os direitos fundamentais das pessoas, acerca das quais os Serviços pretendam reunir informações, e zelar pelos interesses da segurança interna (pública) e de combate à criminalidade organizada, bem como a espionagem e o terrorismo. Apesar de mencionarmos o tipo de crime - espionagem – por razões de objetividade e ser um tema que resultaria de uma abordagem diferente para além de ser uma matéria mais sensível, e ser também objeto de um longo estudo, não levantaremos quaisquer razões dogmático-jurídicas.

Portanto, quando falamos neste princípio da concordância prática, impõe-se aqui a coordenação e combinação dos bens jurídicos em conflito de forma a evitar o sacrifício (total) de uns em relação aos outros[82]. Podemos constatar que a intromissão em dados de comunicações coloca em conflito direitos e valores constitucionais. Por um lado, revela-se num espetro de bens jurídicos ou direitos fundamentais tão eminentes como a dignidade humana, o desenvolvimento da personalidade, a integridade pessoal, a privacidade/intimidade, a autodeterminação informativa e a confidencialidade e integridade dos sistemas técnico-informáticos; por outro lado, como já foi referido, assegura valores constitucionais endereçados à salvaguarda da comunidade, como a segurança interna (pública) e a defesa nacional.

Tentaremos assim abordar estes direitos e outros que acharmos pertinentes, à luz de uma melhor introspeção sobre a temática do papel fundamental de um serviço de informações

[82] Cf. J. J. Gomes Canotilho – Direito Constitucional e Teoria da Constituição. 7ª ed. 17ª (reimp). Coimbra, p.1225.

íntegro, pautado pelos valores constitucionais de um estado de direito democrático e dignificado com a seriedade que lhe é merecida. Deixando de uma vez por todas o rótulo de um Serviço manejado por cabalas e teorias da conspiração, que apesar de alguns episódios constrangedores e que comprometem a confiança que se almeja de um organismo de inteligência do século XXI, nenhum governo poderá dar-se ao luxo de menosprezar a utilidade de tão vital Serviço.

3.2 Princípios relacionados com os direitos, liberdades e garantias dos cidadãos e que se atribuem ao núcleo essencial da inviolabilidade das comunicações e dos metadados?

Na análise do princípio da proporcionalidade, como já foi mencionado, não pode o Estado arredar-se de delimitar o acesso aos dados pessoais dos cidadãos. Assim, além de exigir um fundamento preciso e determinado, na lei – princípio da determinabilidade - não pode ser um acesso utilizado para além do estritamente necessário e adequado. Impõe-se que obedeça naturalmente a requisitos da necessidade, exigibilidade e proporcionalidade (ou proibição do excesso).[83]

Foi reiterado diversas vezes no douto acórdão de 2015 do TC que a "concordância prática" entre os valores constitucionais de perseguição e punição do crime com os direitos fundamentais, deve ser feita em sede de processo criminal, logo fora do âmbito de atuação dos Serviços, por se entender que a estes não está atribuído quaisquer funções (por maioria de razão), competência e coadjuvação entre os diversos órgãos policiais e judiciários na descoberta da verdade.

Qualquer ação preventiva que interfira, no sentido de comprimir Direitos Fundamentais ou devassar direitos, liberdade e garantias não pode ter lugar fora de um processo criminal devidamente formalizado. "É evidente que uma atuação investigatória processualizada e publicizada, na forma de inquérito preliminar ou de instrução, não só salvaguarda a liberdade e segurança no decurso do processo como dá a garantia de que a prova para ele canalizada foi obtida com respeito pelos direitos fundamentais. A mesma conclusão não se pode extrair de uma ação de prevenção não processualizada ou mesmo não suficiente formalizada, coberta pelo segredo de Estado, que decorre na total ausência de instrumentos defensivos que comportem um mínimo de dialética processual"[84].

[83] Cfr. Acórdão 464/2019 do TC, ponto 11.2.3, pp.41/123
[84] Cf. Ac. n.º 403/2015 do TC, ponto 19.

Sendo certo que uma lei vaga, imprecisa e demasiado abrangente converteria as medidas restritivas em arbítrio, por ausência de critérios objetivos quanto à razão de ser da sua utilização.

Tanto mais que o acesso aos dados, sejam estes de tráfego, de base ou de localização, representa uma intromissão sem que os respetivos titulares tenham conhecimento do facto, ou nem dele se apercebam, e até mesmo uma vez que nem são notificados, nem se prevê quaisquer atos ou procedimentos que permitam o conhecimento ou a cognoscibilidade da intromissão pelos visados. De acordo com o TJUE "importa que as autoridades nacionais competentes às quais foi concedido o acesso aos dados conservados informem desse facto às pessoas em causa, no âmbito dos processos nacionais aplicáveis, a partir do momento em que essa comunicação não seja suscetível de comprometer as investigações levadas a cabo por essas entidades"[85].

Vejamos, a título de exemplo que no direito Sueco,

> *a LEK* [Lei (2012:278) sobre a comunicação de dados relativos a comunicações eletrónicas no âmbito das atividades de informação das autoridades repressivas, e pelo rättegångsbalken (Código de Processo Judicial, a seguir «RB»)], no âmbito de acesso aos dados conservados No âmbito dos serviços de informações, a polícia nacional, a Säkerhetspolisen (Serviço de Segurança, Suécia) e a Tullverket (Serviços Aduaneiros, Suécia) podem, ao abrigo do artigo 1 da Lei 2012:278, nas condições estabelecidas nesta lei e sem o conhecimento do operador de uma rede eletrónica de comunicações ou de um serviço de comunicações eletrónicas autorizado ao abrigo da LEK, proceder à recolha de dados respeitantes às mensagens transmitidas numa rede de comunicações eletrónicas, aos equipamentos de comunicação eletrónica presentes numa determinada zona geográfica e na ou nas zonas geográficas onde se situa ou estava situado um equipamento de comunicações eletrónicas. Em conformidade com os artigos 2 e 3 da Lei 2012:278, os dados podem, em princípio, ser recolhidos se, em função das circunstâncias, a medida for particularmente necessária para prevenir, impedir ou constatar uma atividade criminosa que implique uma ou várias infrações sancionadas com uma pena de prisão igual ou superior a dois anos, ou um dos atos enumerados no artigo 3 desta lei que inclua infrações sancionadas com uma pena de prisão inferior a dois anos. Os motivos que justificam esta medida devem ser superiores às considerações relativas à infração ou ao prejuízo que esta implica para o seu destinatário ou para um interesse que se lhe oponha. Em conformidade com o artigo 5 da referida lei, a duração da medida não pode ser superior a um mês. A decisão de adotar tal medida compete ao diretor da autoridade em causa ou a uma pessoa com poderes delegados para o efeito. Não está sujeita à fiscalização prévia de uma autoridade judiciária ou de uma autoridade administrativa independente. O RB regula a comunicação dos dados conservados às autoridades nacionais no âmbito de inquéritos preliminares. Em conformidade com o artigo 19 do capítulo 27 do RB, a «monitorização de comunicações eletrónicas» sem o conhecimento de terceiros é, em princípio, autorizada no âmbito de inquéritos preliminares que visam, nomeadamente, infrações sancionadas com uma pena de prisão igual ou superior a seis meses[86].

Como já foi referido anteriormente, a génese da Constituição funda-se na prossecução de dois desideratos: o primeiro, ordenar e limitar o poder político, e o segundo, garantir os direitos e liberdades do indivíduo.

[85] Cf. Ac. n.º 464/2019 do TC, ponto 11.2.4.

[86] Acórdão Tele 2. Disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A62015CJ0203# [consult. 28 maio. 2021].

A tutela da privacidade está ligada por inerência à liberdade individual e é neste contexto que o Tribunal Constitucional[87] analisou a liberdade de ação e uma série de direitos relacionados com a esfera íntima e a esfera privada (direito à solidão, direito ao anonimato e a autodeterminação informacional) como reserva da intimidade da esfera privada e, mais amplamente, do direito ao desenvolvimento da personalidade (artigo 26.º da CRP).

Ora, imposto pelo n.º 2 do artigo 18.º da Lei Fundamental estabelece-se o escopo do princípio da proporcionalidade em matéria de intervenções restritivas de direitos fundamentais. A que a lei deve limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos. Na circunstância da definição de um cidadão alvo, a lei não indica critérios objetivos para a seleção, relacionados com a probabilidade de as pessoas visadas estarem envolvidas, direta ou indiretamente, na preparação ou execução de ataques terroristas, ou uma relação, pelo menos indireta, com atos de criminalidade grave, nomeadamente a espionagem, não passando a norma (artigo 4.º da Lei Orgânica n.º 4/2017), no teste da proporcionalidade, por falta de densificação do regime jurídico que lhe serve de pressuposto.

É nosso entendimento, na ótica do princípio da especificação e da limitação da finalidade do tratamento de dados que, por um lado a finalidade do tratamento de dados tem de estar visivelmente definida antes das operações de tratamento terem início, por outro, a utilização posterior dos dados para uma finalidade incompatível com a finalidade original exige outra base legal, e também, a transferência de dados para terceiros constitui uma nova finalidade que exige uma outra base legal.

Essencialmente, o princípio da especificação e da limitação da finalidade significa que a legitimidade do tratamento de dados pessoais dependerá da finalidade do tratamento. Essa finalidade deverá ser especificada e claramente comunicada pelo responsável pelo tratamento antes do início do tratamento de dados. Esta comunicação deverá ter lugar por meio de uma declaração ou, por outras palavras, de uma notificação, à autoridade de controlo competente ou, pelo menos, através de documentação interna, que deverá ser disponibilizada pelo responsável pelo tratamento às autoridades de controlo para inspeção.

Sempre que os dados forem tratados para uma nova finalidade, é necessária uma base legal específica, sendo irrelevante o facto de os dados terem sido inicialmente adquiridos ou tratados para outra finalidade legítima. A divulgação de dados a terceiros terá de ser ponderada com especial cuidado, uma vez que a divulgação constitui habitualmente uma nova finalidade e, por conseguinte, exige uma base legal distinta da base legal para a recolha dos dados.

[87] Cf. Acórdão n.º 464/2019 do TC, ponto 9

Posto isto, atendendo a natureza e prossecução das atribuições a que o SIRP está incumbido em sede de prevenção, e portanto antes sequer da notícia de um crime, muitas das vezes têm os serviços de inteligência, a dificuldade por si só de não possuírem as informações suficientes e não reconhecerem com certeza um alvo em concreto, seja pela complexidade da identificação ou do rastreio dos elementos de prova ou ainda de indícios de elementos suficientes de suspeita de um potencial ilícito criminal, ainda que aparentemente insignificantes num determinado contexto, ou seja, a montante da investigação criminal propriamente dita. A questão é que a menos que tenhamos os instrumentos adequados à repressão em tempo útil, não conseguiremos impedir um atentado terrorista ou ameaça grave à segurança nacional, a proteção efetiva dos cidadãos e a consequentemente perda inevitável de vidas humanas.

Noutra perspetiva, menos ingénua, o facto é que não podemos ficar num "*braço de ferro*" constante, sob o receio de atribuirmos um poder discricionário aos Serviços de Informações interferindo, por isso, na efetividade das suas funções.

Na circunstância de não haver um verdadeiro impulso legislativo de forma a dotar aqueles Serviços de instrumentos adequados e de inovação no quadro político-criminal, não passaram de um mero "gabinete de estudos"[88]. Como refere Rui Pereira, "os serviços não são uma polícia nem têm possibilidades de atuar como as forças de polícia (…). Estão vinculados a um estreito respeito pelos direitos, liberdades e garantias (…), positivamente, são um organismo incumbido em Portugal de produzir as Informações destinadas a garantir a segurança interna, contra quaisquer ameaças à segurança interna, ameaças que podem ser catalogadas segundo a Lei Orgânica, como a espionagem, do terrorismo, de atos de subversão, de sabotagem, ou da criminalidade organizada, que pela sua dimensão, sofisticação a até internacionalização, ponham em causa a segurança interna de Portugal"[89].

Atualizando a perspetiva destas novas ameaças não nos é alheio a nova criminalidade com recurso às novas tecnologias, que hoje em dia podem colocar em causa a integridade e confiança das instituições. Vejamos por exemplo, um ataque informático ao "*data center"* de um hospital, onde para além de dados pessoais estão também alojados outro tipo de dados que se inserem naquela categoria de dados salvaguardados pela própria constituição e por isso reservados à ingerência por terceiros. Por outro lado, encontram-se aparelhos eletrónico que podem ser acedidos remotamente e donde dependem vidas humanas. Quem se responsabilizará? Como podemos detetar os sujeitos responsáveis por tais ataques? Como podemos prevenir tais ações? Que medidas poderíamos adotar a montante das investigações criminais? Questões que se

[88]Cf. Pedro Simões – Os serviços secretos em Portugal. Prefácio, 2002, *op.cit*., p.57 e ss.
[89] *Ibidem*.

colocam, mas[90], não impedem, contudo, de atuar conveniente e adequadamente no momento em que seria possível incapacitar os agentes de perpetrarem esses atos. Caso em que, se de facto, o nosso quadro legal tivesse munido dos instrumentos adequados a dotarem os organismos de atuar conforme seria esperado e em harmonia inclusive, com os seus congéneres, com certeza conseguiríamos "sincronizar" as funções, a que cada órgão judiciário, policial e de inteligência está reservado.

No Acórdão do TC[91] reiterou-se que as ações de prevenção (realizados pela polícia) devem traduzir-se, em medidas de defesa contra perigos concretos. Com efeito, a probabilidade/previsibilidade de ocorrência de situações potencialmente lesivas de bens jurídicos cuja proteção se encontra a cargo do Estado, reclama medidas necessárias para as evitar, e por isso, as medidas preventivas pressupõem habilitações legais de ingerência contra situações de perigo, entendido no sentido de "ameaça objetiva de lesão imediata de bens jurídicos por condutas ilegais particularmente suscetíveis de a gerar numa situação concreta"[92].

Como refere o douto Acórdão, é certo que o princípio da necessidade, numa das suas *dimensões da proibição do excesso*, impõe que o acesso aos dados de tráfego lesivo da autodeterminação informativa se destine a reagir a situações de perigo suficiente indiciadas, ou seja, a situações em que se nada for feito para evitar, serão provavelmente lesados. Contudo, na perspetiva de afirmar-se a concordância prática entre os valores constitucionais de perseguição e punição do crime com os direitos fundamentais, deve ser feita em sede de processo penal. Não podendo ter lugar fora de um processo criminal devidamente formalizado. Assim julgamos ainda, ter presente que a atividade exercida pelos serviços de informações, revestindo-se de uma natureza secreta e não observável pelos cidadãos afetados (a norma constante do artigo 4.º da LOSIRP), deverá estar sujeita a um rigoroso controlo. Controlo esse, que de acordo com o ínsito da norma constitucional, dispõe expressamente a "proibição de toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação"[93].

[90] Neste âmbito têm havido que cada vez mais iniciativas em desenvolver exercícios e formação especializada nestas áreas, nomeadamente alguns cursos livres como o Curso de Cibersegurança e Gestão de Crises no Ciberespaço (IDN), e o Curso Geral de Cibersegurança (CNCS), a fim de proporcionar uma maior conhecimento e detalhe a um maior leque de cidadãos (não reservado apenas a militares ou elementos das forças e serviços de segurança).
[91] Cf. Acórdão n.º 464/2019 do TC.
[92] Cfr Acórdão 464/2019, *apud* Sérvulo Correia, o Direito de Manifestação – Âmbito de proteção e Restrições, Coimbra, 2006, p.98
[93] Cf. Art. º 34. º, n. º 4 da CRP.

Não deverá, contudo, ser vista esta proibição de forma perentória sem enquadrarmos as finalidades dos Serviços e o seu contributo material no que se refere à descoberta da verdade na perspetiva da prevenção e salvaguarda de bens jurídico penalmente relevantes.

Como se verificou no douto Acórdão de 2019 do TC, no âmbito das ações de prevenção criminal, a lei não tem previsto intromissões nas comunicações eletrónicas. O acesso ao conteúdo das comunicações só poder ser autorizada no "inquérito" ou em qualquer outra fase do processo penal[94].

Como refere Germano Marques da Silva, o princípio da legalidade "tem uma natureza essencialmente política, que significa, político antes do jurídico, tendo sido dirigido contra os abusos do «ancien regime»"[95]. Assim de forma a garantir a segurança do cidadão perante o Estado e a garantia da igualdade de tratamento, o essencial está na densificação da lei penal, em obediência à Constituição, sendo esta garante da supressão do arbítrio e da opressão.

Como é frequente, a referência ao «processo justo» ou «processo equitativo» e a própria CRP no seu artigo 20.º, n.º 4, à CEDH no seu artigo 6.º, o PIDCP no seu artigo 14.º assim dispõem. Este princípio é, como refere Germano Marques da Silva, "próprio dos princípios, estruturalmente vago e por isso aberto à ponderação se no processo em concreto foram efetivamente assegurados todos os meios de defesa o que pode ser objeto de apreciação pelo Tribunal Constitucional, já que os direitos, liberdades e garantias são diretamente aplicáveis (art.18.º, n.º 1, da CRP) "[96]. O autor releva este atributo «equitativo» ou «justo» ao que a jurisprudência norte-americana designa por «*due process of law*», e que traduz a ideia de um equilíbrio, entre a acusação e a defesa (e que designamos habitualmente por «igualdade de armas»[97].

Quanto ao princípio da lealdade não se define apenas numa noção jurídica autónoma, sendo de natureza essencialmente moral, com respeito dos direitos e da dignidade de todas as pessoas que participam no processo. Adotar o caminho da deslealdade seria optar pelo autoritarismo, próprio das ideologias totalitárias. "A eficácia da justiça é também um valor que deve ser perseguido, mas, porque numa sociedade livre e democrática os fins nunca justificam os meios, só será louvável quando alcançada pelo engenho e arte, nunca pela força, pelo artifício ou pela mentira, que degradam quem as sofre, mas não menos quem as usa"[98].

---

[94] Cf. Art.ºs, 187.º e 189.º do CPP e artigo 18.º da Lei do Cibercrime
[95] Cf. Germano Marques da Silva, Direito Penal Português. Introdução á teoria da lei penal. Verbo, 2010, p. 256.
[96] Cf. Germano Marques da Silva, Direito Processual Penal Português Vol. I. 2.ª Ed. Universidade Católica Editora, 2017, p.48.
[97] *Ibidem*.
[98] Cf. Germano Marques da Silva, Curso de Processo Penal. Vol. II. 5ª Ed. Revista e atualizada. Lisboa. Verbo, 2011, p.81.

Não menos relevante será o princípio da oficialidade, que através do inquérito, da competência do MP, a investigação pré-acusatória é pública, ou seja, traduz-se no monopólio de poderes do MP para abertura de um processo e ainda uma consequência da conceção do direito penal como instrumento de controlo social pelo Estado[99]. Associado ao princípio da oficialidade encontra-se o princípio da legalidade que como já foi referido, segundo o qual o MP deverá proceder sempre que se verifiquem os pressupostos jurídico-factuais da incriminação e processuais da ação penal[100].

A legalidade da prova é diferente, decorre do art.º 125.º do CPP – "são admitidas as provas que não forem proibidas". Que adiante iremos abordar.

Tendo em consideração que o nosso processo penal tem uma estrutura acusatória, fará todo o sentido em chamarmos à colação todos estes princípios (o princípio da lealdade, o princípio do processo justo ou processo equitativo, o princípio da oficialidade e da legalidade) e entroncar de forma integrada no princípio da investigação judicial.

Este princípio - *da investigação* - não impende ou limita a atividade probatória do Ministério Público, do assistente ou do arguido e o seu total aproveitamento pelo tribunal. É do n.º 1 do art. 340.º do CPP que encontramos subjacente a este princípio e como ensina Figueiredo Dias, "a adução e esclarecimento do material de fato não pertence aqui exclusivamente às partes, mas em último termo ao juiz: é sobre ele que recaio ónus de investigar e esclarecer oficiosamente - independentemente das contribuições das partes – o facto submetido a julgamento"[101]. (*in fine* do artigo 340.º, n.º1: "e para tanto se afigure necessário à descoberta da verdade e à boa decisão da causa").

Posto isto no artigo 126.º do mesmo diploma está prevista, entre outras, a nulidade das provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular.

O Estado e a comunidade não tem interesses opostos ao arguido, ainda que muitas vezes se tem assistido, derivado da conjuntura económico-social e a nível nacional, também se verificar uma censura popular relativo a determinados tipos de crimes perpetrados por figuras públicas. Antes lhe interessa exclusivamente a realização da Justiça, a condenação do culpado e a absolvição do inocente[102]. Germano Marques da Silva fala-nos em razão da natureza e fins da própria sanção penal, "se considera insatisfatória a mera "verdade formal" e insuportável

[99] *Idem*, p.84.
[100] *Idem*, p.85.
[101] Cf. J. Figueiredo Dias, Clássicos Jurídicos. Direito Processual Penal. Coimbra, 2004, *op.cit.*, p.192.
[102] Cf. GERMANO MARQUES DA SILVA, Direito processual penal português. 2011, *op.cit.*, p.159.

admitir-se que alguém possa ser punido apenas por insuficiência de defesa. Sendo igualmente eticamente insuportável que, tendo o tribunal de decidir sobre a culpabilidade do arguido, a convicção dos juízes tivesse de ser formada considerando apenas as provas produzidas pela acusação e defesa o que certamente geraria muitas mais situações de dúvida[103]".

A respeito da "verdade", esta não é senão o resultado probatório processualmente válido, ou seja, a convicção de que certa alegação elementar de facto é justificavelmente aceitável como pressuposto da decisão, por ter sido obtida por meios processualmente válidos. Não uma verdade obtida a todo o preço, mas processualmente válida[104].

Daí que o princípio da legalidade da prova ser indubitavelmente um princípio norteador do processo penal que baliza as provas admitidas, e por isso só serem admitidas as provas que não forem proibidas por lei (cfr. art.º 125.º do CPP). Pressupõe esta norma que existam ou possam existir meios de prova proibidos e proíbe que esses meios de prova sejam utilizados no processo penal.

Quanto ao princípio da legalidade, importa referir a este respeito que este colocaria em causa, caso não for respeitado na sua dimensão formal, o "*princípio da inocência"* do arguido, consagrado no n.º 2 do artigo 32.º da CRP, pois este será também um princípio estrutural do processo que assenta no reconhecimento dos princípios do direito natural como fundamento da sociedade. Estes princípios aliados à soberania do povo, ao culto da liberdade, constituem os elementos essenciais da democracia. Deste modo, se fossem admitidas provas que comprometessem a liberdade comunicativa, seja nas comunicações telefónicas ou a circunstância da navegação na internet (os dados de tráfego ou de localização), representaria um gravíssimo atentado à dignidade da pessoa humana[105]. Portanto as proibições de prova são

[103] *Ibidem*. O autor em nota de rodapé refere ainda que em relação aos críticos do sistema do processo acusatório integrado pelo princípio da investigação e que defendem um processo estrito de partes, assente no princípio da discussão ou acusatório puro, fazem-no porque ele é, em regra, gerador de maiores dúvidas no espirito do decisor e consequentemente conduziria a mais absolvições (in dubio pro reo); e ainda *Op.cit*. Beccaria, Dos delitos e das penas. Fundação Calouste Gulbenkian, 2014, pp.88-90. «Quando as leis são claras e precisas, a tarefa de um juiz não consiste em outra coisa senão em constatar um facto. Se para investigar as provas de um delito é necessário habilidade e destreza, se para apresentar o resultado é necessária clareza e precisão, para ajuizar o resultado em si não é necessário senão um simples e vulgar bom senso (…). É da maior utilidade aquela lei segundo a qual cada homem deve ser julgado pelos seus pares, porque, quando se trata da liberdade e da sorte de um cidadão, é preciso calar os sentimentos que inspira a desigualdade (…). Que os julgamentos sejam públicos, que sejam públicas as provas do crime para que a opinião, que é talvez o único cimento das sociedades, imponha um freio à força e às paixões, para que o povo diga: nós não somos escravos e estamos protegidos» e p.159, "a deficiente produção da prova pode ter também o efeito mais grave que é o de por deficiência da defesa conduzir a mais condenações pois que a atividade da defesa nem sequer chega para suscitar a dúvida no espírito do juiz".

[104] Cf., GERMANO MARQUES DA SILVA, Direito processual penal português. 2011, p.161, *op.cit.*

[105] *Idem*, pp.96 e 97. O autor considera o "princípio in dúbio pro reo um princípio lógico de prova". Uma vez que que é na incerteza que se logrará a maior das arbitrariedades e estando a dúvida na sua base permanecendo frequentemente até ao final. Assim, "ao princípio da presunção da inocência imporá a absolvição do acusado já que a condenação significaria a admissão da responsabilidade sem prova, fruto do azar do arguido que por qualquer razão se viu suspeito da prática de um crime".

por isso verdadeiras limitações á descoberta da verdade, barreiras colocadas à determinação dos factos que constituem objeto de processo penal[106]. Conveniente referir ainda a este propósito; «a indisponibilidade do objeto processual era já uma razão para a exclusão do princípio da "autorresponsabilidade probatória" (…), a atendibilidade do princípio do inquisitório justifica que o material de facto aduzido pelos sujeitos processuais não seja o limite da atividade do julgador, e, a inexistência de ónus de alegação e prova, consagrada quanto ao arguido, no n.º 2 do artigo 32.º da Constituição da República.»[107]

Por fim, não sendo talvez descabido mencionarmos que a regra é o "*princípio da publicidade",* só se justificando o regime de segredo quando esse se afigure necessário para assegurar os interesses da investigação ou os direitos dos sujeitos processuais (no caso do arguido, o seu bom nome e a preservação da presunção da inocência), e ainda como garantia do contraditório (do arguido)[108]. Como resulta da redação do artigo 86.º, n.º 2 do CPP e quando estejam em causa preocupações ligadas à presunção da inocência do arguido, ao respeito pela imagem que os sujeitos pretendam preservar, é dado ao arguido, ao assistente e ao ofendido, a possibilidade de requerer ao JIC que se cubram os autos com a opacidade do segredo de justiça.

4. (In)Viabilidade de uma Revisão Constitucional.

Aqui chegados foi inevitável ponderarmos quais seriam as alternativas de uma reforma constitucional, ou se seria viável ou não uma revisão constitucional relativa a esta matéria. Posto isto, será nossa intenção analisarmos de forma sistemática a questão previamente considerada, desde os limites da revisão às leis restritivas e casos especiais de restrição.

Cientes das funções que se destinam à revisão constitucional, revela-se sobretudo, uma tarefa árdua e complexa face à possibilidade de alteração da Ordem Constitucional originariamente estabelecida, e os efeitos que dessa modificação possa resultar. Como refere Bacelar Gouveia, não será despiciendo afirmar que "as funções atribuídas á revisão constitucional consolidam-se no realismo que ela expressa na sempre difícil e, sobretudo, instável ligação do Direito Constitucional à realidade constitucional, (…) pois que deverá

[106] Cf., MANUEL DE COSTA ANDRADE, Sobre as Proibições de Prova em Processo Penal. Coimbra, 1992, p.83, *op.cit.*
[107] *Op.cit.* GIL MOREIRA DOS SANTOS, Princípios e prática processual penal. Coimbra Edª. 2014, p.53 e 54.
[108] *Idem*, p.59.

constantemente refletir a evolução da situação político-social, ao mesmo tempo que a deve também comandar"[109]. Como adianta o autor, também relativo às tarefas que se exige de uma revisão constitucional, sejam elas a de atualizar, adequando-se a novas necessidades e preocupações, interpretar, estabelecendo novos critérios de interpretação ou ainda de completar a Ordem Constitucional, suprindo falhas e lacunas nas disposições, mantêm-se assim as válvulas de segurança para a permanência do atual sistema constitucional sem ferir ou induzir mecanismos radicais de modificação da Ordem Constitucional[110].

Afigura-se, no entanto, que os direitos fundamentais se referem a determinados domínios da realidade social, considerando por exemplo: o direito à vida como referente à vida humana, a inviolabilidade do domicílio e da correspondência com respeito ao domicílio e às comunicações (escrita, oral, telefónica e cibernética), estando para isso a descrever, em termos materiais, o âmbito da proteção de um direito fundamental[111]. Ainda que de forma necessariamente perfuntória, atentos à economia deste espaço, impõe-se aprioristicamente, a análise do sentido e alcance dos limites da revisão constitucional face ao contexto do acesso aos metadados pelos Serviços de informações e à inviolabilidade das comunicações.

Não obstante, os diversos limites de revisão que alguns autores costumam distinguir[112], realçamos apenas alguns, para termos um fio condutor que nos ajude à perceção da viabilidade ou inviabilidade de uma revisão constitucional.

Quanto aos limites temporais julgamos não haver dúvidas, uma vez que decorre da própria norma constitucional (artigo 289.º) que impede o exercício do poder de revisão constitucional em qualquer momento. Dadas as circunstâncias pandémicas em que vivemos, nestes últimos tempos, a norma deixa explicitamente claro e indubitavelmente esclarecidos, ainda que tenham decorridos cinco anos sobre a data da publicação da última lei de revisão e, salvo a exceção prevista no n.º 2 do artigo 284.º da CRP, que permite à Assembleia da República assumir em qualquer momento poderes de revisão extraordinária, contudo, sujeita aos limites circunstanciais de revisão do artigo 289.º da CRP [113].

---

[109]Cf. BACELAR GOUVEIA, Manual de Direito Constitucional, Vol. I, 5.ª Ed. 2014, *op.cit,* p.572.
[110] *Idem*, pp.573 e 574.
[111] Cf. Gomes Canotilho, Direito Constitucional e Teoria da Constituição, 7ª ed. 17ª Reimp, 2003, *op.cit.,* p.448.
[112] Cf. Bacelar Gouveia, Manual de Direito Constitucional, Vol. I, 5.ª ed. 2014, *Op.cit.,* p.574 e ss.
[113] Cf. Gomes Canotilho, Direito Constitucional e Teoria da Constituição, 7ª ed. 17ª Reimp, 2003, *op.cit.,* pp.1063 e ss. Retira-se ao longo da história, como refere o autor, que "certas circunstâncias de anormalidade (como o estado de guerra, estado de sítio ou estado de emergência), podem constituir ocasiões favoráveis à imposição de alterações constitucionais, limitando a liberdade de deliberação do órgão representativo. Explicando para isso o teor do art.º 289.º, impositivo de limites circunstâncias, que proíbem a revisão Constitucional em situações de anormalidade constitucional."

De uma forma sucinta, julgamos ser pertinente fazer ainda uma abordagem introdutória relativa à problemática no que toca à legitimação dos serviços de informações, através de uma revisão constitucional. Para isso chamamos à colação as reflexões de Manuel Abrantes [114], que em particular se foca na categoria de crimes, que não raras vezes tem suscitado vários debates – os crimes de terrorismo e de espionagem - mas não se esgotando apenas nestes.

O grande desafio no Estados de Direito Democráticos traduz-se na resolução da problemática de como fazer um combate preventivo a um crime antes de ele ocorrer, considerando que o nosso sistema penal assenta no facto e não no agente[115]. O autor refere ainda que no caso de uma ameaça terrorista, os agentes que perpetuam atos preparatórios e instrumentais, ou seja, que antecedem de facto e em concreto aquele tipo de crime, a estratégia seguida pelo legislador tem sido o de recuar a tutela penal o mais possível[116]. Nomeadamente, na antecipação da obrigação de criminalização das condutas de incitamento público, de recrutamento, de fornecimento ou receção de treino, de deslocações para fins de terrorismo e de financiamento.

Outros autores, num segmento mais humanista, como é o caso de Manuel Valente, fala-nos de uma mudança de paradigma penal [material e processual], referindo um aumento das molduras penais abstratas nomeadamente no âmbito da punibilidade dos atos preparatórios e dos atos de execução, como também na consequente diminuição das garantias processuais penais, sem prévio controlo e autorização das autoridades judiciárias. O autor refere "uma «despersonalização» do autor do crime, convertendo o cidadão em inimigo ou em "coisa" reduzindo-o quase a uma «não-pessoa»"[117].

É verdade que devemos assumir cada vez mais um Direito (penal/processual) garantista e humanista, em que enaltecemos e fomentamos uma cooperação-social, no sentido de em vez de impormos uma determinada conduta individual ou condenar *à priori* uma ação pelo facto de um individuo ter-se resignado a um comportamento desviante das normas assumidas como

[114] Cf. António Manuel Abrantes, Academia Edu [em linha]. Revista do Ministério Público 156 (Out. – Dez. 2018). P. 157-208- [Consult.20 Abr. 2021]. O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações. Disponível em https://arquitectura-ucp.academia.edu/Ant%C3%B3nioManuelAbrantes.

[115] *Idem*, p.182 e 183. Sobre este assunto ver também Figueiredo Dias, Direito Penal, Tomo I, 2ª ed. 2012, p.235. Aqui o autor releva um duplo sentido: «no que toda a regulamentação jurídico-penal liga a punibilidade a tipos de factos singulares e à sua natureza, não a tipos de agentes e às caraterísticas da sua personalidade; e também no do que as sanções aplicadas ao agente constituem consequências daqueles factos singulares e neles se fundamentam, não são formas de reação contra uma certa personalidade ou tipo de personalidade. (…) constituindo em última análise, que a construção dogmática do conceito de crime é afinal a construção do conceito de facto punível».

[116] Vejamos no caso europeu a Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho de 15 de Março de 2017 que visou a harmonização das legislações penais dos Estados-Membros em matéria de combate ao terrorismo.

[117] Cf. Manuel Guedes Valente, Direito Penal do Inimigo e o Terrorismo: O «Progresso ao Retrocesso». 2ªed. Reimp. Edições Almedina, S.A, 2018, *op. cit*. p. 82 e 83. Ver ainda nota n.º 149 da obra.

válidas, "uma conduta exemplar numa determinada sociedade", devemos apelar sim, insistentemente, a uma consciência coletiva capaz de figurar um entendimento razoável da maioria e "espicaçar" as mentes daqueles que julgam não terem qualquer responsabilidade comunitária.

Também não seria despiciendo afirmar que existe uma tendência securitária, na medida em que, a segurança tornou-se o valor imperial para a aquisição da liberdade. Mas, não queremos suportar este enviesamento dogmático que se aproximaria da construção de um direito penal do inimigo de Günther Jakobs. Não menos relevante seria referir, a teoria do contrato social preconizado por Rosseau, que enunciava "o homem ao deixar o estado de natureza para aderir ao estado social deixando-se de motivar pelo instinto, assumindo a justiça como dínamo das suas decisões. O homem ao aderir ao contrato social cede a sua liberdade natural e um direito ilimitado a tudo aquilo que lhe é necessário e ganha a liberdade civil e a propriedade de tudo o que possui"[118]. Assim, torna-se imperativo fazer uma relação com os valores constitucionais dentro de um estado de direito democrático primado pela dignidade da pessoa humana.

Deste modo "as caraterísticas próximas da conceção do direito penal do inimigo teorizado por Günther Jakobs, têm sido fundadamente criticadas pela doutrina constitucionalista e penalista, por se revelar incompatível como vários princípios basilares de direito constitucional nomeadamente o princípio da dignidade humana, o princípio do Estado de Direito Democrático e o princípio da proporcionalidade (em toda a sua latitude - latu sensu e stricto sensu)"[119].

Por muito que o legislador queira ou tente recuar na tutela penal até aos atos que precedem um atentado terrorista, como refere Manuel Abrantes, não deixa de haver um momento em que tal antecipação deixa de ser legítima e até mesmo possível, no plano prático[120]. Não impende, contudo, de vermos estatuído à semelhança do artigo 272.º da CRP, um regime apropriado que admita a intervenção e as delimitações dos Serviços de Informações. Julgamos não ser assim tão inócuo fazer uma leitura desta natureza, uma vez que a própria LSI na al. e), n.º 2 do art.25.º incorpora o serviço de informações de segurança na sua estrutura de organismos públicos e concorrem para garantir a segurança interna. Como refere José Fontes, apesar de os Serviços de Informações não puderem exercer funções policiais, estando expressamente vedados pela

[118] Cf. Manuel Guedes Valente, Direito Penal do Inimigo e o Terrorismo: O «Progresso ao Retrocesso». 2ªed. Almedina, 2018, *op. cit.* p. 47 (ver nota 77) *apud* Rosseau. Contrato social. Tradução do francês de Manuel João Pires. 2012, pp.57,66,69-70.

[119] Cf. António Manuel Abrantes [Consult.25 Jan. 2021]. O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações. Disponível em https://arquitectura-ucp.academia.edu/Ant%C3%B3nioManuelAbrantes, *op.cit.* p. 183.

[120] *Idem, op.cit.,* p.184.

sua própria Lei-quadro (Art.º 4.º) [121], e da Lei Orgânica do SGSIRP (Art.º 6.º)[122], "materialmente desempenham funções de autoridade em segurança, por equivalência ou por lógica de paridade e função e a estrutura – independentemente da realidade nominativa conjuntural – deveria ter, também, referência e dignidade constitucionais"[123].

Não obstante este entendimento, também foi justificado na declaração de voto da Juiz Conselheira Maria Amaral no Ac. n.º 403/2015 do TC, que a existência de Serviços de Informações visa, num Estado de Direito Democrático, tutelar bens jurídicos, coletivos e individuais, que são valorados constitucionalmente num lugar não menor que os bens tutelados por normas penais incriminadoras.

De acordo ainda, com as normas que enformam o sistema de organização dos serviços de informações e, considerando as suas competências, não decorre uma ameaça lesiva da liberdade individual que seja, pela sua intensidade, equiparável aquela que emerge, inevitavelmente, da aplicação das normas de processo criminal. Havendo por isso, uma afinidade valorativa entre as finalidades prosseguidas pelos serviços de informações e as normas penais incriminadoras – aferindo-se que se houvesse sido outra a posição conceptual e metódica de que se partisse, que a autorização constitucional para restringir a inviolabilidade das telecomunicações em «matéria de processo criminal» se estenderia, por maioria de razão, aos Serviços de Informações. Mas não é este o entendimento daquele tribunal e muito menos da doutrina, que por diversas razões impede que se faça uma «interpretação extensiva» do texto da norma e isoladamente. Um dos significados político-constitucionais da reserva de competência sob a forma de leis orgânicas é neste caso controlar o regime do sistema de informações da república portuguesa[124].

Não menosprezando outros traços jurídico-constitucionais caraterizadores das leis orgânicas, para além de estarem vinculadas pelo princípio da tipicidade, observa-se também o princípio da exclusividade em razão da matéria, consagrando igualmente princípios vetores de um determinado regime jurídico. No caso do regime jurídico do SIRP (LQSIRP) estabelece-se as grandes linhas orientadoras e princípios da atividade daquele organismo. Porquanto limita no caso em apreço a uma limitação material e formal de quaisquer atividades de pesquisa, processamento e difusão de informação que envolvam ameaça ou ofensa aos direitos, liberdades

[121] Da Lei n.º 30/84, de 05 de setembro, e conforme a quinta alteração, Lei Orgânica n.º 4/2014, de 13 de Agosto.
[122] Da Lei n.º 9/2007, de 19 de fevereiro, relativo à orgânica do Secretário-Geral do Sistema de Informações da República Portuguesa (SGSIRP), do Serviço de Informações e Segurança (SIS) e Serviço de Informações e Defesa (SIED).
[123] Cf. José Fontes, A Constituição e os Serviços de Informações. "Segurança e Defesa" [Em linha]. Nº 15 (out.-dez. 2010), p.2. [Consult.26 Jun.2021]. Repositório aberto. Universidade Aberta. Disponível em https://repositorioaberto.uab.pt/handle/10400.2/1788
[124] Cf. José J. Gomes Canotilho – Direito Constitucional e Teoria da Constituição. 7ª Ed. 17ª (Reimp). Coimbra. *op.cit*., p.750 e 751.

e garantias previstos na lei fundamental. Talvez seja impressão, mas não estamos perante mesmo uma certa contradição com o que verdadeiramente um organismo desta natureza é suposto fazer? A verdade é que aquele regime se encontra desadequado à realidade hodierna, urgindo fazer uma alteração profunda dos vetores, dos princípios e de todos os contornos necessários para a salvaguarda dos interesses nacionais, em conformidade com os princípios de direito internacional, da separação e interdependência de poderes dos órgãos de soberania, bem como, pelo regular funcionamento das instituições democráticas e no respeito e garantia dos direitos, liberdades e garantias fundamentais dos cidadãos no quadro do Estado de Direito Democrático.

Não é demais relembrar neste contexto que não é nossa intenção justificar a restrição de direitos fundamentais em prol, de que tudo se justifica em nome da segurança, reavivando a memória de um estado politicamente fragilizado e corroborado com ideais totalitários e, por isso, propensos a políticas de segurança abusivas de direitos fundamentais dos cidadãos. Em consequência da evolução tecnológica, económica e social "não sendo estanque" cada vez mais assistimos a uma mudança do paradigma securitário.

Alguns autores defendem a ilegitimidade que os serviços de informações pugnam a fim concretizar as suas atribuições, nomeadamente no acesso aos metadados. Alegando que não são OPC[125], defendendo que existem outros mecanismos por parte dos operadores do Estado, estes por um lado, "integram um estado de necessidade justificante, como causa supralegal de justificação"[126] por outro, "os órgãos de polícia criminal aplicam as medidas cautelares e de polícia"[127]. Desta forma, a função dos serviços de informações não é uma função de polícia, como se afere da própria Constituição e das respetivas leis orgânicas e como adiante iremos abordar, uma vez que também podemos falar das denominadas "sanções inteligentes", impostas pelo Conselho de Segurança das Nações Unidas (CSNU), aplicadas pelos Estados no plano interno para fazer face às ameaças e atividades terroristas.[128] Posto isto também não se refere a separação de poderes, e aqui no que respeita às funções a que cada organismo está incumbido. Julgamos que a linha é bastante ténue quando falamos da atuação quer dos OPC, e neste caso

[125] Facto que decorre expressamente da lei como já foi referido.
[126] Cf. Manuel Guedes Valente, Direito Processual Penal: Da Sociedade Internético-Personocêntrica. Lisboa. 2020. *Op.cit.,* p. 169.
[127] *Ibidem*.
[128] Cf. Manuel Abrantes, [Consult.25 Jan. 2021]. O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações. Disponível em https://arquitectura-ucp.academia.edu/Ant%C3%B3nioManuelAbrantes, *op.cit.* p. 184. O autor refere ainda no âmbito da aplicação de sanções inteligentes à margem do processo penal de três diferentes medidas restritivas sobre indivíduos e entidades suspeitos de envolvimento em atividades terroristas: 1) o congelamento de todos os bens; 2) a interdição da sua entrada ou trânsito no território dos Estados; 3) a interdição de venda de armas ou de material relacionado.

em particular da PJ, que é o órgão de polícia criminal com competência reservada, conforme disposto da al. l) do n.º 2 do art.º 7º da LOIC, quer dos serviços de informações aquando referimo-nos de "inteligência policial" (o primeiro) versos "inteligência de investigação" (o segundo).

Abordando a perspetiva dogmático-constitucional quanto à admissão de interceção das comunicações privadas com a finalidade exclusivamente preventiva, também é de referir que neste domínio, as Constituições atuais na maioria dos Estados Membros da UE encontram-se preparadas para a admissão de interceção das referidas comunicações privadas. A Constituição espanhola, prevê, no seu n.º 3 do artigo 18.º, que "é garantido o segredo das comunicações e, em especial, das telefónicas, postais e telegráficas, salvo resolução judicial". Já na Constituição italiana, no seu n.º 2 do artigo 15.º, estabelece que "a liberdade e o segredo da correspondência e o de qualquer comunicação são invioláveis, contudo prevê ainda que a sua limitação pode ocorrer por determinação da autoridade judiciária, sendo mantidas as garantidas estabelecidas por lei". Neste sentido a Lei Fundamental da República Federal da Alemanha é mais permissiva ao estabelecer, no seu n.º 2 do artigo 10.º, que "as limitações só podem ser ordenadas em virtude da lei e tiver por finalidade proteger a ordem fundamental livre e democrática ou a existência e segurança da Federação e de um Estado Federado, pode a Lei determinar que a limitação não seja levada ao conhecimento do individuo atingido e que, em vez de se se seguir a via judiciaria, o controlo seja realizado por órgãos principais e auxiliares, nomeados pelos representantes do povo".

Tendo em conta que o direito penal tem uma natureza essencialmente reativa e não uma natureza preventiva é ainda necessário que o acesso seja feito no âmbito de um processo criminal em curso, daí operar dentro de um processo penal que só se inicia após ter recebido a notícia de um crime e não antes de um crime ocorrer.[129]

É evidente que uma atuação investigatória processualizada e publicizada, na forma de inquérito preliminar ou de instrução, não só salvaguarda a liberdade e segurança jurídica como dá as garantias necessárias para que a prova não seja contaminada e que sejam igualmente salvaguardados os direitos fundamentais dos cidadãos. Analogamente aos procedimentos preventivos previstos na lei fundamental que enquadra "*ações de prevenção"* no direito constitucional de polícia (art.272.º), a atividade relativa à produção de informações pelo SIRP com a finalidade de prevenir crimes contra a segurança do Estado (terrorismo "transnacional",

[129] Cf. Manuel Abrantes, [Consult. 2 julho. 2021]. O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações. Disponível em https://arquitectura-ucp.academia.edu/Ant%C3%B3nioManuelAbrantes, *op.cit.* p. 194.

espionagem, criminalidade altamente organizada), soberania nacional e realização do Estado de Direito, poderia ser abrangida por esse preceito.[130] Para diversos autores, a par do entendimento do TC, as ações de prevenção do SIRP são considerados procedimentos administrativos[131] devendo respeitar os direitos, liberdades e garantias, não obedecendo aos princípios jurídico-constitucionais conformadores do processo penal (cf. art.º 32 da CRP).[132]

Uma vez mais levantamos a questão, se aquele entendimento se revela adequado á realidade e se de facto não seria ultrapassado por entendimento diverso, como por exemplo assumir que os órgãos que integram o SIRP (no caso, o SIS), serem considerados como organismos públicos que concorrem para garantir a segurança interna, como decorre da própria Lei de Segurança Interna (al. f) n.º 2 do artigo 25.º). Compreendemos que talvez ainda estejamos sobre o efeito e rescaldo das ações praticadas pela então designada polícia política[133], mas talvez deveria chegar o momento de ultrapassar o fantasma de que os serviços de informações, apesar de serem apelidados de "secretos", o não são, porque só existem e agem dentro da juridicidade, e não fora dela.[134]

Constatamos durante esta investigação e até recordamos aos académicos, que se à Polícia de Segurança Pública e Guarda Nacional Republicana estão incumbidos as competências e áreas de atuação (técnica, operacional e territorial) nas respetivas Leis Orgânicas, à Polícia Judiciária que assenta essencialmente na coadjuvação às magistraturas (em especial à Magistratura do Ministério Público) no âmbito da investigação da criminalidade mais grave, organizada e complexa (bem como ao fenómeno do terrorismo), que reclama uma adequada e eficaz resposta por parte deste organismo do Estado[135], à Polícia Marítima que se circunscreve maioritariamente na área e jurisdição marítima nacional, designadamente em espaços integrantes do domínio público marítimo (DPM), sem prejuízo do seu estatuto enquanto órgão de polícia criminal nas áreas de jurisdição da Autoridade Marítima Nacional (AMN). É ainda, atribuída, à Polícia Municipal uma forma de descentralização e desconcentração de funções

[130] Cf. Ac.TC n.º 403/2015 de 17/09/2015, (Lino Rodrigues Ribeiro), pp. 8245-8279. [Em linha]. (Consult. 30 Jun. 2021). Disponível em https://dre.pt/home/-/dre/70300353/details/maximized?p_auth=OsYd65lz. (Ponto 19), apud Jorge Miranda e Rui Medeiros, *Op.cit.* pp. 663 e 664.
[131] Cf. Art.º 5.º do Decreto n.º 426/XII.
[132] *Idem* (Ponto 19).
[133] Referimo-nos não só à PIDE e seus predecessores como a DGS, o SDCI mas também da própria DINFO (a designada Repartição de Pesquisa Coberta). Para melhor ilustração sobre a DINFO ver também Fernando Cavaleiro Ângelo, Dinfo: "A queda do último serviço secreto militar". Casa das Letras, 2020.
[134] Cf. Bacelar Gouveia, Direito da Segurança. Cidadania, Soberania e Cosmopolitismo, 1ª ed., Almedina, 2018, *Op.cit.* p. 697, apud Paulo Otero, Manual de Direito Administrativo, I, pp.216 e217.
[135] Como decorre da Nova Estrutura Organizacional da Polícia Judiciária através do Decreto-lei n.º 137/2019, de 13 de setembro (contém a retificação n.º 55/2019, de 23 de outubro)

administrativas[136] das tarefas incumbidas ao Estado local e central. Não seria despiciendo afirmarmos que a previsão normativa constitucional de tão importante organismo do Estado como é o SIRP, deveria encontrar de forma expressa, inequívoca e precisa, a sua fonte de legitimação na Constituição.

Como procurámos demonstrar no ponto dois deste capítulo, quanto à interpretação do n.º 4 do artigo 34.º da Constituição, efetivamente o legislador constitucional "não equacionou provavelmente a necessidade, de um dia existir, a necessidade de combater determinadas ameaças logo num plano preventivo, com recurso a medidas restritivas que, tradicionalmente, apenas seriam de admitir no âmbito de um processo penal"[137].

Assim, julgamos que uma das soluções, seria atualizar o texto da norma constitucional e consagrando, desta forma, uma fonte legítima que mencionasse aquele organismo enquanto órgão relevante na garantia da segurança interna e externa do Estado Português, em estreita colaboração com os órgãos competentes de investigação criminal e demais órgãos administrativos e judiciários.

5. Relevância das Políticas Criminais face à obediência vinculada das garantias constitucionais.

Como refere Manuel Valente, ao direito penal reserva-se o desiderato de limitar a ação punitiva do Estado, e de tutelar interesses essenciais da comunidade, que a ordem jurídica transforma em bens jurídicos dignos de tutela penal. Este autor refere-se a uma «hipertrofia legislativa do Direito penal que tudo quer tutelar e nada tutela», gerando desta forma «uma popularização e vulgarização do Direito Penal, acompanhado pelos fenómenos da securitização e do justicialismo»[138]. Nesta senda, julgamos haver uma certa semelhança no direito em geral - uma massificação de legislação avulsa que afasta o cidadão "comum" de uma consulta breve e simplificada, bem como das responsabilidades morais e éticas - noutro prisma, torna-se

[136] Na manutenção da tranquilidade pública e na proteção das comunidades, conforme o disposto do n.º 3 do artigo 237.º da CRP.
[137] Cf. Manuel Abrantes, O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações. Disponível em https://arquitectura-ucp.academia.edu/Ant%C3%B3nioManuelAbrantes, *op.cit.*, p. 195.
[138]Cf. Manuel Guedes Valente, Direito Penal do Inimigo e o Terrorismo: O «Progresso ao Retrocesso». 2ªed. Reimp. Almedina, 2018, *op.cit*. pp.19-20.

evidente a manifestação do fenómeno da securitização, dada a escalada de um outro fenómeno como o é o do terrorismo.

Não cabendo no âmbito desta investigação analisar as teorias da "criminologia" dos diversos autores, que exaustivamente esboçam uma investigação profunda e vital para a compreensão do fenómeno do terrorismo, reservamos apenas uma breve alusão ao cidadão delinquente.

Assistimos a uma relativa descredibilização generalizada do direito penal na comunidade, com o rumor sempre presente de que não se previne e não se consegue responsabilizar os agentes do crime altamente especializado, violento, organizado e transnacional, não deverá existir por este motivo a tentação de se socorrer de medidas restritivas de direitos e liberdades que ferem e colidem grandemente com os direitos fundamentais dos cidadãos.

O recurso à atuação do Estado, numa fase ainda premonitória de um crime, de mecanismos suficientes a prevenirem e atuarem antes da notícia de um crime sugere uma certa "perversidade" e abuso de poderes, que em última análise atribuiria a organismos do estado uma competência ilimitada e perigosa que levaria a um «retrocesso» do Direito Penal.

Percorreu-se um longo caminho até chegar ao Estado de Direito. De entre as diversas abordagens das correntes filosóficas, como o contratualismo, o iluminismo ou o individualismo, destaca-se a proliferação das declarações de direitos, que reconhecem um limiar mínimo de respeito pela dignidade da pessoa humana.

Como refere Manuel Valente[139], não existem sistemas perfeitos e tendo em consideração as diversas correntes doutrinárias do crime dos quais destacamos, por um lado, a corrente que tendo em conta as caraterísticas físicas, psíquicas, genéticas e raciais de um indivíduo, este, nasce predisposto para o crime. No entanto noutra linha de raciocínio, defende-se a hereditariedade como linha de transmissão de tendências criminosas, e há ainda quem defenda, que o terrorista, o traficante de droga, o traficante de armas e de seres humanos, os membros de organizações de crime organizado, são considerados como delinquentes de elevada perigosidade e por isso, nefastos à sociedade, devendo submeter-se à construção jurídico-criminal de inimigo. Coloca-se a questão: – acompanhando o autor - *de ser esta a legitimidade que se quer entregar ao Ius puniendi do estado?*

A realização e adoção de políticas criminais[140] pro-securitárias destruiu as "fronteiras tradicionais do Estado de Direito entre as autoridades responsáveis pela persecução penal,

[139] De entre as diversas correntes de escolas face aos sistemas políticos e políticas criminais (Valente, 2018, p. 24 a 27) in Direito Penal do Inimigo e o Terrorismo. O «Progresso ao Retrocesso»; Figueiredo Dias e Manuel Andrade - Teorias bioantropológicas, in O homem delinquente e a Sociedade Criminógena, pp.170 a 176.

[140] Cf. Manuel Valente, Direito Penal – Fundamentos Político Criminais, p.25 e 26; refere a visão preconizada por Luigi Ferrajoli, de uma "Democracia Constitucional", subordinando a política criminal á lógica do

polícia, serviços secretos e FA de modo a legitimar intervenções que são, simultaneamente, persecução penal, prevenção policial e guerra"[141].

Os desafios colocados pela ameaça terrorista têm deixado notoriamente claras limitações do direito penal para intervir de forma legítima e eficaz no seu combate, tendo em consideração que este ramo do direito tem uma natureza essencialmente reativa e não, para a prevenção de crimes; "daí operar dentro de um processo penal que só se inicia após ter recebida a notícia de um crime e não antes de um crime ocorrer"[142]

Não obstante, cristalizaram-se instrumentos jurídicos como a DUDH, a CEDHLF e a CDFUE, em que a centralização do poder político e a consagração dos direitos fundamentais revelam a preocupação de proteger a pessoa face ao Estado[143]. Neste sentido, a implementação de mecanismos de limitação do poder do Estado, destinados a assegurar a supervisão da sua atuação e a sua conformidade com o direito vigente, revelam-se imperativos.

Importa reiterar a relevância da adoção de medidas, políticas criminais, de um equilíbrio entre um direito penal material, processual e o constitucionalismo democrático. Será necessário, reduzir o desiderato decorrente da prossecução dos valores de um Estado de Direito sob escopo e afirmação da liberdade do ser humano e a ação preventiva/ repressiva do Estado, não olvidando que a justiça tem como objetivo substituir a violência, "a segurança é o resultado da liberdade e da justiça e não o resultado da restrição ilimitada dos direitos fundamentais"[144].

Na perspetiva jurídico-penal constitucional, é certo que a prossecução e as finalidades dos serviços de informações decorrentes do artigo 2.º da LOSIRP[145], reconhece que "aos serviços incube assegurar, no respeito da Constituição e da Lei, a produção de informações necessárias à preservação da segurança interna e externa, bem como à independência e interesses nacionais e á unidade e integridade do Estado", circunscrevem-se nestes termos e fora do âmbito de um processo penal. Ou seja, no que concerne à investigação criminal em concreto, as diligências que daqui decorrem sob a orientação do MP deixam este organismo do Estado à margem de qualquer intervenção num processo penal. Apesar do SIS (e apenas o SIS, deixando de fora o SIED) contemplar as forças e serviços de segurança, como podemos constatar no artigo 25.º da LSI e também mencionar que o controlo das comunicações se encontra sob a égide da Polícia

constitucionalismo e do garantismo democrático, que reside na submissão de todo o poder – político-legislativo, judicial e executivo – aos limites impostos pela constituição.

[141] Cf. Manuel Valente, Direito Penal do Inimigo e o Terrorismo. O «Progresso ao Retrocesso», p.37.

[142] Cf. Manuel Abrantes, O Acesso aos Dados de Tráfego pelos Serviços de informações à Luz do Direito Fundamental à Inviolabilidade das Comunicações. [Revista do Ministério Público 156: Outubro: Dezembro 2018

[143] Cf. Sofia Casimiro, Liberdade e Segurança no Combate ao Terrorismo: Quis Custodiet ipsos custodes? Uma perspetiva jurídica, *Op.cit.*, pp.24 e 25. [Publicações IDN, Nação e Defesa nº 152: Terrorismo e Violência Politíca]

[144] Cf. Manuel Guedes Valente, Direito Penal – Fundamentos Político Criminais, *op.cit,* p.27

[145] Em conformidade com a última alteração da LOSIRP – Lei Orgânica n.º4/2014, 13/08.

Judiciária, mediante o controlo judicial (artigo 27.º da LSI), não se justifica a resistência em dotar os Serviços de Informações da República Portuguesa de um quadro legal digno e capaz de responder as exigências a que está incumbido. Mencionamos anteriormente a "resistência" pelo simples facto de ter havido já dois acórdãos do Tribunal Constitucional - respetivamente em 2015 e outro em 2019[146], que obtiveram votos desfavoráveis relativamente ao acesso aos metadados. Por um lado, o Ac. de 2015, resultante do pedido de apreciação por parte do Presidente da República da conformidade constitucional do n.º 2 do artigo 78.º do Decreto n.º 426/XII, assentava no acesso à "informação bancária, fiscal, a dados de tráfego, de localização ou outros dados conexos de comunicações (…) identificar o equipamento de telecomunicações ou a sua localização, sempre que sejam necessários, adequados e proporcionais (…) para o cumprimento das atribuições legais dos serviços (…) mediante a autorização prévia e obrigatória da Comissão de Controlo Prévio…", resultando posteriormente de uma evolução e profunda ponderação destinada a ultrapassar o juízo de inconstitucionalidade aí expresso através da Lei Orgânica n.º 4/2017[147]. Já o Ac. de 2019, do qual trinta e cinco deputados da Assembleia da República, pediram a apreciação e declaração de inconstitucionalidade agora das normas constantes nos artigos 3.º e 4.º da Lei Orgânica n.º 4/2017, de 25 de agosto, que aprovou e regulou o procedimento especial de acesso a dados de telecomunicações e Internet pelos oficiais de informações do SIS e do SIED.

Deixando para oportuna apreciação, não podemos deixar de ficar perplexos pela tentativa de se encontrar a solução de pelo menos dois, dos problemas suscitados. Quanto à outra questão suscitada nos doutos acórdãos, julgamos[148] que esta que poderia ser ultrapassado através de uma interpretação extensiva do n.º 4 do artigo. 34º da CRP, incluindo os Serviços no leque de atores (Forças e serviços de segurança – conforme decorre da alínea e) do nº 2 do artigo 25º da LSI – que concorrem para garantir a segurança interna) que poderiam auxiliar no âmbito de um

[146] Respetivamente, Lino Rodrigues. – Acórdão do Tribunal Constitucional com o n.º 403/2015; e, Lino Rodrigues. – Acórdão do Tribunal Constitucional com o n.º 464/2019.

[147] Aqui acompanhamos a visão de António Manuel Abrantes de acordo com o seu artigo – o acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações - publicado na RMP 156: Outubro: Dezembro 2018, 177, quando constatou na resolução efetiva, de pelo menos dois dos três problemas de constitucionalidade enunciados no Ac.n.º403/2015 do TC.

[148] Conforme refere Mariana Machado, o facto de os Serviços, na sua génese, atuarem á margem de um processo criminal (antes de um auto de notícia), impede e restringe a eficácia daqueles. Conforme referimos os diplomas legais em vigor, nomeadamente a LSI, por uma lado no seu artigo 25º «trás os serviços para o jogo de coordenação das múltiplas entidades encarregues de assegurar a segurança interna, sem que, contudo, se lhes possa atribuir idoneidade para, alterar a materialidade das funções prosseguidas, tal como definidas na lei orgânica e na Lei-quadro do SIRP», por outro lado, é-lhes expressamente vedado por estes mesmos diplomas, os respetivos limites da sua atividade incorrendo até numa certa contrariedade funcional e terminológica. Facto é a de que «a atuação das forças policiais e do Mº Pº inicia-se, apenas, a partir da notícia do crime. Porém, evidentemente que, numa sociedade global há riscos e ameaças que importa acompanhar e supervisionar, antes de se materializarem».

processo criminal. Não obstante, em nosso entendimento aquele problema de constitucionalidade que a Lei Orgânica n.º4/2017 continua a suscitar, prende-se com o facto de o acesso aos dados de tráfego ser feito fora do âmbito de um processo penal em curso, contrariando aparentemente, o âmbito da autorização constitucional decorrente da parte final do n.º 4 do artigo 34.º da CRP.

Esta abordagem revela-se necessária, uma vez que reconhecemos o desprezo que se tem revelado na "urgente" renovação do regime jurídico do SIRP, de forma a consolidar mecanismos para evitar determinados crimes, com particular ênfase na sua prevenção e repressão. Também será necessário atribuir meios e instrumentos necessários ao SIRP para a prossecução das suas atribuições - com maior eficácia, e, ao mesmo tempo, ver salvaguardado a sua atuação por meios legais, controlo judicial e constitucionalmente protegidos.

De forma sucinta a análise da Proposta de Lei n.º 46/XIV/1.ª, que prevê bienalmente, a condução da política criminal, mediante a definição de objetivos, prioridades e orientações em matéria de prevenção da criminalidade, investigação criminal, ação penal e execução de penas e medidas de segurança, esta culminou na aprovação da Lei n.º 55/2020, em cumprimento da Lei n.º 17/2006, de 23 de maio, que aprova a Lei-Quadro da Política Criminal. Em conformidade com aquela proposta, na exposição de motivos, num quadro que tem em consideração os dados do RASI de 2019, as análises prospetivas internacionais, designadamente da EUROPOL, bem como na lógica de continuidade face ao diploma do último biénio (2017-2019), está integrada num plano de prevenção da criminalidade, programas e planos de segurança e de policiamento, destinados a proteger vítimas especialmente vulneráveis e a controlar as fontes de perigo, nomeadamente no que refere às associações criminosas e organizações terroristas, bem com aos meios especialmente complexos, como a informática e a internet.

Resultante desta proposta, como referimos, foram definidos os objetivos, prioridades e orientações de política criminal para o biénio de 2020-2022, que na al. a) do artigo 3.º contempla entre os seus objetivos específicos, a cibercriminalidade, o terrorismo e o seu financiamento e as organizações terroristas.

Vejamos ainda, as prioridades definidas no artigo 4º "*crimes de prevenção prioritária*", seguindo a ordem sistemática do diploma, coloca os crimes de terrorismo de imediato na al. a) e na sua alínea d) a cibercriminalidade, incluindo os crimes cometidos por meio de um sistema informático ou de comunicação. Talvez não seja despropositado afirmar que neste quadro o próprio diploma reforça a *atenção* dada a este tipo de crimes. Neste sentido e no cumprimento das atribuições dos Serviços, dada a complexidade de obtenção de prova, não menosprezando

as atribuições e competências das diversas forças policiais, seria uma mais valia delegar alguma autonomia e liberdade de ação, dentro de um sistema de controlo judiciário rigoroso, como fora previsto pelo Decreto n.º 426/XII através dos vários órgãos de controlo. Estes órgãos que fora de um contexto de necessidade premente poderiam inclusive estar sob um crivo Parlamentar, sem prejuízo do grau de complexidade e operacionalidade que determinadas missões exigem, bem como do sigilo de determinadas informações, sendo estas reservadas quanto à sua publicação e divulgação, devendo restringir-se aos órgãos estritamente necessários.

Como refere Joanisval Gonçalves[149] "não dispor de órgãos de informações pode deixar um Estado em situação de grande vulnerabilidade (…) da dicotomia necessidade versus risco da inteligência para a democracia, tem-se no controle público dos serviços de inteligência (…), o controle eficiente e eficaz é que garantirá que os serviços de inteligência operem dentro dos princípios democráticos e realizem uma atividade verdadeiramente em benefício do Estado e da Sociedade"[150].

Na abordagem desta questão[151], presume-se que a sombra de um regime totalitário que terminou há menos de meio século em Portugal, ainda prevaleça não sendo o suficiente para impulsionar uma efetiva alteração ao regime de atuação dos serviços.

Apesar do nosso país ter ficado imune aos atentados terroristas que ocorreram em outros países, refere-nos Júlio Pereira[152] "sem interceção de comunicações a prevenção do terrorismo chegará tarde demais", pois em certa medida verificamos que a iniciativa para a produção de legislação mais intrusiva neste domínio, têm-se revelado reativa. Sugerindo a possibilidade de um alargamento de poderes da PJ, por forma a abranger o recurso a esse meio com vista à produção de informações. Defendemos que de certa forma fere a matriz dos Serviços, uma vez que estes foram estruturados com base numa clara separação entre a atividade de polícia e a atividade de recolha de informações[153].

---

[149]Cf. Joanisval Brito Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, *op.cit*. p. 136

[150] *Idem*, p.72, a missão natural dos serviços de inteligência doméstica é reunir, processar e produzir conhecimentos relacionados à segurança interna, de modo a proteger a sociedade, o Estado e as instituições. Referindo-se à produção de conhecimentos para prevenção e neutralização de ameaças em áreas como por exemplo: a espionagem, o terrorismo, o crime organizado e crimes cibernéticos etc..

[151]Cfr. Proposta de Lei n.º79/XIII/2.ª [Consult. 06 Mar.2021. Disponível em https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=41364, do Governo, e no Projeto de Lei n.º 480/XIII/2ª [Consult. 06 Mar.2021. Disponível em https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=41212], da iniciativa de dezoito deputados do Grupo Parlamentar do CDS/PP. Com o propósito de fazer a alteração legislativa à LQSIRP (Lei n.º 30/84), sendo este último, aprovado em votação final, com os votos favoráveis do PSD, PS e CDS-PP, votos contra do BE,PCP e PEV e abstenção do PAN.

[152] Cf. Júlio Pereira - Vigilância Vídeo, Interceção Preventiva de Comunicações e Contraterrorismo. Nação e Defesa, Terrorismo e Violência Política. Ed. Instituto de Defesa Nacional, 2019, p.46.

[153] Cf. Júlio Pereira - Vigilância Vídeo, Interceção Preventiva de Comunicações e Contraterrorismo. Nação e Defesa, Terrorismo e Violência Política. Ed. Instituto de Defesa Nacional, 2019, pp.39-47

Por último, a título de curiosidade, e não menos relevante são os esforços que a UE tem empenhado no combate à prevenção de crimes como o terrorismo, com a criação do EU INTCEN[154], bem como outros mecanismos necessários à sua prossecução, designadamente atuando preventivamente na antecipação de crimes. Na esfera da cibercriminalidade têm-se registado de forma reiterada alvos institucionais e não institucionais, como por exemplo, centro de dados de vários organismos estatais, infraestruturas de telecomunicações, hospitais, seguradoras, universidades e escritórios de advogados, desta forma terão de se encontrar mecanismos legais mais eficazes sem prejuízo dos valores e princípios de um Estado de Direito Democrático.

Importa fazer uma abordagem relativa aos conceitos que comumente definem os designados "metadados" e que muitas das vezes não se revelam exatos, ou uniformes no seu conceito, considerando os vários diplomas nacionais e comunitários. Para além das atribuições a que está incumbido um serviço de informações também destacamos as funções que se espera de um organismo de inteligência do Seculo XXI, num Estado de Direito Democrático, bem como do aparelho de controlo que não pode ser menosprezado, tendo em conta a natureza e objeto que se trata, fomentando um rigoroso e rígido controlo, fiscalização – interno e externo – dos organismos de segurança do Estado. Espera-se que estes operem dentro dos preceitos constitucionais e legais, não desmerecendo necessariamente um controlo parlamentar a par de outros mecanismos de fiscalização, não só para que se evitem abusos por parte daqueles organismos, mas também para modificar a sua cultura organizacional e a perceção que a sociedade civil tem destas instituições, dos seus agentes e da atividade que exercem.

[154] Veja-se por exemplo o Clube de Berna (CdB), num quadro de cooperação institucional dos vários serviços de inteligência (grupo este, informal) integrado por todos os países da União Europeia, a Noruega e a Suíça. A este propósito veja-se o caso em 2015, do qual participou Ismaël Omar Mostefaï, um dos terroristas suicidas do Bataclan. [em linha] Disponível em https://www.dn.pt/portugal/secretas-portuguesas-e-europeias-ativam-grupo-de-elite-4891599.html

CAPÍTULO II – OS METADADOS E O ACESSO À INFORMAÇÃO. O CONTROLO EFETIVIVO E OS PRINCÍPIOS NORTEADORES DA ATIVIDADE DE INTELIGÊNCIA.

1. Desafios no acesso aos metadados numa "era digital", no combate á "nova criminalidade".

Estando nós a atravessar, a designada quarta revolução industrial, e como refere Rodrigo Ziembowicz no seu recente artigo "Estimular e proteger o desenvolvimento económico diante da criminalidade organizada", "a sociedade encontra-se em um período de relevantes (e acelaradas) metamorfoses a nível mundial, com enorme repercussão nas dinâmicas económicas, sociais e Políticas. (…) Trazendo consigo avanços relevantes para a sociedade, mas também resultando em dificuldades de controlo estatal"[155].

Impondo ainda ao Estado, para além do dever de assegurar, constitucionalmente, a segurança dos seus cidadãos, encontrar um ponto de equilíbrio dos interesses conflituantes entre a criminalidade "geral" e a grande e nova criminalidade, como é o terrorismo e a criminalidade organizada.[156]

A inviolabilidade das comunicações privadas, previstas no artigo 34.º da Constituição da República Portuguesa, veio assegurar que qualquer cidadão pudesse estabelecer uma comunicação em segurança e que ninguém interferiria, seja de que forma fosse, nomeadamente por interceção, gravação e divulgação do teor da própria comunicação[157].

Como podemos constatar noutras constituições europeias "o segredo de correspondência, o segredo postal e o segredo das telecomunicações garante o livre desenvolvimento da personalidade através do intercâmbio privado, secreto perante o público"[158]. Assim, tanto o privado como o próprio Estado, estão limitados quanto ao seu tratamento e análise, permitindo a todos os cidadãos que tenham confiança, de que quando estabelecem uma comunicação, esta permanece tal como é.

---

[155] Cf. Rodrigo Ziembowicz, Estimular e proteger o Desenvolvimento Econômico diante da Criminalidade Organizada. In: Manuel Monteiro Guedes Valente (Coord.). Criminalidade Organizada Transnacional – Corpus Delictii III. Coimbra: Almedina, pp. 87-138. *op.cit.*, p. 88.

[156] Como nos explica Rita Castanheira Neves, As ingerências nas comunicações eletrónicas em processo penal. 1ª Ed. Coimbra Editora, 2011, *op.cit*., p.54.

[157] *Idem*, p. 51.

[158] *Ibidem*.

A necessidade premente de encontrarmos uma solução "pacífica" de minimizar os riscos e a disseminação de ataques terroristas ou ciberataques (ciberterrorismo), vê-se infrutífera dada a escalada que atualmente se assiste nesta "era digital". Os meios que os órgãos de polícia criminal possuem, ainda que com uma "alegadamente" renovada estrutura, e meios tecnológicos sofisticados, vê-se constrangida a montante da investigação criminal pelo facto de não raras vezes imiscuir-se do recurso a técnicas e práticas criminosas. Não estamos a dizer com isto que estão a praticar algum tipo de crime, mas a linha que separa da prática de um ato criminoso com a técnicas e meios de investigação, poderia por vezes questionar algumas mentes mais inquietantes da legitimidade com que de facto aqueles órgãos verdadeiramente atuam. Presume-se que qualquer órgão do Estado atue conforme os princípios e garantias que um processo penal admite num Estado de Direito Democrático. Daí a necessidade de dotar «todos» de um rigoroso controlo externo e interno bem como de uma legislação clara e de inequívoca hermenêutica.

Julgamos que um modelo Orwelliano não seria o caminho que desejaríamos, mas se não estivermos atentos, esse caminho revelar-se-á não tão distante assim. Partidos políticos de «extremas», poderão ver justificado a necessidade de uma maior intervenção do estado, escamoteado como propaganda política, e fazer (re)emergir regimes totalitários e tendencialmente autocráticos. Orwell compreendia que a maior ameaça para a humanidade residia no totalitarismo e que esta implicava uma ameaça aos valores humanos, à liberdade, justiça social, à fé na honestidade natural e na correção das pessoas comuns, à diversidade dos homens[159] e por isso alertou para que não permitíssemos que isso acontecesse.

A permanente recolha de dados pelas grandes empresas de prestação serviços e redes sociais, como a Google, a Amazon, o Facebook (entre outras) permitem que estes detenham uma enorme base de dados. Nenhum Estado poderá evitar a partilha dessa mesma informação, apesar dos esforços em regulamentar a proteção de dados pessoais, a verdade é que não evitam escândalos mediáticos[160] colocando à prova as próprias democracias.

Face aos avanços tecnológicos, numa era de riscos e ameaças transfronteiriças, arrastando consigo, toda uma panóplia de incertezas e inseguranças torna-se imprescindível um ponto de equilíbrio, no combate à nova criminalidade. Será necessário dotar os órgãos responsáveis pela

[159] Ver George Orwell, Mil Novecentos e Oitenta e Quatro. Antígona, Reimpressão, 2015.

[160] Veja-se, por exemplo, o escândalo da Cambridge Analytica (2018) [consult. 23 julho.2021], disponível em https://www.jn.pt/inovacao/facebook-multada-em-560-milhoes-pelo-escandalo-cambridge-analytica-10084371.html; o caso mais recente em que Luxemburgo queria multar a Amazon por violar a proteção de dados (2021) [consult. 23 julho.2021], disponível em https://www.jornaldenegocios.pt/empresas/detalhe/luxemburgo-quer-multar-amazon-em-425-milhoes-por-falhas-na-protecao-de-dados

segurança interna e externa dos meios adequados, que por vezes, a invasão da privacidade do agente é a única forma de lograr o combate ao crime.[161]

Analisaremos de seguida a tentativa de uma harmoniosa concetualização dos dados de tráfego, de base e de localização para depois nos debruçarmos sobre a avaliação de impacto da proteção de dados e respetivo consentimento e, por fim, o ocasional acesso aos "metadados" pelos serviços de informações e o seu testemunho face à nova criminalidade.

1. Os dados de tráfego, dados de localização, dados de base e os dados de telecomunicações e de internet.

Cumpre-nos fazer uma breve introdução neste capítulo, a respeito da definição dos conceitos, designados metadados, que comporta os dados de base, os dados de tráfego, os dados de localização bem como os dados de telecomunicações e de internet.

A fim de tentarmos encontrar algum consenso em definir os designados metadados, começamos por chamar à colação o entendimento de alguma doutrina, concatenando com jurisprudência e por fim enunciando os respetivos diplomas que de facto consagram a definição daqueles "dados".

A ambiguidade que gira em torno de uma definição concreta e inequívoca dos conceitos de dados de tráfego, de base e de localização julgamos que não se revela assim tão relevante a distinção no plano conceitual, mas antes num plano material e teleológico a fim de servir de referência à apreciação da conformidade constitucional da possibilidade de acesso aos metadados pelos serviços de informações. Contudo, não podemos deixar de mencionar os conceitos básicos que levaram o tribunal constitucional a pronunciar-se sobre a legitimidade de acesso aos metadados pelos serviços de informações.

Segundo a terminologia corrente, consideram-se dados pessoais os dados relativos a uma pessoa identificada ou, pelo menos, identificável. Por seu turno, considera-se que uma pessoa é identificável se for possível obter informações adicionais, sem um esforço desproporcionado, que permitam a identificação do titular dos dados.[162]

[161] Cf. Rita Castanheira Neves, As ingerências nas comunicações eletrónicas em processo penal - 1ª ed. Coimbra editora, 2011, *op.cit*., p.53

[162] Conforme Manual de Legislação Europeia sobre a Proteção de Dados. [consult. 06 Jul. 21]. Disponível em http://publications.europa.eu/resource/cellar/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1.0017.03/DOC_2

A este propósito, o Acórdão n.º 403/2015 do TC, acolheu o que já tinha sido classificado desde o Acórdão n.º 241/2002, de 29/05/2002 bem como do Acórdão 486/2009, de 13/01/2009, do mesmo tribunal, uma classificação tripartida dos referidos dados subsumindo à *posteriori* entre duas categorias apenas, nomeadamente *dados de telecomunicações,* de *dados de internet*. Os primeiros, entendem-se como sendo 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 de rede, de comunicações vocais, serviços de mensagens e multimédia e de ouras formas de comunicação", os segundos, como "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 de dados, quando não deem suporte a uma concreta comunicação" [163].

Considerando a definição legal daquela classificação tripartida, compreende a identificação e morada bem como o contrato de ligação à rede (dados de base), os dados tratados numa rede de comunicações eletrónicas ou no âmbito de um serviço de telecomunicações que indiquem a posição geográfica do equipamento terminal de um serviço de telecomunicações acessível ao público (dados de localização) e os dados tratados para efeitos de envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação (dados de tráfego), estes não estariam associados a uma comunicação efetiva[164], ou seja, não dariam suporte a uma comunicação. Acabando por refletir-se, na determinação do parâmetro constitucional, que protege o acesso a tais dados e classificando-os como dados de internet.

Dissociados destes dados, que não dão suporte a uma comunicação, são os dados de telecomunicações que, como descreve o n.º 1 do art..2º da referida LO, reportam-se a comunicações vocais, mensagens e outras formas de comunicação e, portanto, associados a atos de comunicação[165]. Contudo, aquele Tribunal reconheceu que *"mesmo que não haja acesso ao conteúdo, a interconexão entre dados de tráfego poderia fornecer um perfil complexo e completo do visado – com quem conversa, que lugares frequentes, quais os seus*

[163] Cf. n.º 1, artigo 2.º da LO n.º 4/2017, de 25 agosto.
[164] Cf. Acórdão n.º 464/2019 do TC veio a esclarecer no ponto 7.
[165] A este propósito, ver Manuel de Costa Andrade, "Comentário ao art.194.º do Código Penal ", in J. Figueiredo Dias (direção), Comentário Conimbricense do Código Penal – Tomo I, 2.ª ed., 2012, cit. p. 1103. O autor refere que a delimitação do conceito de telecomunicação encontra-se protegido contra a intromissão arbitrária. Não sendo aqui abrangidos os dados que não se reportam a atos efetivos de comunicação (tentados ou falhados) entre duas pessoas. Caindo fora deste conceito o regime de telecomunicações dos dados de localização obtidos mediante recurso a GPS.

horários" (ponto 9), e por conseguinte, poderia dar azo a uma manipulação daqueles dados para fins diversos e por isso violar a privacidade dos interlocutores, intervenientes, bem como a sua manipulação.

Já na Lei do Cibercrime[166] apenas vemos expressamente definido os dados de tráfego, e que a nosso ver, já torna o conceito um pouco mais discriminado em relação à LO n.º 4/2017, de 25 de agosto, consagrando outros elementos - a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente – que em certa medida assistimos a uma relativa diacronia de rigor do conceito. O que no Acórdão 403/2015 do TC, em linguagem informática, qualifica como metadados ou "dados sobre dados", como uma concreta comunicação, que seja fornecida ou transmitida como um conjunto de informações sobre diversas formas. Informações que acrescem aos dados e que têm como objetivo informar sobre eles, por forma a tornar mais fácil a sua organização. Sendo que, tratando-se de dados sobre dados, acabam por fornecer informação sobre a localização, tempo, tipo de conteúdo, origem e destino, entre outras.

Assim, assistindo a uma constante evolução legislativa, acompanhada de jurisprudência, de acordo com aquele tribunal continua a ser consensual a classificação a que o Parecer n.º16/94 da Procuradoria-Geral da República faz referência quando distingue entre dados de base, dados de tráfego e dados de conteúdo[167].

Em harmonia com os pareceres e jurisprudência nacionais, distinguem-se então: os dados à conexão à rede designados por dados de base; os dados funcionais necessários ao estabelecimento de uma ligação ou comunicação; e os dados gerados pela utilização de rede (designadamente a localização do utilizador, a localização do destinatário, duração, data e hora, frequência), dados de tráfego; e os dados relativos ao conteúdo da comunicação ou da mensagem, ou seja, dados de conteúdo.[168]

Já os dados de localização propriamente ditos, "consistem em dados tratados numa rede de comunicações eletrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações, podendo reportar-se sobre a latitude, longitude ou altitude do equipamento, sobre a direção da deslocação, identificação da célula de rede em que

[166] Lei n.º 109/2009, de 15 de setembro.

[167] Cf. Parecer n.º 16/94 da PGR, de 07/07/1994. Relator: Salvador da Costa. [consult. 14 Julho de 21]. Disponível em https://www.ministeriopublico.pt/pareceres-pgr/8715; Vide também parecer 100/2007 do Conselho Consultivo da PGR, de 17/07/2007. Relator: Pereira Coutinho. [consult.14 julho de 21]. Disponível em http://www.dgsi.pt/pgrp.nsf/7fc0bd52c6f5cd5a802568c0003fb410/b90edf9f8e8a47e480257515003eb4e8?OpenDocument.

[168] Cf. Transposição para a ordem jurídica nacional da Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, o disposto do artigo 2.º da Lei n.º 41/2004, de 18 de agosto, com as alterações introduzidas pela Lei n.º 46/2012, de 29 de agosto.

o equipamento está localizado em determinado momento e sobre a hora de registo da informação de localização"[169].

Não esgotado o tema sobre esta questão concetual dos metadados, não só por uma questão de economia de espaço, mas também pelo nosso objetivo circunscrever-se na matéria da legitimidade e cooperação institucional por parte dos serviços de informações com os órgãos de polícia criminal, não podemos deixar de prescindir deste espaço para fazer o enquadramento concetual adequado.

De seguida, passemos a analisar algumas questões relacionadas com a avaliação de impacto sobre a proteção de dados bem como o acesso a estes pelos serviços de informações, e de que forma podíamos conjeturar uma relação mais próxima e coesa entre aquele organismo e os demais órgãos de investigação criminal no combate à "nova criminalidade".

2. A avaliação de impacto sobre a proteção de dados e o consentimento.

Dos 173 considerandos do Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, relativo á proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, destacamos alguns deles quanto ao impacto a que certo tipo de tratamento e em particular quando utilizadas novas tecnologias, tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar consideravelmente um risco que afete os direitos, liberdades e garantias das pessoas singulares.

Sem necessidade de transposição, por se tratar de um regulamento, e que através do artigo 8º da CRP vigora diretamente na ordem interna vinculando imediatamente o Estado Português, bem como os seus cidadãos, independentemente de qualquer ato de mediação[170], impôs uma certa disciplina entre os Estados Membros, e que já tínhamos assistido através da Diretiva 95/46/CE (revogada pelo referido regulamento)[171].

Apesar de ainda assistirmos a uma relativa despreocupação[172], por parte de alguns organismos públicos, em implementar as normas a que o RGPD pretende uniformizar em

[169] Cf. Catarina Castro, Direito da Informática, Privacidade e Dados Pessoais, Almedina, 2005, *op.cit.,* p.181.
[170] Cf. Gomes Canotilho e Vital Moreira – Constituição da República Portuguesa Anotada, Vol. I, 4ª ed. Coimbra Editora, 2007, *op.cit.* p. 263 e 264.
[171] Cf. Ana Fazendeiro, Regulamento Geral sobre a Proteção de Dados, 3ª ed. Almedina, 2018, *op.cit.,* p.9.
[172] Aqui fazemos referência ao caso mediático que surgiu recentemente relativo à alegada partilha de dados pela Câmara Municipal de Lisboa à Embaixada Russa a respeito de uns manifestantes russos, que participaram num protesto em frente à embaixada Russa em lisboa, pela libertação de Alexei Navalny, opositor do governo russo. Disponível em https://www.tsf.pt/portugal/politica/partilha-de-dados-com-a-russia-o-que-se-sabe-do-caso-que-levou-medina-a-pedir-desculpa-13823398.html

relação às regras de proteção de dados, e que, não obstante, também serve para fomentar algum mediatismo, o facto é que o Estado em conjunto com as autoridades de controlo devem estabelecer a tal "disciplina" no tratamento de dados pessoais a par de uma limitação desse mesmo tratamento.

Como refere Ana Fazendeiro, cabe à autoridade de controlo elaborar uma lista dos tipos de operações de tratamento sujeitos a avaliações de impacto, que como descreve, consubstancia-se numa avaliação levada a cabo por um responsável pelo tratamento de dados, por forma a minimizar os riscos de incumprimento das regras de proteção de dados.[173] A autora faz ainda referência ao artigo 35.º do Regulamento, relativo a obrigatoriedade de conduzir este tipo de avaliação, em determinadas situações, de forma a evitar por exemplo o designado "*profilling*" (definição de perfis), e como base nele adotar decisões que produzam efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente[174].

Para além desta obrigatoriedade, a avaliação inclui uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, bem como a avaliação da necessidade e proporcionalidade das operações em relação aos objetivos, uma avaliação dos riscos face aos direitos e liberdades dos titulares dos direitos, incluindo as garantias de segurança e procedimentos, destinados a assegurar a proteção daqueles dados e a demonstrar a conformidade tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas.

Quanto à previsão constante no artigo 4.º, n.º 11, do RGPD, este reporta-se "á manifestação de vontade, livre, específica, informada e explícita, pelo qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento". Ou seja, o consentimento tem de ser explícito, e que não obstante, de silêncio ou omissão, não deverão, por conseguinte, constituir consentimento.[175]

No considerando 50 do RGPD, faz-se menção ainda ao tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos. Caso seja necessário para outras finalidades, nomeadamente para o exercício da autoridade pública, para fins de investigação científica ou histórica ou ainda para fins estatísticos, deverão ser considerados tratamento lícito compatível.

---

[173] Cf. Ana Fazendeiro, Regulamento Geral sobre a Proteção de Dados, 3ª ed. Almedina, 2018, *op.cit.*, p.26.
[174] *Ibidem, op.cit*., p.26
[175] Cf. O considerando 32. do Regulamento (UE) 2016/679, de 27 de abril de 2016 do Parlamento Europeu e do Conselho. [Consult. 17 Julh.21]. Disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679

É certo e admissível que assim o seja, desde que constitua uma medida necessária e proporcionada, numa sociedade democrática, para salvaguardar em particular outros objetivos de interesse público, contudo, relativo a atos criminosos ou ameaças à segurança pública também deverão ser considerados como sendo do interesse legítimo do responsável pelo tratamento, como assim prevê o mesmo considerando (50).

Tendo em consideração os princípios relativos ao tratamento, de dados pessoais [176], só é lícito, se tiver sido dado o consentimento pelo seu titular e existir necessidade de exercer funções de interesse público ou ao exercício de autoridade pública, nomeadamente para efeitos de prevenção, deteção, investigação e repressão de infrações terroristas e da criminalidade grave[177].

3. O acesso aos metadados por parte dos serviços de informações e o seu contributo no combate à "nova criminalidade".

Considerada a necessidade dos Estados adotarem instrumentos de combate à prevenção e luta contra o terrorismo, espionagem e criminalidade violenta altamente organizada num mundo cada vez mais dependente dos recursos digitais, passemos a analisar a importância de dotar todos os organismos do Estado responsáveis pela segurança, com competência e dotados de estruturas técnicas, com o conhecimento, a arte e o engenho necessário, no combate a estes tipos de crimes[178].

Deste modo, reconhece-se a necessidade de uma resposta integrada, a mobilização, coordenação e cooperação de todas as estruturas nacionais com responsabilidade direta e

[176] A licitude, lealdade, transparência, adequação, pertinentes e limitados ao que é necessário relativamente as finalidades «minimização dos dados», exatos e atualizados «direito ao apagamento», da segurança, integridades e confidencialidade.

[177] Para além dos demais atos legislativos em matéria de proteção de dados, veja-se também a Diretiva (EU) 2016/681 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016, relativa á 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.

[178] Esta necessidade não se esgota apenas nesta temática. Como refere Rodrigo Ziembowicz, Estimular e proteger o Desenvolvimento Econômico diante da Criminalidade Organizada. In: Manuel Monteiro Guedes Valente (Coord.). Criminalidade Organizada Transnacional – Corpus Delictii III. Coimbra: Almedina, *Op.cit.*, pp.93 e 94. "Os Estados têm como atribuição constitucional, não somente apoiar, estimular e facilitar o desenvolvimento econômico das empresas, mas também promover um mercado econômico sadio e sustentável, inclusive tutelando penalmente bens jurídicos jusfundamentais relacionados como o mercado econômico e ao seu equilíbrio". "Vendo esta tarefa paradoxal, entre a obrigação de estimular o desenvolvimento econômico e a tarefa de prevenir e reprimir as condutas delituosas (…) torna-se ainda mais espinhosa diante do enfraquecimento do poder dos Estados (…), pouco ou nenhum poder (…), especialmente quanto à capacidade de legislar e de vincular os agentes econômicos às normas que estabelece".

indireta e assim podermos ver plasmada toda esta sinergia nalguns diplomas a fim de legitimar as ações dos Estados.[179]

Foi contudo, através da Resolução de Conselho de Ministros n.º 7-A/2015, definida a Estratégia Nacional de Combate ao Terrorismo, que assenta objetivamente em detetar, prevenir, proteger, prosseguir e responder[180] contra esse tipo de ameaças.

Conforme descrevemos estes cinco pilares de ação da Estratégia Nacional de combate ao Terrorismo (detetar, prevenir, proteger, perseguir e responder), por maioria de razão estender-se-ia igualmente para os casos da criminalidade violenta altamente organizada (transnacional) e espionagem, que de acordo com o n.º 2 do artigo 187.º do CPP prevê a admissibilidade de interceção e gravação de conversações ou comunicações telefónicas. Nestes casos, julgamos que a atuação dos serviços de informações vê-se justificada na circunstância dos dois primeiros pilares (detetar e prevenir), pois segundo, as linhas de ação definidas na referida Resolução do Conselho de Ministros, o primeiro pilar assenta essencialmente em identificar atempadamente potenciais ameaças terroristas, mediante a aquisição do conhecimento essencial para um combate eficaz, e para tanto prosseguir na recolha, tratamento e análise de dados e informações que permitam antecipar o conhecimento e avaliação de ofensivas em preparação.

O diploma ainda refere, na prossecução dos objetivos estratégicos, ser essencial para além dos meios de produção, tratamento e análise, reforçar os mecanismos à eficiência na partilha da informação entre as forças e serviços de segurança[181], bem como reforçar os mecanismos adequados à cooperação institucional entre o SIRP e o Sistema de Segurança Interna (SSI), de modo, a garantir a partilha de informação[182].

Uma vez que o lugar de atuação dos serviços de informações situa-se à margem de um processo penal e no campo da prevenção, circunscreve-se em observar e monitorizar condições propensas à adesão para a prática de atividades terroristas permitindo desta forma a adoção de medidas que obstem ao seu surgimento em preparação, entendemos que o segundo pilar também se encontra preenchido.

---

[179] A este propósito ver também a Lei n.º 5/2002, de 11 de Janeiro que veio estabelecer medidas de combate à criminalidade organizada e económico-financeira; a Lei n.º 83/2017, de 18 de Agosto que estabeleceu as medidas de combate ao branqueamento de capitais (revogando a Lei n.º 25/2008, de 5 de Junho) e a Lei n.º 52/2003, de 22 de Agosto (com as alterações introduzidas pelos restantes diplomas sendo a última versão a da Lei n.º 16/2019, de 14 de Fevereiro)

[180] Quanto a estes cinco pilares definidos pela Estratégia nacional contra o terrorismo, de acordo com a estratégia Europeia, Portugal acrescentou "ex-ante" mais um pilar, o "detectar" conforme a Resolução de Conselho de Ministros n.º 7-A/2015.

[181] Do qual o SIS integra este grupo, de acordo com a al. e), n.º 2 do artigo 25.º da LSI.

[182] Cf. n.º 4 da RCM.

O objeto e a matriz de um serviço de informações é a informação, é produzir conhecimento com base em informação em *"bruto"* (*raw information*) convertendo-a em "*informação acabada"* (*finished intelligence*).[183]

De acordo com a terminologia utilizada por Joanisval Gonçalves, a obtenção do "*dado negado*" é de vital importância na atividade de inteligência no contributo para o processo decisório de uma determinada ação, "uma vez que os Estados ou outros atores buscam esconder informações de outros Estados ou atores, essa informação deve ser obtida por meios sigilosos ou encobertos"[184]. O autor refere ainda, que este "*dado negado*" é inerente à atividade de inteligência bem como inclusive, por parte das ações dos governos na "manutenção da soberania" e da "obtenção de vantagens estratégicas para o país sobre o manto de proteção às informações ditas de segurança nacional"[185]. Como iremos abordar mais adiante, em regimes democráticos, em que impera a especial proteção dos direitos fundamentais, é fundamental que os serviços de informações estejam sob rígidos mecanismos de controlo, quer externo quer interno, para que se evitem abusos e arbitrariedades por parte dos seus agentes.

Deste modo, enquanto a atividade de inteligência se baseia em prospetiva (inteligência e contra-inteligência), as forças policiais atuam em retrospetiva, ou seja, numa investigação criminal o que se pretende é uma reconstituição dos factos.

Por exemplo, na doutrina brasileira Joanisval Gonçalves distingue a inteligência interna (ou doméstica) da inteligência policial (ou criminal), evidenciando uma clara distinção nos fins a que estão destinados. Apesar das competências e os métodos operacionais se evidenciarem semelhantes, o autor carateriza a inteligência doméstica como "a produção de conhecimento com o objetivo de apoiar o processo decisório com informação de caráter estratégico, devendo o sigilo das suas atividades ser preservado". Por outro lado, o autor define a inteligência policial como aquela "que tem por objetivo apurar a autoria e materialidade de delitos para instruir inquéritos e subsidiar o processo penal"[186].

De facto, parece-nos não ser muito diferente em Portugal, uma vez que os serviços de inteligência ("*doméstica"* ou serviços de informações) não têm poderes de polícia, mormente de OPC.

---

[183] Cf. Joanisval Brito Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, *op.cit.* p. 19.
[184] *Idem, op.cit*. p.13. «Daí a necessidade de uns serviços de inteligência», *apud* Greg Hannah, Kevin O'Brien, Andrew Rathmewll. *Technical Report: Intelligence and Security Legislation for Security Reform. United Kingdom's Security Sector Advisory Team, RAND Europe, Cambridge, June* 2005. Disponível em https://www.rand.org/pubs/technical_reports/TR288.html (sobre a obtenção do Dado Negado).
[185] *Ibidem*.
[186] Cf. Joanisval Brito Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, *op.cit.* p.72 e 73.

Destarte, uma vez que as funções a que, tanto os serviços de informações como das polícias, não se confundem, apesar da sua estreita relação quer quanto aos métodos operacionais utilizados, como aos meios de obtenção de conhecimento, defendemos que devem atuar em cooperação, num contexto de segurança nacional. Não é despiciendo afirmar que muitas das vezes o objeto ou "*alvos*" dos serviços de inteligência estão envolvidos diretamente com atividades criminosas, sendo do interesse comum conjugarem os esforços e a necessidade de cooperação, tanto na partilha de informação como no desenvolvimento de operações conjuntas entre polícias, fisco e serviços de informações[187].

Aproveitamos para fazer alusão as teorias de prevenção geral em direito penal, e que como nos descreve Germanos Marques da Silva, "a prevenção da criminalidade pode obter-se por duas vias, que, aliás, se complementam: a prevenção geral positiva da prevenção geral negativa"[188].

A primeira, prevenção geral positiva, assenta essencialmente na "educação, na integração, na reafirmação dos valores comunitariamente assumidos"[189].

Já a segunda, prevenção geral negativa, e que talvez nos faça mais sentido, não obstante "*de se questionar a sua legitimidade axiológica e validade empírica*" como refere o autor, "corresponde a uma visão utilitarista do direito penal"[190].

Chamamos por esta via à colação, o que o autor faz menção na sua obra, conforme a "*teoria da coação psicológica"* de *Feurbach*[191], segundo o qual "seria necessário ameaçar um potencial delinquente com um mal superior ao que lhe resultaria da renúncia à sua prática", talvez pudéssemos contribuir para a "eficácia do direito penal, na sua função de prevenção, não tanto para a irradicação do crime, o que seria utopia, mas pela contenção da criminalidade", a certeza ou grande probabilidade da sua aplicação, ou seja, adaptado ao contexto, seria dissuadir potenciais terroristas, e de facto reconsiderarem a participação ou adesão a grupos ou associações criminosas, dando a legitimidade neste caso aos serviços de informações, de utilizarem os instrumentos necessários a fim de monitorizarem os movimentos suspeitos e a relação com esses grupos e associações. No fundo o que se pretendia seria responsabilizar cada indivíduo pelas suas ações. E naturalmente haveria também, de se criar uma escalada progressiva, além de princípios éticos para fundamentar as

[187] *Idem*, p.73.
[188] Cf. Germano Marques da Silva – Direito Penal Português. Vol. I: Introdução e Teoria da Lei Penal. 3ª Ed. Verbo, 2010, *op.cit*. p. 63.
[189] *Idem*, p. 63.
[190] *Idem*, p.61.
[191] *Idem*, p.60 (nota 1).

atividades de inteligência, das fontes de inteligência, a que os serviços de informações haviam de recorrer por forma a esgotar todos os recursos, quanto à origem dos dados, até não haver outro meio de recolha de informação (as ditas fontes de informação), como por exemplo: OSINT, HUMINT, IMINT entre outras.

Compreendemos, no entanto, que seria bastante controversa a questão a que nos propomos, pelo facto de ser necessário uma alteração substancial do paradigma doutrinário e nalguns diplomas, como por exemplo no CPP, CP, entre as demais legislações aplicáveis ao tema, sendo que o primeiro seria a própria Constituição da República Portuguesa.

2. A atividade de inteligência

Na perspetiva de Pedro Cardoso, "a qualidade da ação política de um país depende em larga medida do rigor dos conhecimentos em que ela se baseia"[192], norteando assim as linhas de ação do poder político para fazer face às dificuldades previstas, que oportunamente e com a antecedência possível, apoia o processo de decisão e adota a atitude mais adequada.

Assim, a função de produção de informações traduz-se numa incumbência funcional, no atual quadro institucional dos organismos de Estado, ao SIRP, e que conforme o artigo 2.º da LQSIRP e o artigo 2.º da Proposta do Decreto n.º 426/XII transcrevem na letra da lei, a ideia, a que Arménio Ferreira descreve como "elementos de conhecimento sistematizado em quadros interpretativos, através de critérios que sobrepõem a estrutura de sentido à relação causal"[193].

Apesar dos traumas psicológicos, históricos e políticos das designadas polícias políticas do Estado Novo, responsáveis por perseguições a opositores do regime político de então, o facto é que não podemos desprezar a necessidade de legitimar a atividade prosseguida pelos serviços de inteligência (serviço de informações), que decerto também necessitariam de um assento constitucional por forma a tornar transparente (dentro de um mínimo de fundamento jurídico plausível) as atividades prosseguidas pelos seus agentes[194].

É por isso imprescindível falarmos não só dos princípios estruturantes que deverão nortear a atividade de inteligência, em paralelo com a função de inteligência policial no âmbito da prevenção criminal, como também dos instrumentos de controlo e órgãos de fiscalização.

[192] Cf. Pedro Cardoso, As Informações em Portugal. 2ª Ed. Gradiva – Publicações IDN. 2004, *op.cit.* p.150.
[193] Cf. Arménio Marques Ferreira, "O sistema de informações da república portuguesa", in Bacelar Gouveia, Rui Pereira (Coords), Estudos de Direito e Segurança. Almedina, 2007, pp.67-93, *op.cit.* p.69.
[194] Bacelar Gouveia, Rui Pereira (Coords) - Estudos de Direito e Segurança. Almedina, 2007, *op.cit.* p.176.

Apesar dos desafios colocados pelas atividades prosseguidas pelos serviços de inteligência a nível mundial, em Estados de Direito Democráticos na defesa dos direitos, liberdades e garantias (preservando acima de todos a dignidade da pessoa humana), a arte de governar, será mais eficiente, acessível e praticada com mais segurança se for apoiada por um eficaz serviço de informações[195].

2.1 Os princípios norteadores da atividade de inteligência e o contributo da produção de informações na prevenção criminal.

Seja qual for a categoria de *intelligence* – militar, estratégica ou policial – a produção de conhecimento (informações) deverá ser conduzida sob um código ético rigoroso, entre vários princípios norteadores da atividade de inteligência, através de leis, regulamentos adequados e de um sistema de controlo democrático regular e eficiente.

Assim, a atividade dos serviços de informações encontra-se sob um véu de princípios estruturantes consolidada pela Constituição e pela lei.

Constituindo a essência da produção de *intelligence* na recolha e tratamento de informação maioritariamente através de fontes abertas (OSINT)[196], o ciclo de produção de informações, nas sua funções consubstancia-se no pedido, na pesquisa seguida da análise e por fim na difusão[197].

Apesar da OSINT revelar-se fundamental, fornecendo grande parte da informação aos serviços de inteligência, face às ameaças transnacionais e reconhecendo o seu caráter assimétrico e multifacetado, os Estados vêem-se incapazes de enfrentar os desafios impostos pela revolução digital que estamos atualmente a atravessar de forma eficaz, tornando-se quase impossível não recorrer às fontes tecnológicas de informações (*techint*)[198].

Deste modo, destacamos alguns princípios subjacentes à atividade de inteligência - o que se torna incondicionalmente difícil na sua aplicação pelo facto da atividade dos serviços

---

[195] Cf. Pedro Cardoso, As Informações em Portugal. 2ª Ed. Gradiva – Publicações IDN. 2004, *Op.cit*. p.154.
[196] OSINT (Open Source Intelligence)
[197]Cf. Bacelar Gouveia, Direito da Segurança. Cidadania, Soberania e Cosmopolitismo, 1ª ed., Almedina, 2018, *op.cit*. p. 703.
[198] *Idem*, p.704. Quanto a estas fontes tecnológicas de informações (techint – *tecnological intelligence*) o autor faz menção ainda a diversos tipos como por exemplo as informações de sinais (sigint – *signal intelligence)*, as informações de comunicações (comint – *communication intelligence*), as informações eletrónicas (elint – *eletronic inteligence*), as informações telemétricas (telint – *telemetry intelligence*), as informações de imagem (imint – *imagery intelligence*), as informações fotográficas (photint – *photografic intelligence*), e as informações eletromagnéticas (masint – *measuremente and signature intelligence*).

de inteligência se caracterizar pelo sentido de oportunidade e de ações consideradas marginais (mas dentro da legalidade).

Como descreve Bacelar Gouveia, a atividade dos serviços de informações deverá, acima de tudo, nortear-se pelas normas emanadas pela própria Constituição e pela lei (*princípio da constitucionalidade e da legalidade*), salvaguardando em matéria de proteção de direitos fundamentais, os dados informatizados e ainda sujeitos a todas as restrições legalmente estabelecidas em matéria de defesa de direitos, liberdades e garantias perante a informática[199].

O "princípio da especialidade e da objetividade"[200], consubstancia-se na atividade prosseguida pelos Serviços[201], na medida em que apenas se circunscreve às suas específicas atribuições no quadro dos objetivos e finalidades legais e de harmonia com as orientações e diretivas adotadas pelo Primeiro-Ministro[202]. Para além de expressar os conhecimentos sobre determinados factos e atos com a maior exatidão e rigor possível, mediante a utilização de linguagem clara e simplificada.

Outro princípio importante é o da "restrição funcional"[203] que, como já mencionamos anteriormente, a atividade dos serviços de informações encontra-se delimitada no seu âmbito de atuação, uma vez que os seus funcionários ou agentes não podem exercer atividades, praticar atos ou desenvolver atividades com a competência específica dos tribunais ou das entidades com funções policiais[204].

Por outro lado, em contraste com este último princípio temos o "*princípio da exclusividade*" das atividades prosseguidas pelos serviços de informações, para que prossigam objetivos e atividades idênticos aos previstos na LQSIRP[205] atendendo à circunstância das finalidades do SIRP[206]. Este princípio revela-se *sui generis* uma vez que a lei, apesar de considerar esta exclusividade da atividade desenvolvida pelos serviços de informações, não impede, contudo, que outros organismos de polícia o façam. Neste ponto julgamos, que por maioria de razão, em relação por exemplo, às atribuições conferidas aos órgãos de polícia criminal no que respeita à restrição das liberdades fundamentais consagrada no n.º 4 do artigo 34.º da CRP deveria se estender igualmente aos serviços de informações.

---

[199] *Idem*, p.707. Cf. Art.º 3.º n.º 1 e 2, da LQSIRP e art.2.º do Dec. N.º 426/XII.
[200] Cf. Joanisval Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, cit. p. 127.
[201] As atribuições definidas aos dois Serviços (SIS - Serviço de informações e segurança - e SIED – Serviço de informações estratégicas de defesa).
[202] Cf. Art.º 3.º, n.º2 da LQSIRP e art.7º, n.º1 do Dec. N.º 426/XII.
[203] Cf. Bacelar Gouveia, Direito da Segurança. Cidadania, Soberania e Cosmopolitismo, 1ª ed., Almedina, 2018, cit. p. 707.
[204] Cf. Art.º 4.º, n.º1 da LQSIRP e art.5º, n.º2 do Dec. n.º 426/XII.
[205] Cf. Art.º 6.º, do diploma legal.
[206] Cf. Art. º 2. º, da LQSIRP e Art. º 2. º, Art. º 4. º, n. º 2 do Dec. n. º 426/XII.

Uma vez que também a estes está incumbido a salvaguarda da segurança, da independência e interesses nacionais, contribuindo assim para um reforço de cooperação institucional face a algumas tipologias de crime, como já mencionámos, e a prática de atos, que pela sua natureza possam alterar ou destruir o Estado de Direito Democrático.

Não obstante, de os órgãos de polícia criminal estarem consignados a um conjunto de diligências, que nos termos da lei processual penal, estes garantem o mínimo ético da inviolabilidade de determinados direitos fundamentais, e ainda no âmbito daquela tipologia de crimes descrita, a competência da investigação estar reservada à Polícia Judiciária, não impede igualmente que sejam utilizados os mesmos meios de obtenção de prova aos serviços de informações. Aqui preconizamos o princípio da oportunidade tal como refere Joanisval Gonçalves "a inteligência como produto é passível de rápido processo de deterioração diante do tempo"[207], na medida em que a não observância deste princípio ou a desconsideração deste fator levaria à inutilização das informações produzidas.

Considerando o rigoroso controlo estabelecido pela proporcionalidade [208]. e por isso com elevado escrutínio judicial, o acesso do pessoal do SIRP aos dados e informações conservados em arquivo nos centros de dados dos Serviços só é concedido mediante autorização superior, regulado por despacho do Secretário-Geral e ainda em conformidade com a Portaria n.º 237-A/2018, que estabelece os termos e condições técnicas e de segurança em que se processa a comunicação eletrónica, para efeitos de transmissão diferida de dados de telecomunicações e internet previamente armazenados pelos prestadores de serviços de comunicações eletrónicas às autoridades competentes do SIRP.

Também não podemos menosprezar um outro princípio designado por Joanisval Gonçalves como "*princípio da segurança*", e que considerando todo o ciclo de produção de informação, desde o seu planeamento, produção e difusão, deverá ocorrer sob a égide de um regime de segredo. Julgamos que apesar de uma grande maioria doutrinária convergir conceptualmente na preservação do regime de segredo em determinadas instâncias e organismos de Estado, em virtude de obter uma vantagem competitiva assim como pela salvaguarda de matérias, documentos e as informações cujo conhecimento por pessoas não autorizadas for suscetível de colocar em risco interesses fundamentais do Estado[209], reconhecemos uma incompreensão na necessidade de conhecimento de determinadas informações - os metadados. Com refere Joanisval Gonçalves "*a atividade de inteligência*

[207] Cf. Joanisval Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, *op.cit.* p. 127.
[208] *Idem*, p. 12 e ss.
[209] Cf. Art.º 2.º, n.º 1 da Lei Orgânica n.º 2/2014 – Regime de Segredo de Estado.

deve revestir-se de profundo grau de sigilo, o que de forma alguma significa que seja atividade ilegal e sem controlo"[210]. Não obstante do receio de conferir a um organismo de estado um tal elevado grau de sigilo de informações por razões óbvias, na medida em que, poderia comprometer todo o ciclo de produção de informações, permite igualmente a conservação do conhecimento a terceiros e um traço distintivo dos serviços de inteligência.[211]

O "*princípio da imparcialidade*", permite uma isenção pessoal de outras influências que possam prejudicar a experiência acumulada dos analistas. Como bem reconhecemos, os contextos ideológicos de conflito, bem como os regimes autoritários revelam-se propensos a um risco de ideologias, desvirtuando por isso a produção de conhecimento.

> Apesar das fortes convicções pessoais dos seus agentes sobre assuntos que acompanham, essas não têm lugar na inteligência por eles produzidas, produzindo um conhecimento isento de juízos de valores pessoais. Com base neste princípio, o dever de zelo constante afirma-se com a maior relevância de modo a evitar a politização da inteligência e do conhecimento produzido[212].Os riscos de um desvio da inteligência para fins políticos são elevados, originando consequências devastadoras na credibilidade das organizações como para a própria estabilidade democrática[213].

Na incerteza conjuntural em que vivemos, a segurança é condição essencial ao exercício de Direitos, Liberdades e Garantias[214], neste sentido ganha importância a antecipação de informação em tempo útil, de planeamento, de ação, de verificação, de avaliação e reação. Sob o pretexto de dar resposta à evolução da criminalidade, num quadro cada vez mais dependente das novas tecnologias, os serviços de informações são um ator fundamental na preservação da Democracia.

A cooperação institucional é assim de vital importância para uma eficaz resposta ao combate às novas ameaças. É, contudo, com a descentralização de poderes funcionais e orgânicos que o Estado poderá alcançar ou evitar que os organismos competentes em matéria quer de investigação criminal (e portanto, sob a égide dos pressupostos e requisitos de um processo penal) quer a montante na fase de recolha e produção de informações (pelos serviços

---

[210] Cf. Joanisval Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, *op.cit.* p. 127. Como refere o autor, «este princípio carrega a ideia central de que a inteligência e sigilo são indissociáveis.»
[211] Cf. Bacelar Gouveia, Direito da Segurança. Cidadania, Soberania e Cosmopolitismo, 1ª Ed., Almedina, 2018, *op.cit.* p. 699.
[212] Cf. Joanisval Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, *op.cit.*, p.128 e 129.
[213] *Idem*, p.129.
[214] Cf. Carla Costa, "As alterações legislativas e as estatísticas criminais" in Revista Semestral de Investigação Criminal, Ciências Criminais e Forenses. Investigação Criminal N.º 7, 2014, pp.35-51. *op.cit*., p.35.

de inteligência), que se convertam em organismos com poderes ilimitados e corram o risco de se desviarem das suas competências e atribuições.

Apesar das alterações às fontes legislativas, que regem o Sistema de Informações da República Portuguesa, julgamos não ter havido ainda a necessidade de efetivamente procurar auxílio nos serviços de informações, uma vez que apesar dos esforços e iniciativas em reorganizar a sua estrutura e operacionalizar a atividade de inteligência com as ferramentas necessárias ao processamento da informação disponível, vê-se frustrada com a impossibilidade de utilizar os meios tecnológicos que permitem atuar com acurácia e diligência. Prevaleceu uma aura de desconfiança às propostas de alteração ao regime jurídico dos serviços de informações que consignariam a legitimidade e capacidade que lhes é devida, e que através do acórdão do Tribunal Constitucional de 2019 viu frustrada essa tentativa, ficando muito aquém dos seus congéneres, comprometendo assim a viabilidade de concretizar as missões a que estão incumbidos.

2.2 Fiscalização, controlo judicial e autorização prévia.

Como é sabido, a fiscalização e controle na Administração Pública, de um modo geral, são essenciais num Estado de Direito Democrático, com especial atenção nos órgãos de segurança do Estado. Neste sentido, a preservação da democracia encontra desafios, uma vez que os seus aquando organismos de segurança prosseguem atividades que colocam qualquer Governo sob um foco constante de desconfiança, quanto aos métodos e técnicas que os serviços de inteligência (alegadamente) recorrem. Como foi referido anteriormente, é importante que tenhamos em mente que a atividade de inteligência não sobrevive sem os princípios norteadores e com particular incidência nos altos padrões de ética dos seus agentes e administradores (Quadros Superiores – SGSIRP, Diretores, Diretores Adjuntos, Coordenadores etc.). Sem eles, a atividade de inteligência fica sujeita a uma debilitada estrutura de produção de informações, erros e ações tendentes ao fracasso.

Como descreve Joanisval Gonçalves, "é por meio da ética que o serviço secreto se diferencia como órgão a serviço de um bem maior, ganha confiança da sociedade e dos tomadores de decisão e mostra que não se encontra no mesmo nível de criminosos que usam técnicas como espionagem e meios intrusivos"[215].

[215] Cf. Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, *op.cit*. p. 133 e ss. O autor descreve ainda como "princípios éticos", "o respeito da dignidade do indivíduo e os interesse coletivos, a "imparcialidade"

Considerando o facto de os Serviços de Informações incluírem-se no seio da Administração Pública, o seu controlo deverá enquadrar-se na ideia clara do termo "*acountablitty*", que se traduz na "*prestação de contas*" ou na obrigação de fazê-lo, por outras palavras "trata-se de um processo por meio do qual um órgão ou agente do estado está obrigado a responder clara e completamente perante uma autoridade à qual deve prestar contas"[216].

Importante referir que este controlo não se restringe à fiscalização de contas públicas, mas também ao controlo político e social dos agentes e organizações do Estado, indispensável para uma democracia moderna num Estado de Direito Democrático.

Importa salientar que perante um cenário em que as organizações terroristas e as atividades criminosas atuam para além-fronteiras de forma concertada e com elevada capacidade tecnológica, os Estados vêem-se encruzilhados nos seus próprios sistemas, burocracias e consequentemente na capacidade ou incapacidade de resposta a este tipo de ameaças. Reconhecendo a existência de regimes autoritários que utilizavam (e ainda utilizam em algumas ditaduras os serviços de inteligência) para oprimir eventuais insurgentes contra um regime estabelecido, como refere Joanisval Gonçalves, "a inteligência é um instrumento à disposição dos entes públicos e pode ser usada para o bem e para o mal". Daí concluir-se que numa sociedade democrática deve haver a necessidade de criar um sistema de "freios e contrapesos" – o tão conhecido *Check and Balance* - para garantir que a atividade de inteligência e mais concretamente os seus agentes ajam de acordo com a Constituição e com a lei. Cabendo ao executivo supervisionar e gerenciar, ao poder Judiciário punir casos em que se evidencie um abuso e violação dos direitos, liberdades e garantias fundamentais dos cidadãos sem o devido fundamento legal, proporcionalidade, exigibilidade e adequação face as circunstâncias e ameaças em causa, e ainda deverá caber ao poder Legislativo estabelecer o enquadramento legal para a atividade de inteligência e fiscalizar se os serviços de informações atuam em conformidade com a lei[217].

Abordando a perspetiva de controlo interno, no caso português, existem vários diplomas que asseguram de forma direta e indireta esse mesmo controlo, contudo, como referimos

na perspetiva da busca da verdade no interesse do estado e da sociedade, sem deixar se influenciar por ideias preconcebidas, interesses particulares ou corporativos, a "cooperação" sistemática e proactiva dos conhecimentos úteis para a promoção e defesa dos interesses do Estado e da sociedade, a " discrição", do seu trabalho com reserva e sigilo dos conhecimentos produzidos, o "senso crítico" com o que analisam e refletem sobre as implicações morais das suas ações e decisões, e a "excelência" com que realizam as atividades, com dedicação, qualidade, profissionalismo, de forma metódica, diligente e oportuna".

[216]Cf. Joanisval Gonçalves, Políticos e Espiões. O Controle da Atividade de Inteligência. 2ª Ed. 2019, *op.cit.*p.15.

[217]Cf. Joanisval Gonçalves, Políticos e Espiões. O Controle da Atividade de Inteligência. 2ª Ed. 2019, *op.cit*. p.51.

anteriormente nunca podemos olvidar da probabilidade constante de risco de um desvio da *intelligence* para fins políticos, pois também como referido poderá originar consequências devastadoras na credibilidade das organizações e estabilidade democrática.

Por último, temos ainda a Resolução de Conselho de Ministros n.º 188/2017, de 5 de dezembro, acerca de centro de dados dos serviços de informações (SIS e SIED) vieram a estabelecer-se regras de funcionamento, critérios, normas técnicas, medidas e procedimentos tendentes à segurança das informações neles processados. Para além da fixação de critérios de atuação e delimitação de competências no processamento de dados, o Regulamento do Centro de Dados (doravante designado, RCD) compreende várias operações no âmbito do processamento e conservação de dados, nomeadamente a receção, registo e indexação/normalização, gestão, controlo e validação, e arquivo, supressão e destruição[218]. A recolha de dados pessoais para tratamento automatizado limita-se ao necessário para a produção de informações que contribuam para o cumprimento das atribuições institucionais dos dois serviços[219] e além disso os dados não podem ser conservados por período superior ao necessário às finalidades para que forem inseridos[220]. Reconhecemos neste enquadramento a possibilidade de que a disposição legal não tenha aferido ou estipulado um prazo determinável, de modo a ser o mais objetiva possível. No entanto, os números seguintes daquela disposição legal preveem as circunstâncias quanto à sua manutenção, supressão[221] e respetiva destruição[222]. Desta forma, julgamos que apesar de se tratar de um regulamento e não de uma lei, não deixa de estabelecer os procedimentos necessários a fim de preencher o *iter processualis*, em conformidade e respeitando os princípios de um Estado de Direito Democrático.

No relatório da supervisão democrática sobre serviços de segurança, adotada pela Comissão de Veneza na sua 71ª Sessão Plenária, de 01-02 de junho de 2007[223], afirma-se que os controlos internos consistem em dois elementos. O primeiro, exercido pelas agências de inteligência sobre si mesmo, por meio de estruturas de tomada de decisão projetadas para garantir as medidas e políticas que deverão ser devidamente autorizadas, e os procedimentos a ser seguidos. O segundo elemento, opera dentro do próprio executivo, ou seja, o controlo

[218] Cf. n. º 3 do Art.5. º do RCD.
[219] Cf. n. º 1 do Art.6. º, do RCD.
[220] Cf. n. º 1 do art.10. º do RCD.
[221] Cf. n. º 3, 4 e 5 do art. º 10. º do RCD.
[222] Cf. n. º 3 do art.11.º do RCD.
[223] Relatório sobre a supervisão democrática sobre serviços de segurança. Adotada pela Comissão de Veneza na sua 71ª Sessão Plenária, de 01-02 de junho de 2007. Studies no. 388/2006 e no. 719/2013. CDL-AD(2015)010. II. Proteção dos direitos fundamentais. Segurança, terrorismo e direitos humanos. Disponível em https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e.

administrativo exercido através de uma comissão de controlo prévio ou conselho de fiscalização, que no caso Português é constituído pelo Conselho de Fiscalização e pela Comissão de Fiscalização de Dados (ambos) do SIRP, constituindo assim, como o referido relatório designa, departamentos governamentais a que as agências estejam subordinadas, ou à qual podem prestar contas (*accountability*). Como foi mencionado, este controlo administrativo, segundo o entendimento do Tribunal Constitucional, não preencheria os limites da intervenção administrativa na liberdade individual, conquanto exigiria reserva de lei e precisão necessária para os limites daquela intervenção, bem como algum critério preciso ou determinado, de distinção da intervenção lícita da ilícita. De acordo com n.º 2 do artigo 78.º do decreto parlamentar[224], ainda que o acesso aos metadados pelos oficiais de informações (SIS e SIED) tivesse de passar pelo crivo da Comissão de Controlo Prévio, esta autorização não preencheria por si só a necessidade de controlo e fiscalização interna da intervenção administrativa. Conforme a declaração de voto vencido da Juiz Maria Amaral no douto acórdão de 2015 do TC, refere que "perante o silêncio da lei quanto aos limites da legalidade dessa intervenção, nenhuma garantia efetiva podia ser dada aos cidadãos de que a simples autorização prévia por parte da Comissão constituiria em si mesmo um procedimento eficiente de controlo da atuação da atuação administrativa, que prevenisse ou evitasse intromissões abusivas nas liberdades individuais"[225].

Questionamos a composição e a designação dos elementos que constituiriam aquela Comissão. Segundo o artigo 35.º do referido decreto parlamentar a Comissão de Controlo Prévio seria composta por três magistrados judiciais, designados pelo CSM, de entre os juízes conselheiros do STJ, com pelo menos três anos de serviço naquela qualidade[226]. Acresce que a Comissão tem de elaborar anualmente um relatório de atividades ao Conselho de Fiscalização do SIRP estando igualmente sujeita a inspeções, com ou sem aviso prévio e com a regularidade mínima trimestral[227], bem como receber do Secretário – Geral, com a regularidade mínima bimensal, uma lista integral dos processos em curso e os pedidos de autorização de acesso à informação submetidos à Comissão de Controlo Prévio, e a um

[224] Da Proposta de Decreto n.º 426/XII e conforme previa o projeto de Lei n.º 480/XIII/2.ª - "Acesso a dados de tráfego, de localização ou outros dados conexos das comunicações por funcionários e agentes dos serviços de informações da República Portuguesa" - e a proposta de Lei n.º 79/XIII – "Acesso a dados previamente armazenados pelos prestadores de serviços de comunicações eletrónicas pelo Sistema de Informações da República". [consult. 21 Ago.21]. Disponível em https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=41212.

[225] Ac.TC n.º 403/2015 de 27/08/2015, (Lino Rodrigues Ribeiro), pp. 8245-8279. [Em linha]. (Consult. 30 Jun. 2021). Disponível em https://dre.pt/home/-/dre/70300353/details/maximized?p_auth=OsYd65lz.

[226] Cf. Art.º 38.º do Decreto n.º 426/XII.

[227] Cf. Art.º 23.º do mesmo Decreto.

procedimento descriminado quanto às matérias requeridas a este órgão[228]. Recordamos que também a composição do Conselho de Fiscalização é composta por três cidadãos de reconhecida idoneidade, eleitos pela Assembleia da República, por voto secreto e maioria de dois terços dos deputados presentes, precedida por uma audição pela comissão parlamentar competente para os assuntos constitucionais, direitos, liberdades e garantias que aprecia, para além do perfil, o currículo dos candidatos. Aqui também constatamos que o Conselho de Fiscalização do SIRP não deixa de ser eleito pela própria Assembleia da República, verificando-se uma descentralização do poder de controlo e supervisão tutelada igualmente pelo próprio Primeiro-Ministro. Para além das competências a que o Conselho de Fiscalização do SIRP está incumbido destacamos o acompanhamento que este órgão tem sobre o conhecimento das modalidades admitidas de permuta de informações entre serviços com outras entidades, especialmente de polícia, incumbidos de garantir a legalidade e sujeitos ao dever de cooperação[229] podendo ainda requerer meios e recursos técnicos que considere necessários e adequados para garantir a autonomia da atividade de inspeção[230].

Neste contexto o relatório da Agência Europeia dos Direitos Humanos (FRA)[231] refere que o principal objetivo dos serviços de inteligência é proteger os valores fundamentais de uma sociedade (aberta) usando métodos ou ferramentas "secretas". É por causa deste paradoxo que os serviços de segurança e inteligência devem ser objeto de responsabilidade democrática e controlo civil. Assim a supervisão/controlo, é o meio de garantir a responsabilidade pública pelas decisões e ações dos serviços de informações de forma a evitar o abuso de poder, legitimar o exercício de poderes intrusivos e alcançar melhores resultados após uma avaliação de ações específicas.

É de consenso geral, e inclusive através de relatórios da Comissão de Veneza[232] bem como de estudos académicos, que a supervisão e controlo deverá ser uma combinação de um controlo por parte do executivo, supervisão parlamentar e uma fiscalização judiciária composta por um corpo de peritos especialistas nestas matérias.

---

[228] Cf. Art.º 37.º do referido Decreto.
[229] Cf. n.º 3 do art.23.º do decreto parlamentar.
[230] Cf. n.º 5 do mesmo artigo.
[231] Relatório da Agência Europeia dos Direitos Humanos (FRA), 2017. Surveillence by intelligence services: fundamental rights safeguards and remedies in the EU. Vol I: Member States´legal framework (consult. 13/08/21). Disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-voi-1_en.pdf.
[232] Relatório sobre a supervisão democrática sobre serviços de segurança. Adotada pela Comissão de Veneza na sua 71ª Sessão Plenária, de 01-02 de junho de 2007. Studies no. 388/2006 e no. 719/2013. CDL-AD(2015)010. II. Proteção dos direitos fundamentais. Segurança, terrorismo e direitos humanos. Disponível em https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)010-e

Como decorre de vários diplomas nacionais, este controlo e fiscalização já existe em Portugal. Como referimos, o Conselho de Fiscalização acompanha e fiscaliza a atividade do Secretário-Geral e dos serviços de informações, velando pelo cumprimento da Constituição e da Lei, com particular incidência em matéria de preservação de direitos, liberdades e garantias.

Por outro lado, a Comissão de Controlo Prévio assegura a concessão de autorização prévia de acesso à informação bancária, fiscal, a dados de tráfego, de localização ou outros dados conexos das comunicações. Tendo ainda em consideração que este pedido de concessão de autorização prévia é apresentado por escrito, indicando a concreta ação operacional, os factos que suportam o pedido, finalidades e razões que fundamentam e aconselham a adoção das medidas requeridas, identificação da pessoa ou pessoas, local onde as medidas devam ser realizadas, duração das medidas requeridas e ponderadas, relevância dos seus fundamentos e salvaguarda dos direitos, liberdades e garantias constitucionalmente previstos. A decisão é da competência do juiz a quem tenha sido distribuído o pedido, podendo haver decisões do coletivo em matérias de particular complexidade sendo que o procedimento é coberto pelo regime de segredo de Estado[233].

Outro órgão é a Comissão de Fiscalização de Dados do SIRP, que exerce através de verificações periódicas dos programas, dados e informações. Perante uma denúncia ou suspeita fundamentada da recolha de dados ilegítima ou infundada. Esta Comissão, apesar de ser parte integrante dos órgãos do SIRP, não deixa de ser constituída por três magistrados do Ministério Público, que elegem entre si o presidente, sendo os seus membros designados e empossados pelo Procurador-Geral da República e com sede na Procuradoria-Geral da República.[234]

Para além destes órgãos de controlo e fiscalização, resultou da Resolução de Conselho de Ministros n.º 188/2017, de 5 de dezembro, o regulamento comum dos Centros de Dados, respetivamente, do SIS e do SIED, tendo em vista a necessidade de aperfeiçoar os procedimentos tendentes à segurança de informações neles processados, e uma uniformização de atuação de modo a contribuir para a melhor prossecução dos objetivos dos serviços de informações e uma mais rigorosa defesa dos direitos individuais das pessoas, facilitando desta forma a atividade dos órgãos de fiscalização.

Nesta abordagem de investigação ao tema a que nos propusemos, consideremos também o importante papel dos órgãos de comunicação social como freio da atividade de inteligência.

[233] Cf. Artigos 35.º, 36.º e 37.º do Decreto n.º426/XII. Nos termos da Lei Orgânica n.º 2/2014, de 6 de agosto.
[234] Cf. Artigo 29.º do Decreto n.º 426/XII.

Importa distinguir jornalismo da atividade de inteligência, pois enquanto os serviços de informações, pela sua própria finalidade e natureza circunscrevem-se à segurança, com vista á prevenção de riscos, e por isso revestem-se de um caráter secreto, já a informação obtida pelos órgãos de comunicação (informação jornalística), indispensável em qualquer Estado de Direito, tem como principal finalidade o direito de qualquer cidadão estar informado e de se informar.[235]

Como descreve Pedro Simões, a relação entre serviços de informações e comunicação social é bastante estreita e tem alguns pontos em comum, nomeadamente o facto de ambos buscarem uma grande quantidade de informações.

Sendo o papel fundamental da comunicação social manter o cidadão informado e inclusive formar opinião pública estes podem exercer em paralelo um papel de "controladores" da atividade de inteligência. Daí, como refere o autor acima referido, deveria de ser "*estabelecida uma via de maior abertura, tornando acessíveis mais factos*", que lhes seja possível retratar o trabalho dos serviços, de uma forma mais transparente.[236]

Joanisval Gonçalves comenta ainda a respeito desta fiscalização e controlo por parte da imprensa (*media*), "que este controlo não deixa de estar restringido pelo sigilo com que operam os serviços de inteligência, de modo que com pouco informação disponibilizada, a atuação desses meios acaba muito limitada"[237].

O que pretendemos com esta exposição é demonstrar que para além dos órgãos e mecanismos de controlo e fiscalização formais[238], possamos acolher também os órgãos de comunicação social a desempenhar uma função de controlo informal monitorando as atividades dos serviços. O exemplo dos EUA surge-nos nesta temática, pois alegadamente a CIA solicitava jornalistas para exercer funções de agentes de informações ou utilizava carteiras profissionais de jornalistas para que os seus agentes fossem considerados jornalistas profissionais, por forma a realizarem investigações e atividades encobertas. Contudo, em Portugal de acordo com o Estatuto de Jornalista[239], o exercício da profissão de jornalista é expressamente incompatível com o desempenho de funções de informações e segurança ou qualquer outro organismo ou cooperação policial.

---

[235] Cf. Pedro Simões, Os Serviços Secretos em Portugal. Os serviços de informação e a comunicação social. Prefácio, 2002, *op.cit.* pp. 94 e 95.
[236] *Idem,* p.92.
[237] Cf. Joanisval Gonçalves, Políticos e Espiões. O Controle da Atividade de Inteligência. 2ª Ed. 2019, *op.cit.* pp. 82 e 83.
[238] Que vão desde o controlo executivo (governo), legislativo (orçamentário, regulamento do centro de dados, comissões de fiscalização, conselhos de fiscalização), administrativo e judicial (comissão de controlo prévio).
[239] Lei n.º 1/99, de 13 de janeiro) na alínea c) do seu artigo 3.º.

Assim, a liberdade de imprensa é garantida nos termos da Constituição e da Lei[240] abrangendo o direito de informar, de se informar e de ser informado, sem impedimentos nem descriminações e ainda não podendo ser impedido ou limitado por qualquer tipo ou forma de censura. Como decorre da Lei da imprensa também impõe-se alguns limites de forma a salvaguardar o rigor e a objetividade da informação, nomeadamente a garantir os direitos ao bom nome, à reserva da intimidade da vida privada, à imagem e à palavra dos cidadãos e a defender o interesse público e a ordem democrática[241].

Reconhecemos que os meios de comunicação poderão ser vistos como "parasitas" da comunidade de inteligência, pois enquanto o primeiro procura divulgar a informação que recolhe e distribuir pelo público em geral, os segundos pautam-se pela descrição e o sigilo. No entanto, apesar do desencontro de interesses, os meios de comunicação social poderão atuar como um verdadeiro desafio à comunidade de inteligência na medida em que colocam os serviços num estado de prontidão e alerta permanente.

Deste modo, nas palavras de Joanisval Gonçalves, "o escrutínio independente exercido pela sociedade civil, com destaque para os meios de comunicação social, pode assim controlar a atividade de inteligência monitorando e denunciando os abusos e cobrando reações dos governantes"[242].

Por último, a este respeito e apesar de todas as medidas constitucionais, legais e regulamentares de controlo, nas palavras do General Pedro Cardoso, "reconhece-se (…) que o controlo mais eficaz é a existência de órgãos de comunicação social verdadeira e inteiramente livres e esclarecidos para criticar a atuação dos serviços e dos seus elementos, detetar os seus pontos fracos e manter uma potencial capacidade de desafio permanente, que contribui poderosamente para a condução das atividades dos serviços dentro da legalidade e do respeito pelas liberdades e garantias constitucionais"[243].

Resumidamente, face a um sistema de controlo do Estado e ainda, por pressão dos órgãos de comunicação social, que poderão dar a conhecimento público atividades dos serviços de inteligência, os Serviços de Informações em Portugal ficaram comprometidos e com pouca margem para efetivamente cometerem abusos.

Desta forma não compreendemos a resistência que existe nas diversas propostas legislativas acerca do acesso aos metadados pelos Serviços, pois apesar de não ser um órgão

[240] Cf. Art.º 1.º da Lei n.º 2/99, de 13 de janeiro – Lei de Imprensa.
[241] Cf. Art.º 3.º da Lei de Imprensa.
[242] Cf. Joanisval Brito Gonçalves, Políticos e Espiões. O Controle da Atividade de Inteligência. 2ª Ed. 2019, *op. cit*. p.85.
[243] Cf. Pedro Cardoso, As Informações em Portugal. 2ª Ed. Gradiva – Publicações IDN. 2004, *op. cit.* p.161.

de fiscalização "formal" os órgãos de comunicação social nunca se excluiriam dessa função (no caso de terem acesso à mesma) portanto, não podermos ter uma posição ingénua para uma realidade que sabemos que existe. Tendo ainda em consideração, que a nível europeu como já referimos, outros países já permitem, com normas bastante claras, que os seus serviços de inteligência possuam e utilizem este meio de recolha de informações. Não olvidando que os papéis importantes dos meios de comunicação garantem igualmente um controlo eficaz dos serviços e dos seus elementos, detetando os seus pontos fracos e mantendo capacidade de desafio permanente na condução das atividades dos Serviços dentro da legalidade e no respeito pelas liberdades e garantias constitucionais.

3. Ingerência abusiva e o acesso aos dados conservados

Tendo em consideração a legislação em vigor relativa ao acesso aos dados de telecomunicações e internet, à sua conservação e tratamento pelos serviços de telecomunicações, propomos uma análise no âmbito da ingerência, por parte dos serviços de informações, nos dados pessoais.

Realçamos ainda a aplicação prática, as divergências e conjunturas que se sobrepõem à atividade de inteligência aquando da recolha de informações de um determinado individuo, com relevantes indícios de associação criminosa e práticas ilícitas no âmbito dos crimes de terrorismo, espionagem, criminalidade organizada e violenta transnacional.

Como referido, as objeções materiais levantadas no Acórdão n.º 464/2019 do TC, circunscreveram-se à escassa densificação da moldura legislativa, no respeito pelo princípio da proporcionalidade, pois estava comprometido por um amplo poder discricionário de intervenções estaduais restritivas de direitos fundamentais. Primeiro, foi considerada uma atuação de natureza administrativa do processo e não judicial; segundo, foi reconhecida uma indefinição relativamente ao papel do Procurador-Geral da República, considerando esta função do MP, com escassa relevância prática; e por último, à dificuldade de exercício do direito de acesso aos dados conservados nos centros de dados do SIS e do SIED, que correspondia a uma competência exclusiva da Comissão de Fiscalização de Dados do SIRP, atuando como intermediário entre o cidadão e os serviços de informações, cabendo aquela comissão ordenar o cancelamento ou retificação de dados recolhidos que envolvam a violação dos direitos, liberdades e garantias consignadas na Constituição e na Lei[244].

[244] Cf. Ponto 11.1.2. – Fundamentos – do Ac. n.º464/2019 do TC.

Feito este enquadramento das questões suscitadas pelo TC, ficou vincado que, qualquer ação preventiva que interfira, no sentido de comprimir ou devassar, quaisquer direitos, liberdade e garantias, não podia ter lugar fora de um processo criminal devidamente formalizado. Assim com "o princípio da proporcionalidade preceitua que este poder do estado, no acesso a dados pessoais dos cidadãos, exige um fundamento preciso e determinado, na lei – princípio da determinabilidade - não podendo ser utilizado para além do estritamente necessário obedecendo aos requisitos da necessidade, exigibilidade e proporcionalidade (strito sensu)"[245].

Como referido no douto acórdão no contexto da Lei Orgânica n.º 4/2017, de 25 de agosto, a natureza preventiva da atividade de recolha e tratamento de dados surge reforçada, e existindo indícios da prática de crimes de espionagem e terrorismo, estes são imediatamente comunicados ao Ministério Público (Procurador-Geral da República) conforme prevê o artigo 13.º daquele diploma. Não obstante das garantias conferidas pelo mesmo diploma, no que se refere ao controlo judicial pela formação das secções do Supremo Tribunal de Justiça, que visam garantir o respeito pelos direitos, liberdades e garantias, por assegurar que as finalidades dos dados recolhidos são explícitos, determinados e legítimos, adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos, também aqui não se entende onde é que não possa estar de facto assegurado ou o (des)respeito pelo princípio da proporcionalidade.

Para além deste controlo, como também já foi referido, a Comissão de Fiscalização de Dados do SIRP, apesar de pertencer à sua estrutura atual, e considerando o facto de encontrar-se na Procuradoria-Geral da República, justificará a imparcialidade necessária e exigível de um órgão de fiscalização, no entanto, não deixa de haver uma fiscalização externa, especializada e independente.

Não obstante, a admissibilidade do pedido só poder ser autorizada quando houver razões para crer que a diligência é necessária, adequada e proporcional sobre um alvo ou intermediário determinado, e ainda a informação ser de difícil ou impossível obtenção em tempo útil para responder a uma situação de urgência, sendo que o processo de autorização de acesso aos dados é sempre comunicado a Procurador-Geral da República[246]. Não ignorando o facto da interconexão em tempo real com as bases de dados dos operadores de telecomunicações, para o acesso direto em linha aos dados requeridos, ser expressamente proibida pelo n.º 2 do artigo 6.º do diploma.

[245] Ponto 11.2.3 do Ac.n.º 464/2019, do TC.
[246] Cf. Art.º 6.º do da Lei Orgânica de acesso aos metadados pelo SIRP.

Esta burocracia procedimental não deixa de ser necessária para evitar abusos e restrições dos direitos, liberdades e garantias. Tendo esta autorização prévia de acesso, ainda ter de passar pela anuência do Secretário-Geral do SIRP contendo os elementos, por escrito, fundamentados, detalhados e circunstanciados conforme prescreve o artigo 9.º daquele diploma.

Quanto à duração do acesso aos dados, também podemos verificar uma previsão determinável relativa à duração das medidas pontuais de acesso requeridas, não podendo exceder o prazo máximo de três meses, renovável por um único período sujeito ao mesmo limite, mediante autorização expressa e desde que se verifiquem os requisitos de admissibilidade.

Ainda quanto á durabilidade de conservação dos dados, defendemos uma maior harmonia de acordo com as diretivas europeias, no que respeita à conservação de dados gerados ou tratados no contexto das operadoras de serviços de telecomunicações, ainda que, a respeito do período de conservação previsto na Lei n.º 32/2008, de 17 julho, seja mais restritivo comparado com a diretiva europeia que previa até dois anos[247], e considerando também o facto de esta mesma Diretiva ter vindo a ser declarada inválida pelo TJUE no caso "Digital Rights[248]".

Quanto à ingerência (propriamente dita) que referimos no âmbito da intromissão dos serviços de informações nos metadados, na produção de informações e prevenção criminal, realçamos também uma preocupação constante, não só do legislador como também do entendimento consensual dos juízes conselheiros do Tribunal Constitucional, de um subprincípio densificado do Estado de Direito Democrático como é o princípio da proibição do excesso.

Como refere Gomes Canotilho, o princípio da proporcionalidade em sentido restrito, ou seja, aquele que pressupõe uma justa medida, implica que uma lei restritiva, "mesmo adequada e necessária, pode ser considerada inconstitucional, quando adote cargas coativas de direitos, liberdades e garantias desmedidas, desajustadas, excessivas ou desproporcionadas em relação aos resultados obtidos"[249].

Ora, como refere o Acórdão n.º 464/2019 do TC, no âmbito das ações de prevenção criminal, a lei não tem previsto intromissões nas comunicações eletrónicas, só podendo ser

[247] Cf. Art.º 6.º da Diretiva 2006/24/CE, de 15 de março de 2006.
[248]Acórdão Digital Rights of Ireland Disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A62012CJ0293.
[249] Cf. José J. Gomes Canotilho – Direito Constitucional e Teoria da Constituição. 7ª Ed. 17ª (Reimp). Coimbra. *op.cit*., p. 457.

autorizado conforme os artigos 187.º e 189.º do CPP e art.18.º da Lei n.º 109/2009, de 15 de setembro, no domínio do cibercrime. Dito isto, a prevenção de um perigo concreto ou repressão de uma infração determinada, a conservação e transmissão de dados têm por finalidade exclusiva a investigação, deteção e repressão de crimes graves. Como afirmado no aresto, a concordância prática entre os valores constitucionais de perseguição e punição de crimes deverá ser feita em sede de processo penal. No entendimento do tribunal os pressupostos enunciados no artigo 6.º da Lei Orgânica n.º 4/2017, revelam-se insuficientes, consubstanciando-se numa incerteza bastante grande sobre os pressupostos de acesso aos metadados, atendendo à singularidade de cada caso concreto (ponto 11.2.4), revelando assim a ausência de instrumentos defensivos que comportem um mínimo de dialética processual.

Com efeito, a intromissão nas comunicações e acesso aos metadados, no âmbito de ação preventiva, foi encarada por aquele Tribunal, como uma abertura de conceitos (alvo determinado, situação de urgência, muito difícil de obter e em tempo útil), dependendo de um juízo de prognose e de uma avaliação que os serviços de informações façam da situação em concreto. Consequentemente, a relevância dos fundamentos do pedido[250] limitava a salvaguarda dos direitos fundamentais concretamente em causa, pelo facto de ser apreciada de acordo com o que os próprios serviços enunciassem no pedido.

Quanto à questão suscitada pelo Tribunal Constitucional, no que respeita à definição do cidadão alvo julgamos que podia ser facilmente ultrapassada na medida em que este acesso circunscrever-se-ia à prevenção de atos de espionagem e terrorismo[251], consequentemente encontrar mos os "critérios objetivos" de seleção dos alvos (como referido no douto Acórdão n.º 464/2019) tendo em consideração a designação e definição dos crimes relacionados com o terrorismo, organizações terroristas ou associação terrorista e espionagem previstas no Código Penal e na Lei de Combate ao Terrorismo[252]. Achamos evidente que o fenómeno da prevenção propícia a uma clara abertura para a conveniência de algumas medidas e que, com efeito se consubstanciaria um descontrolo da circulação do tráfego de dados pessoais. Para o evitar julgamos que algumas medidas de controlo e fiscalização foram garantidas pela Lei Orgânica n.º 4/2017, desde o seu acesso, á comunicação ao Ministério Público e autorização judicial bem como o controlo judicial e autorização prévia do pedido. Por outro lado, aquando na exposição e motivos do Projeto de Lei n.º 480/XIII-2.ª, como também sublinhou o CF-SIRP,

[250] Comunicado ao Ministério Público e dependente de uma autorização prévia e obrigatória, de um coletivo juízes do Supremo Tribunal de Justiça.
[251] Cf. Previsto no art.4.º da Lei Orgânica em apreço.
[252] Cf. Art.º 317.º do CP e Art.os 2.º, 3.º,4.º, 5.º e 5.º- A da LCT.

"as ameaças que os serviços de informações visam detetar e prevenir não desaparecem nem diminuíram, insistindo na grande conveniência em dotar os serviços (…) de meios que lhes permitam detetar tais ameaças, dentro de um espírito de integral respeito pelos direitos, liberdades e garantias e de todos os limites constitucionais e legais à atuação daqueles". Uma vez mais sublinhamos a necessidade e a importância que os serviços devem ter para cooperar, em igualdade de circunstâncias com os serviços congéneres europeus - e demais países que respeitem as exigências do Estado de Direito Democrático - na deteção e prevenção de ameaças terroristas.

No fundo, o que o Tribunal Constitucional e a mais autorizada doutrina defendem relativamente a esta ingerência no caso *subjudice,* julgamos prender-se com o facto de a exigência da adequação, da necessidade e da proporcionalidade (em sentido restrito), revelarem-se ou não, apropriadas para a prossecução dos fins invocados pela lei (em conformidade com os fins). Ou seja, como descreve Gomes Canotilho, "uma medida será então exigível ou necessária quando não for possível escolher outro meio igualmente eficaz, mas menos coativo, relativamente aos direitos restringidos (…). O princípio da proibição do excesso (ou da proporcionalidade em sentido amplo) (…) constitui um limite constitucional à liberdade de conformação do legislador (…), sendo que a Constituição, ao autorizar a lei a restringir direitos, liberdades e garantias, de forma a permitir ao legislador a realização de uma tarefa de "concordância prática" justificada pela defesa de outros bens ou direitos constitucionalmente protegidos (como por exemplo o artigo 27.º da CRP), impõem uma clara vinculação ao exercício dos poderes discricionários do legislador"[253]. Como refere ainda o mesmo autor quanto à liberdade de conformação do legislador, "exige das entidades judiciais de controlo uma relativa prudência quanto á aplicação do princípio da proibição do excesso"[254] que no caso em apreço, conforme prevê a Lei Orgânica n.º4/2017 confere esse controlo judicial a uma formação de juízes do STJ prevista no artigo 8.º da LO.

Quanto ao abuso de ingerência no acesso aos metadados por parte dos serviços de informações, tem-se registado uma malha cada vez mais apertada desde 1985, verificando-se um aumento dos poderes de fiscalização. Com efeito, como referem alguns autores, teoricamente, o Conselho de Fiscalização do SIRP pode fiscalizar tudo e a qualquer momento. Teoricamente porque, se de facto qualquer serviço de inteligência que se preze quiser enganar

[253] Cf. José J. Gomes Canotilho – Direito Constitucional e Teoria da Constituição. 7ª Ed. 17ª (reimp). Coimbra. *op.cit.,* pp. 458 e 459.
[254] *Ibidem*, p.459.

os órgãos de fiscalização, fá-lo-ão certamente[255]. Mas como abordado anteriormente, é necessário que tenhamos confiança, ainda que esta seja relativa, de forma a não tomarmos o normal funcionamento e integridade dos organismos públicos como garantido. Atendendo ainda a um quadro institucional com elevada responsabilidade ética e moral, correspondendo respetivamente a um regime sancionatório coercivo na circunstância da violação dos princípios basilares, que se exige aos funcionários de um organismo como os serviços de informações.

4. Inteligência *"policial"* (investigação criminal) *vs* inteligência *"estratégica"* (intelligence).

"Em 1941, sobre a presidência de Franklin D. Roosevelt, este convocou o Cor. (e mais tarde Maj.Gen.) W. J. Donovan para criar um serviço de inteligência. Reconhecido como o "pai" dos serviços de inteligência dos EUA criou e organizou durante a II Guerra Mundial a OSS (Office of Strategic Services). De acordo com a vasta experiência no terreno do General Donovan, este, frisava a verdadeira importância, a vital significância das comunicações. "*It is useless to collect information unless you can quickly and accurately get it to the user*"[256].

Como refere David Ramalho, "as disposições processuais em matéria probatória estão pensadas, na sua totalidade, para a prova fisicamente visível, palpável e audível"[257]. Contudo, com a evolução jurídica e a adaptação inevitável à nova realidade (digital) e tendências, levou a que por força de circunstâncias, a formulação de um juízo de eficácia, com referência na realidade do mundo físico, valesse igualmente para a realidade virtual. Destacando ainda o autor para o facto de a tendência do nosso sistema processual penal conjugado com a reduzida literacia informática dos juristas, será, por analogia, testar os seus limites na medida em que a realidade tem de ser adaptada ao direito e não o contrário[258]. Com efeito, o resultado desta analogia foi a aplicação das regras do "*mundo físico*" ao "*mundo digital*"[259].

[255] Cf. Carlos Montez Coelho, Direito, Segurança e Democracia, n.º 1, Maio 2021,CEDIS Working Papers, in "As informações em Portugal: Reflexão crítica sobre as secretas e a Constituição", [Consult. 05 set.2021]. Disponível em https://cedis.fd.unl.pt/wp-content/uploads/2021/06/DISED_2021_MAIO-01.pdf
[256] Cf. Allen W. Dulles, *The Craft of Intelligence*. Lyons Press, 2016, *Op.cit*. In personal note. x
[257] Cf. David Silva Ramalho, Métodos Ocultos de investigação Criminal em Ambiente Digital. Almedina, 2009, *op. cit.* p. 240.
[258] *Idem*, p.241.
[259] *Ibidem.*

Realizado este introito cumpre-nos agora caraterizar ou descortinar as diferenças entre a atividade de inteligência prosseguida pelos órgãos de polícia e a atividade de inteligência na sua verdadeira essência (na designada "*intelligence*", aceção clássica).

Fará com certeza todo o sentido realizar um breve enquadramento das finalidades da investigação criminal, que tem como referência a perseguição criminal como atividade auxiliar da justiça penal.

Neste sentido, Guedes Valente carateriza como fim último - o da investigação criminal - a realização efetiva dos fins e interesses da ordem jurídica, subjugados aos princípios constitucionais, permitindo ainda que o processo penal promova a aplicação da lei penal ao caso em concreto, apurando desta forma a verdade material dos factos para que quem julga tenha na sua mão elementos suficientes que determinem a sua vontade no sentido da condenação ou de absolvição[260].

Tomando como referência a declaração de voto no Acórdão n.º 464/2019 do Juiz Conselheiro José Pereira "note-se que estamos, em qualquer caso, perante mundos separados, que atuam com base em racionalidades bem distintas e visando objetivos diferentes, embora, como mundos paralelos que não deixam de ser, designadamente ao lidarem com certos aspetos dos mesmos fenómenos, comunguem algumas dimensões. Tal paralelismo, sugerindo, á superfície, a existência de semelhanças, pode induzir algum enviesamento na diferenciação entre a produção de informações e atividade policial, esquecendo que a essência da diferença, a despeito de uma ou de outra partilha de certos ambientes de trabalho, permanece inequívoca e tem nessa separação uma teleologia própria: evitar mútuas poluições de efeito espúrio contendo a atividade de cada um dos organismos no espaço funcional que lhe é próprio e que justifica o acervo de meios de atuação respetivos"[261].

Não ferindo a autonomia técnica e tática dos OPC na prossecução da investigação criminal – sob a direção e dependência funcional da MP, conforme o Estatuto do Ministério Público (EMP) no seu artigo 4.º, n.º 1, alns. e), o) e p) e artigo 2.º, n.º 4 da LOIC, estes utilizam um conjunto de conhecimentos e métodos de agir, conforme o legalmente admissível na prossecução dos fins de investigação criminal, "respeitando a máxima de que a verdade material não é um bem absoluto que se deve de obter a qualquer custo, pelo que, tudo o que ultrapasse a exigibilidade, a necessidade, a adequabilidade e a proporcionalidade deixa de ser justiça e passa a injustiça"[262].

---

[260] Cf. Manuel Guedes Valente, Teoria Geral do Direito Policial, 5ª ed. Almedina, 2017, *op. cit.* p.463 e ss.
[261] Ponto 2.1.1.
[262] *Idem*, p.498.

Como afirma Guedes Valente, as competências dos OPC no *"quadro jurídico-criminal-processual"*[263], são as medidas cautelares e de polícia previstas na legislação processual-penal. Podendo ainda, de acordo com o previsto no artigo 248.º e ss do CPP, impulsionar e desenvolver atos processuais sujeitos à apreciação e validação por parte da AJ. E, portanto, podem ser considerados [cf. descreve o autor], de "sujeitos processuais acessórios"[264], na estrita medida da sua mera participação enquanto "coadjutores para a descoberta da verdade material"[265], "assumindo-se como protagonistas de intervenções pontuais e específicas, subordinados às autoridades judiciárias competentes"[266].

A investigação criminal carateriza-se então pela finalidade de *"reconstrução jurídica do facto na sua existência histórica, reconstrução que se realiza através do processo penal"*[267]. Por exemplo, relativamente às interceções telefónicas, o CPP vincula a sua admissibilidade apenas durante a fase de inquérito, sendo que o OPC terá de demonstrar a impossibilidade ou dificuldade de obtenção de prova por outros meios. O MP é o responsável pelo requerimento e o JIC terá de fundamentar o seu despacho[268]. Porém, podem ser atribuídos aos OPC[269] a prática de determinados atos da competência do MP, nomeadamente as diligências e investigações relativas ao inquérito, salvo os atos da competência exclusiva do JIC, nos termos dos artigos 268.º e 269.º daquele diploma.

Como defendem alguns autores[270], existem riscos inerentes às delegações genéricas de competências e aos despachos genéricos de delegações de competências consubstanciando-se no fundo, na "policialização da investigação criminal"[271], ou "policialização do inquérito"[272]. Contudo, com a revisão do CPP, em 2007, o legislador veio reforçar a necessidade de controlo

---

[263] *Idem*, p.502
[264] *Ibidem*.
[265] *Ibidem.*
[266] *Idem*, p.503.
[267] Cf. Augusto Silva Dias, Rui Soares Pereira, Sobre a Validade de Procedimentos Administrativos Prévios ao Inquérito e de Fases Administrativas Preliminares no Processo penal. Ed. Almedina, 2018, *op.cit.* p.32. O autor refere ainda, como sustenta Manuel Guedes Valente, "Do ministério público e da polícia: prevenção criminal e acção penal como execução de uma política criminal do ser humano", *Op.cit.*, pp.310 322-324, - a investigação criminal encontra-se dentro de um processo-crime que só existe dentro de uma ação penal", que "no quadro jurídico-constitucional português só é admissível investigação criminal sob tutela judiciária e/ou jurisdicional", apud Manuel Guedes Valente, Teoria Geral do Direito Policial, 4ª Ed. Almedina, 2014, *op. cit*. pp.412-413.
[268] Cf. Carla Costa, "As alteração legislativas e as estatísticas criminais", Revista Semestral de Investigação Criminal, Ciências Criminais e Forenses. Investigação Criminal. N.º 7, 2014. pp. 34-51. Ver também n.º1 do art.187.º do CPP.
[269] Cf. n.º 1 do art.º 270.º do CPP.
[270] Cf. Augusto Silva Dias, Rui Soares Pereira, Sobre a Validade de Procedimentos Administrativos Prévios ao Inquérito e de Fases Administrativas Preliminares no Processo penal. Ed. Almedina 2018, *op.cit.* pp.36-40; e Manuel Guedes Valente, Teoria Geral do Direito Policial, 4ª ed. Almedina, 2014, *op.cit.* pp.504-507.
[271] Cf. Manuel Guedes Valente, Teoria Geral do Direito Policial, 4ª ed. Almedina, 2014, *op.cit*. p.504.
[272] Cf. Augusto Silva Dias, Rui Soares Pereira, cit. p.37, apud José Souto de Moura, "A investigação e as suas exigências no Inquérito", *op.cit*., p.37.

efetivo do inquérito por parte do MP, evitando assim que aqueles despachos de delegação genérica pudessem ser entendidos como uma demonstração fictícia da direção do inquérito pelo MP[273].

Deste modo, questionamos se a realização por exemplo de pré-inquéritos administrativos, são ou não conformes a previsão constitucional e a lei. Augusto Silva e Rui Pereira consideram este tipo de procedimentos feridos de inconstitucionalidade e ilegalidade, louvando o monopólio das autoridades judiciárias.[274] Esta competência das autoridades judiciárias não é beliscada pela tendência de uma investigação criminal assente na prevenção e repressão criminal. Os autores distinguem inclusive os conceitos de prevenção criminal, investigação criminal e repressão criminal, e que apesar de não ser o verdadeiro objeto de investigação, não será com certeza despiciendo e oportuno fazer uma breve alusão a estes conceitos, considerando a confusão concetual e os riscos inerentes às pré-averiguações policiais[275].

Não obstante, julgamos ser comumente aceite que a "*inteligência policial*" poderá ser definida como um "conjunto de ações que empregam técnicas de investigação, procurando confirmar evidências, indícios e obter conhecimentos sobre a atuação criminosa dissimulada e complexa, bem como a identificação de redes e organizações criminosas, de forma a proporcionar um melhor entendimento sobre a maneira de agir e operar, ramificações e alcance das condutas criminosas"[276].

Apoiando-nos na linha de raciocínio de Augusto Silva e Rui Pereira, assistimos, portanto, a uma "instrumentalização do processo penal - na atual sociedade de risco - com finalidades não repressivas, e que em muitos casos, como forma privilegiada para aceder a certo tipo de informações, verificando-se por isso uma subordinação do processo penal a objetivos preventivos da polícia ou dos serviços de informações"[277].

Como temos vindo a assistir nos últimos anos, não só pelos avanços tecnológicos do mundo digital, mas impulsionado também por um investimento cada vez maior por parte das grandes

[273] Cf. Augusto Silva Dias, Rui Soares Pereira, Sobre a Validade de Procedimentos Administrativos Prévios ao Inquérito e de Fases Administrativas Preliminares no Processo penal. Ed. Almedina 2018, *op.cit.,* p.39.
[274] *Idem,* p.41. Apesar de acompanharmos, teoricamente, esta separação de poderes entre o poder judiciário e as polícias, ou seja, entre o controlo e fiscalização efetiva das autoridades judiciárias sobre entidades (qualificáveis ou não como OPC), proibindo assim averiguações preliminares ou atividades de recolha de informação de segurança, não obstante deste entendimento, que se revela essencial do ponto de vista das garantias processuais e na circunstância de uma ponderação de interesses prosseguidos pelo Estado na descoberta da verdade material, difere do conceito da atividade de "inteligência" prosseguida pelos serviços de informações, que como abordaremos mais adiante esta atividade tem uma particular relevância apenas em determinado tipos de crimes.
[275] Cf. Augusto Silva Dias, Rui Soares Pereira, *op.cit.,* p.41.
[276] Conforme no elucida Joanisval Brito Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, *op.cit*. p.38.
[277] Cf. Augusto Silva Dias, Rui Soares Pereira, *op.cit.* p.49.

empresas tecnológicas e também exponenciado pela atual situação pandémica, que tende a criar ao mesmo tempo uma dependência das plataformas digitais, desde as relações laborais (tele-trabalho), das trocas comerciais eletrónicas (e-commerce), negócios eletrónicos (e-business) e do próprio funcionamento da administração pública que cria alternativas cada vez mais diversificadas de atendimento e resolução simplificada, como por exemplo, a renovação de documentos (cartão do cidadão, carta de condução etc..), por outro lado, as próprias reformas refletem muitas vezes soluções que são impostas por novos fenómenos de criminalidade e que dão origem a uma *"«bifurcação do processo penal»*, ou seja a um *«processo penal a duas velocidades»* e ao surgimento de um *«processo penal de exceção»* que se apresenta como alternativa ao designado processo penal clássico sob um sistema de garantias"[278].

É neste sentido que visualizamos uma «*zona cinzenta»*, ou seja, um esbatimento da fronteira entre a investigação e repressão, como atividade própria do processo penal, e a prevenção de perigos como tarefa de polícia.

As fronteiras concetuais entre prevenção criminal, repressão criminal bem como a investigação criminal, têm sido analisadas e debatidas pela doutrina surgindo em legislação extravagante. Contudo, alguns autores referem inclusive que este conceito de "prevenção criminal" poderia ser ampliado a entidades não policiais, designadamente à segurança privada, o que não no nosso entendimento não se evidencia como um facto coerente na sua aplicação, uma vez que se trata de uma "prevenção criminal", ou seja, no âmbito de uma ação com relevância criminal, e portanto, competência atribuída às autoridades judiciárias[279].

Adquirida a notícia do crime, verificamos então, em princípio, a passagem da atividade preventiva da polícia administrativa à atividade repressiva de polícia, passando esta(s) a adquirir(em) o estatuto de órgãos de polícia criminal e de auxiliares do Ministério Público.

Situando a prevenção criminal num momento anterior à consumação ou indício da prática de um crime, evitando por isso que este seja sequer tentado, enfrentamos uma multiplicidade de fatores potenciadores de um possível crime, exigindo diferentes e simultâneos instrumentos de prevenção, quer pelos OPC, quer por polícias administrativas.

Como descreve Eduardo Ferreira, "a lei penal constitui apenas um desses instrumentos"[280] constituindo como tese de prevenção geral, a norma penal, ao proibir um determinado comportamento humano, afirma o seu desvalor do comportamento social em desconformidade

[278] *Idem*, p.49.
[279] Coadjuvadas pelos órgãos de polícia criminal - PJ, PSP e GNR - órgãos estes com competência genérica conforme o disposto do artigo 3.º, n.º 1 da LOIC e também artigo 4.º alíneas a) e b) do mesmo diploma).
[280] Cf. Eduardo Ferreira, "Prevenção do crime na União Europeia", Revista Semestral de Investigação Criminal, Ciências Criminais e Forenses. Investigação Criminal. N.º 7, 2014. pp. 62-71.

com o preceito, significando a vontade do sistema em que não se pratiquem factos em desconformidade com o que a lei impõe ou proíbe.[281]

No âmbito do processo penal como referimos, o despacho previsto no n.º 4 do artigo 270.º do CPP, conferido pelo MP aos OPC, delega quaisquer diligências e investigações relativas ao inquérito, presumindo-se excecional na circunstância de uma atuação preventiva para salvaguarda de bens jurídicos essenciais e preservação de provas.

Conforme nos elucidam os autores Augusto Silva e Rui Pereira, "o quadro de mistura ou confusão de águas e fronteiras, com deslocações verificadas nos domínios da prevenção e da repressão, caraterizado por uma intervenção pró-ativa das polícias que se tende a sobrepor à tradicional resposta reativa, complica este modo de ver e traz como consequência o "esbatimento do que até aqui constituía a marca irredutível e distintiva da investigação/repressão", ou seja, a "reação á suspeita da prática, no passado, de um crime"[282].

Destarte, "os perigos de policialização do inquérito verificam-se associados à crescente atribuição (…) de maiores competências de prevenção criminal às polícias, enfraquecendo a fronteira entre a repressão e a prevenção criminal conduzindo-nos ao designado Estado de Polícia"[283].

Ainda no escopo da inteligência policial, Joanisval Brito lembra que "à função inteligência de uma organização policial compete realizar a coleta de informação sobre atividades de indivíduos e grupos criminosos"[284]. Associando a inteligência básica em algo útil, como a avaliação, análise e a disseminação de material probatório resultante de uma investigação criminal.

O que se pretende com este tipo de inteligência policial, não é a produção de prova material e autoria de crime, uma vez que no caso português, as polícias atuam em conformidade com as disposições e pressupostos de um processo penal, ou seja, quaisquer diligências que firam o núcleo essencial dos direitos, liberdades e garantias fundamentais carecem sempre de uma autorização judicial. Como podemos constatar, o *dominus* para promover o processo penal[285] é o Ministério Público, e portanto, é esta entidade judiciária a quem cabe providenciar todas as diligências dos atos do inquérito[286].Veja-se por exemplo a utilização de agentes encobertos no

[281] Acompanhado aqui com a tese de prevenção geral de Germano M. Silva, Direito Penal Português. Vol. I: Introdução e Teoria da Lei Penal. 3ª Ed. Verbo, 2010, *op. cit.* p.59 e 60.
[282] Cf. Augusto Silva Dias, Rui Soares Pereira, Sobre a Validade de Procedimentos Administrativos Prévios ao Inquérito e de Fases Administrativas Preliminares no Processo penal. Ed. Almedina 2018, *op. cit.* p. 53.
[283] Cf. Augusto Silva Dias e Rui Soares Pereira, *apud* João Conde Correia, "Inquérito: A manutenção do paradigma ou a reforma encoberta", *op.cit.*, p.199.
[284] Cf. Joanisval Brito Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, *op.cit*. p. 39.
[285] Cf. Art.º 48.º do CPP, com as restrições do art.49.º a 52.º.
[286] Cf. Art.º 262.º, 263.º e 267.º do CPP.

âmbito das ações encobertas para fins de prevenção e investigação criminal, um dos requisitos para a realização deste tipo de ações é a de que depende de prévia autorização do competente magistrado do MP, sendo obrigatoriamente comunicada ao JIC e considerando-se a mesma validada se não for proferido despacho de recusa nas setenta e duas horas seguintes[287].

Assim, toda a investigação criminal terá de surgir legitimada e orientada pelos critérios de Estado de Direito, estando a atividade de polícia criminal (a inteligência policial) subtraída aos princípios de Estado de Direito, à constituição e a um sistema normativo (direito processual penal) que defina e condicione o objeto, os objetivos e os limites da sua atuação[288].

Todavia, no que respeita às caraterísticas das diferentes atividades de recolha de informações no âmbito de uma investigação criminal os Estados estão dotados de outras instituições, ou organismos de combate aos fenómenos criminais, nomeadamente os serviços de informações (serviços de inteligência) que dispõem do "*know how",* da longa experiência no terreno durante anos. Apesar de ter existido num contexto de repressão e opressão criminal não poderá ser desprezado o seu conhecimento e contributo aos organismos judiciários e policiais para uma efetiva cooperação no combate aos riscos e à nova criminalidade.

Importa, ainda, fazer uma referência ou melhor distinguir inteligência interna ou doméstica de inteligência externa[289]. A primeira voltada a ameaças internas, designadamente no âmbito de uma investigação criminal, prosseguida pelas autoridades judiciárias e coadjuvadas pelos órgãos de polícia criminal, sujeitos aos pressupostos de um sistema processual penal como forma de realizar o direito penal material, permitindo assim o reconhecimento jurídico da existência de um crime e a aplicação das penas ou medidas de segurança[290]. A inteligência externa é direcionada a alvos estrangeiros incluindo ameaças externas como é o caso do terrorismo, da espionagem e da criminalidade altamente organizada transnacional[291]. Por isso, assistimos à distinção dos serviços de inteligência em países democráticos, organizados e distinguidos claramente pela sua intervenção interna da externa. Relembramos as divisões entre a "CIA e FBI nos EUA; MI6 e MI5, no Reino Unido; Mossad e Shin Bet, em Israel; DGSE e DST, na França, respetivamente, agências de inteligência externa e interna daqueles países"[292]. Existindo entretanto países como o Brasil e o Canadá que não possuindo serviços de

[287] Cf. n.º 3 do Art.º 3.º da Lei n.º 101/2001 de 25 de agosto.
[288] Cf. Augusto Silva Dias, Rui Soares Pereira, Sobre a Validade de Procedimentos Administrativos Prévios ao Inquérito e de Fases Administrativas Preliminares no Processo penal. Ed. Almedina 2018, *op. cit. p.* 55.
[289] Cf. Joanisval Brito Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, *op.cit*. p. 30.
[290] Cf. Manuel Guedes Valente, Teoria Geral do Direito Policial, 5.ª Ed. Almedina, 2017, *op. cit.* p.467.
[291] Atualmente podemos igualmente referir-nos às novas tendências e áreas da "nova criminalidade" nomeadamente, o ciberterrorismo e ciberespionagem.
[292] Cf. Joanisval Brito Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, *op.cit.* p. 31.

informações, atuam no estrangeiro tratando no mesmo organismo a inteligência externa como a inteligência interna[293].

Face à "*guerra de informação*" que temos vindo a assistir nos últimos anos, quer por interesses económicos, ou noutro plano concetual, analisado na perspetiva de conflitualidade das sociedades tecnologicamente desenvolvidas, a competição no domínio da informação poderá ser vista como uma situação de permanente conflito, donde os Estados deverão mobilizar os meios técnicos necessários sem ferir ou de modo a restringir os direitos, liberdades e garantias fundamentais, o mínimo possível na prossecução das políticas criminais e na concertação de medidas de resposta face às ameaças transnacionais.[294]

Considerando que Portugal não dispõe dos meios nem dos recursos necessários para desenvolver programas de interceção e vigilância de comunicações, e ainda para além das restrições constitucionais e legais que se impõem aos serviços de informações, surge-nos os exemplos de casos mediáticos no estrangeiro na utilização destes programas que para além de nos servir de exemplo também são um alerta. Exemplos destes, como já referenciamos, o *Echelon*[295], constituído por uma rede cooperativa de interceção e vigilância de comunicações entre os EUA, Canadá, Reino Unido, Austrália e Nova Zelândia, e que em Outubro de 2000 foi alvo de uma investigação conduzida por uma comissão de inquérito do Parlamento Europeu; o *Carnivore*[296], que consistia num sistema de vigilância eletrónica utilizado pelo FBI para identificar e intercetar comunicações via internet possibilitando a análise de endereços visitados, como também de conteúdos; o *PRISM* [297], que consistia num programa de vigilância eletrónica *massiva* e *data mining* levado a cabo pela NSA[298], que envolvia também a GCHQ[299], tornando-se público com o "*disclosure*"[300] de um antigo funcionário dos serviços de segurança nacional dos EUA.

Segundo a descrição de Joanisval Gonçalves[301], a inteligência estratégica engloba também a formulação de cenários prospetivos com implicações a longo prazo, ou seja, é levada a cabo

[293] Respetivamente aqui se trata da Agência Brasileira de Inteligência (ABIN) e da Canadian Security Intelligence Service (CSIS).
[294] No âmbito do tema "Enquadramento da Utilização Conflitual da Informação" ver, Paulo Nunes, "Sociedade em Rede, Ciberespaço e Guerra de Informação. Contributos para o enquadramento e construção de uma estratégia nacional da informação". 2.ª Ed. IDN, 2016, pp.181-184.
[295] *Idem*, p.181.
[296] Desenvolvido no fim dos anos 90 pelo FBI, que mais tarde foi substituído por um outro software, designado por DCS 1000 a partir de 2001. Disponível em https://tek.sapo.pt/noticias/computadores/artigos/fbi-substitui-carnivore-por-sistemas-comerciais-de-vigilancia-de-emails.
[297] Nome de código atribuído a um programa secreto dos EUA.
[298] *National Security Agency* (NSA).
[299] Serviços de Inteligência do Reino Unido (GCHQ). Disponível em https://www.gchq.gov.uk/.
[300] Tradução: divulgação.
[301] Cf. Joanisval Brito Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, *op.cit.* p. 65 e ss.

com a prospeção de assessorar o poder político. Por exemplo, permite a definição das políticas criminais e a implementação de estratégias de combate ao terrorismo transnacional. É com esta categoria de "*intelligence"* que julgamos ser possível analisar com maior precisão e prever cenários de conflito em que a segurança interna e os interesses nacionais estejam grandemente ameaçados.

Contudo, defendemos que esta perceção clássica da atividade de inteligência encontra-se mais associada à inteligência de Estado, uma vez que está destinada a subsidiar a elaboração de planos militares e políticos no âmbito nacional e internacional.

Não obstante desta definição de inteligência "estratégica", podemos também englobar a designada recolha de informações voltada para a prevenção de atos ou atividades de espionagem, sabotagem e subversão, incluído o terrorismo, com o fim de minar a segurança de um país. Como referia o General Pedro Cardoso, "para se estar em condições de fazer face á ameaças que comprometam a segurança nacional, existe uma efetiva necessidade de manter os serviços de informações com plena capacidade de pesquisa, sobre as capacidades, a oportunidade de desencadeamento de ações e as probabilidades de sucesso das organizações, dos movimentos, das frentes e de grupos potencialmente hostis"[302].

Apesar de haver uma área nebulosa entre as atividades prosseguidas pelos serviços de informações (no âmbito da inteligência interna) e aquelas de caráter estratégico realizadas pelos órgãos de polícia criminal, elas não se confundem. A primeira envolve dados e produz conhecimento, com o objetivo de assessorar o processo decisório quer ao nível estratégico na prossecução e definição de estratégias de combate à criminalidade altamente organizada, espionagem e terrorismo, quer na adoção de medidas concretas no âmbito de outros quadros funcionais. A segunda assenta essencialmente, "na evidente diferença estrutural com a perseguição penal, que parte do conhecimento de uma realidade fática específica, expressa na existência ou indiciação de um crime em concreto, sendo desencadeada e orientada retrospetivamente por este, adjetivando um resultado consequencialmente previsto por essa ocorrência"[303].

Suportamos, ainda, a distinção entre os serviços de informações e os órgãos de polícia criminal com a descrição elucidativa do Juiz Conselheiro José Pereira no Acórdão n.º 464/2019 do TC quando descreve: "pressupõe a função policial, quando direcionada à adjetivação penal,

[302] Cf. Pedro Cardoso, As Informações em Portugal. 2ª Ed. Gradiva – Publicações IDN. 2004, *op. cit*. p. 267.
[303] Cf. Ac. TC n.º 464/2019 de 21/10/2019, (Lino Rodrigues Ribeiro), pp. 5-124 [Em linha]. (Consult. 19 Set. 2021). Disponível em https://dre.pt/home/-/dre/125515884/details/maximized. Vide declaração de voto do Juiz Conselheiro José Pereira (ponto 2.1.1.1)

elementos factualmente expressos, indutores de uma objetivação comportamental que afastam o essencial dos elementos de incerteza e de fluidez na referenciação concreta que observamos nas situações indicadas (risco, incerteza e ignorância) como correspondendo ao espaço próprio da atividade de produção de informações e, consequentemente, de atuação dos serviços de informações. (…)"[304]Por outro lado, "sobrevaloriza-se na visão que tende a confundir produção de informações e atividade policial (o qual reputamos de inadequada a qualquer das duas atividades e estranha ao nosso modelo constitucional) a presença circunstancial do que qualificamos como "pontos de contato" - áreas de proximidade – entre as duas funções. Como efeito, embora ocorram, em algumas situações, coincidências temáticas no material fáctico de base tratado pelas duas atividades, não afasta esta incidência, longe disso, a profunda diferença de lógicas e de objetivos visados por cada uma das funcionalidades e das estruturas que as protagonizam. Esta confusão entre serviços de informações e autoridades policiais, que é gerada por aparências enganadoras e, em grande medida, alimentada por mitos, deve ser esclarecida, descodificando-se o sentido que tais "pontos de contato" apresentam numa democracia constitucional, cujo quadro referencial é absolutamente incompatível da confusão, ou apropriação funcional mútua"[305].

É no entanto, importante salientar a relevância quanto à cooperação entre os serviços de informações e as autoridades policiais (OPC´s), mormente, levando em consideração a especial complexidade das investigações, e produção de prova no âmbito da cibercriminalidade. Assim como, não ignoramos que as redes de organizações criminosas atuam cada vez mais de forma autónoma, mas, ao mesmo tempo, com propósitos semelhantes. Com o objetivo de fomentar a instabilidade e descridibilidade das instituições Estatais, levando muitas vezes à imergência de justificados receios na sociedade de um Estado de Direito Democrático. É importante também referir os efeitos que poderão ser desencadeados ao nível económico e no combate à criminalidade económico-financeira, que têm custos avultados no erário público e privado.

Defendemos que os meios e recursos que o Estado disponibiliza para concertar ou desenvolver mecanismos de combate a esta criminalidade revelam-se muito maiores, do que se o Estado pudesse antecipar a sua consumação, monitorizando de forma progressiva e metodicamente a produção de informações pelos Serviços. Esta monitorização passava naturalmente por uma regulamentação (própria e direcionada para a utilização destes meios)

[304] Cf. Ac. TC n.º 464/2019 de 21/10/2019, (Lino Rodrigues Ribeiro), pp. 5-124 [Em linha]. (Consult. 19 Set. 2021). Disponível em https://dre.pt/home/-/dre/125515884/details/maximized . Vide declaração de voto do Juiz Conselheiro José Teles Pereira (ponto 2.1.1.2)
[305] *Ibidem.*

mais detalhada e discriminada na utilização dos métodos de obtenção de informações, salvaguardando os direitos, liberdades e garantias fundamentais individuais, possibilitando uma escalada progressiva de acordo com a necessidade (de saber), adequação, proporcionalidade e exigibilidade.

Como já aconteceu anteriormente, não muito distante, a sobreposição de funções excede a mera proximidade, e negamos o paralelismo, que corresponde a um modelo de regimes totalitários, que se traduzia frequentemente no que se designava como polícia política.

O modelo e enquadramento legal dos serviços de informações, quanto ao acesso aos metadados, encontra-se atualmente adjetivado na Lei Orgânica n.º 4/2017 e na legislação extravagante referente à proteção e tratamento dos metadados. Como citou o Juiz Conselheiro José Pereira no douto acórdão do TC, "recorrendo ao exagero retórico de Richard Posner em repudiar a mesma ideia: "*they are intelligence agencies, opertaing by surveillance rather than by prossecution. Critics who say that an American equivalente of MI5 wold be a Gestapo understand neither MI5 nor the Gestapo*"[306].

Não faz por isso sentido algum relacionarmos ou colocarmos no mesmo "*padrão*" a atividade prosseguida por um serviço de informações da de uma autoridade policial, atuando esta última num quadro de perseguição criminal. Também não consideramos que comportaria menos riscos relativamente à proteção dos direitos fundamentais do que a atuação de um serviço de informações, no seu espaço funcional legítimo num regime democrático.[307] A circunstância de a perseguição criminal se realizar exclusivamente no âmbito de um processo penal, com todas as devidas formalidades e respeito pelos princípios adjacentes num Estado de Direito Democrático – que como já referimos, expressamente vedada aos serviços de informações -, "corresponde á forma de atuação do Estado com maior potencial agressivo sobre os direitos individuais: a que conduz á aplicação de sanções criminais e pode desenvolver, *in itinere,* a sujeição a medidas de coação fortemente compressoras dos direitos individuais"[308].

De modo a concluirmos a diferença inequívoca da atividade prosseguida pelos serviços de informações, chamamos á colação a caraterização da atividade de produção de informações citada no referido acórdão de 2019 expressando que "os serviços de informações […] atuam num plano que antecede à atividade policial de controlo de perigos. O propósito da sua atuação não obedece ao objetivo direto de implementar medidas de controlo de perigos de investigação. As informações por si reunidas visam antes fundar a avaliação e decisão políticas que depois

[306] *Idem* (ponto 2.1.1.2).
[307] *Idem* (ponto 2.1.1.2).
[308] *Ibidem.*

se manifestarão de diversos modos, por exemplo, através da criação de procedimentos contra associações ou partidos contrários à Constituição ou do desenvolvimento de programas sociais destinados a pessoas sujeitas a extremismos de vária ordem. Compreende-se, assim, que os serviços de informações não tenham típicas competências de polícia, mas apenas a competência de mobilizar meios tendentes à captação e tratamento de informação"[309].

CAPÍTULO III – A INTERCEÇÃO DE COMUNICAÇÕES NOS ORDENAMENTOS JURÍDICOS DOS SERVIÇOS DE INFORMAÇÕES CONGÉNERES FACE À PROTEÇÃO DA CONVENÇÃO DOS DIREITOS FUNDAMENTAIS.

1. Relatório da Agência Europeia dos Direitos Fundamentais

1.1 Quadro Europeu

Proteger o público de ameaças genuínas à segurança e salvaguardar os direitos fundamentais envolve um equilíbrio delicado e tornou-se um desafio particularmente complexo nos últimos anos. Os ataques terroristas desencadearam medidas amplas que permitem aos serviços de inteligência lançar redes cada vez mais amplas na esperança de prevenir mais violência. Ao mesmo tempo, a era digital produziu inovações tecnológicas facilitando a comunicação de dados em grande escala e monitorização - o que poderia facilitar o seu abuso. Estes desenvolvimentos afetam uma variedade de direitos fundamentais protegidos pela legislação da União Europeia (UE), em particular os direitos à privacidade e à proteção de dados, consagrados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, e nos tratados e diretivas da UE.

As revelações de Snowden demonstraram esforços extensos e indiscriminados de vigilância em todo o mundo, destacando que as violações desses direitos não são meramente uma preocupação teórica. A magnitude da atividade de inteligência descoberta despertou inquietação e ressaltou a importância de manter mecanismos eficazes para ajudar a prevenir a violação dos direitos fundamentais.

[309] Cf. Ac. TC n.º 464/2019 de 21/10/2019, (Lino Rodrigues Ribeiro), pp. 5-124 [Em linha]. (Consult. 19 Set. 2021). Disponível em https://dre.pt/home/-/dre/125515884/details/maximized. Vide declaração de voto do Juiz Conselheiro José Teles Pereira (ponto 2.1.1.2) *apud* Manuel Nogueira de Brito "Direito de Polícia", Tratado de Direito Administrativo Especial, (Coords. Paulo Otero, Pedro Gonçalves) Vol. I, Coimbra, 2009, pp. 320-321.

O Parlamento Europeu exortou a Agência Europeia dos Direitos Fundamentais (FRA) a investigar exaustivamente a proteção dos direitos fundamentais no contexto da vigilância, em particular em termos das vias de recurso disponíveis.

O relatório da FRA[310] constituiu a primeira parte da resposta a este pedido visando apoiar a adoção e implementação significativa de mecanismos de supervisão na UE e nos seus Estados-Membros - analisando os quadros jurídicos sobre vigilância em vigor, centrando-se na chamada «vigilância em massa», que apresenta um potencial particularmente elevado de abuso. O relatório não avaliou a implementação das respetivas leis, em vez disso, mapeou os quadros jurídicos relevantes nos Estados-Membros, procurando detalhar os mecanismos de supervisão introduzidos em toda a UE. Assim, descreveu o trabalho das entidades encarregadas de supervisionar as medidas de vigilância e apresentar os vários remédios disponíveis para indivíduos que procuram desafiar tais atividades de inteligência.

Os resultados da pesquisa apresentados demonstraram as complexas considerações envolvidas na proteção dos direitos fundamentais no contexto da vigilância.

Encontrar um equilíbrio entre a proteção da segurança nacional e o respeito para os direitos fundamentais é um desafio que requer um debate exaustivo, completo e complexo.

Esta pesquisa constituiu a primeira etapa de resposta ao pedido do Parlamento Europeu (PE), e forneceu uma visão geral dos quadros jurídicos dos Estados-Membros da UE em matéria de vigilância.

A FRA consolidará ainda mais as suas conclusões jurídicas com pesquisa de campo fornecendo dados sobre a implementação diária dos marcos legais. Enquanto o PE solicitou à FRA que estudasse o impacto de "Vigilância"' dos direitos fundamentais.

O PE refere-se a "Sistemas de longo alcance, complexos e altamente tecnologicamente avançados projetados pela Inteligência dos EUA e de alguns serviços dos Estados-Membros para recolher, armazenar e analisar dados de comunicação, incluindo dados de conteúdo, dados de localização e metadados de todos os cidadãos ao redor do mundo, em uma escala sem precedentes e de forma indiscriminada e não suspeita"[311]. Esta definição abrange dois aspetos essenciais: primeiro, uma referência a uma técnica de recolha e, em segundo lugar, a distinção entre recolha direcionada e não direcionada. O que se visou não foram as técnicas de vigilância em si, mas sim os marcos legais que permitem essas técnicas. Para os Estados-Membros que

[310] Relatório da Agência Europeia dos Direitos humana (FRA), 2017. Surveillence by intelligence services: fundamental rights safeguards and remedies in the EU. Vol. I: Member States´legal framework (consult. 20 set. 2021). [Disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-voi-1_en.pdf

[311] *Ibidem.*

realizarem inteligência de sinais (SIGINT), o foco da análise é nesta capacidade, e não em outras capacidades intrusivas (como a escuta telefónica).

Embora a premissa seja a existência de uma interferência, uma vez que a "monitorização secreta das comunicações" interfere nos direitos de privacidade do ponto de vista dos direitos fundamentais, assume-se, portanto, que permanece um direito legal do respeito pela privacidade das comunicações digitais - não podendo ser contestado[312]. A adoção de vigilância em massa na tecnologia, sem dúvida, colide com a própria essência deste direito.

A análise no quadro jurídico dos Estados-Membros da UE tenta manter a aplicação da lei e informações, serviços separados. Ao fazer isso, reconheçamos que fazer essa divisão nem sempre é fácil. Os governos permanecem em conflito quanto à maneira adequada de lidar com os alegados terroristas, o imperativo de detetar e prevenir o terrorismo levará a uma cooperação cada vez maior entre diferentes partes do governo. "A resolução do PE reconhece este facto e exortou o Órgão Comum de Supervisão (ICC) da Europol a inspecionar se as informações e os dados pessoais compartilhados com a Europol foram legalmente adquiridos pelas autoridades nacionais, especialmente se os dados foram inicialmente adquiridos por serviços de inteligência na UE ou num terceiro país"[313].

Contudo, as revelações de Snowden também levantaram a questão sobre a cooperação entre os serviços de inteligência. "Esta questão, importante para a supervisão das atividades dos serviços de inteligência, foi abordado na resolução do Parlamento Europeu (PE) por órgãos de supervisão e pela Comissão de Veneza"[314].

Ao nível da UE, os direitos à privacidade e à proteção de dados estão consagrados nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia. O direito à proteção de dados também é estabelecido no Artigo 16.º do Tratado sobre o Funcionamento do União Europeia (TFUE), e no artigo 39.º do Tratado da União Europeia (TUE). São também instrumentos legais relevantes, a Diretiva de Proteção de Dados (UE), 2016/679/ do Parlamento e do Conselho, a

[312] A Organização das Nações Unidas adotou o projeto de resolução "O direito à privacidade na era digital", apresentado pelo Brasil e a Alemanha. O que significou que a ONU utilizou o modelo brasileiro baseado no Marco Civil da internet. A iniciativa da organização, aprovada pela Terceira Comissão da Assembleia Geral das Nações Unidas (ONU), aconteceu um ano após a adoção da Resolução 68/167, também apresentada pelos dois países. O documento aprovado reiterou a necessidade de proteção ao direito à privacidade no contexto da vigilância e da coleta de dados das comunicações digitais.
A resolução contou ainda com o patrocínio de 64 países. Disponível em https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167%20

[313] Relatório da Agência Europeia dos Direitos Humanos (FRA), 2017. Surveillence by intelligence services: fundamental rights safeguards and remedies in the EU. Vol. I: Member States´legal framework (consult. 20 set. 2021). Disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-voi-1_en.pdf

[314] *Idem.*

Diretiva da Privacidade Eletrónica, 2002/58 /CE e a Diretiva (UE) 2016/680[315] sobre a proteção pessoal dos dados tratados no âmbito da cooperação policial e judiciária em matéria penal. Estes instrumentos asseguraram, entre outros[316], que em seu respetivo âmbito de aplicação, o processamento de dados pessoais é realizado legalmente e apenas na medida necessária para o cumprimento do objetivo legítimo prosseguido. De acordo com o artigo 52.º, n.º1 da Carta, qualquer limitação a este direito deve ser necessária e proporcionada, cumprir genuinamente os objetivos do interesse geral reconhecido pela União, ser prestado por lei, e respeitar a essência de tais direitos.

O artigo 4.º, n.º 2 do TUE, prevê que "*a segurança nacional continua sendo a única responsabilidade de cada Estado-Membro da UE* ".

Os limites da isenção de segurança nacional são sujeitos a debate, inclusive em relação às atividades dos serviços de inteligência. Apesar de não haver um entendimento uniforme de "segurança nacional" em toda a UE, o conceito não sendo um conceito definido de forma detalhada na legislação da UE ou na jurisprudência do TJUE, o TJUE declarou que as exceções aos direitos fundamentais devem ser interpretadas de forma estrita e justificada. O TJUE também afirmou que o mero facto de que uma decisão diz respeito à segurança do Estado não torna a lei inaplicável. A falta de clareza sobre o escopo preciso da isenção de segurança está aliada hás múltiplas áreas do direito e da segurança nacional de cada Estado Membro. Isto é particularmente verdadeiro com o contra terrorismo, uma vez que o terrorismo é geralmente considerado uma ameaça para a segurança nacional, à lei e à ordem pública.

Como resultado, a divisão de competências entre inteligência e autoridades policiais variam ao longo do Estados-Membros da UE, bem como as modalidades dos seus intercâmbios de informações.

A falta de uma clara delimitação entre a "ordem pública" e "segurança nacional" influência o debate sobre a renovação da Estratégia de segurança interna da UE em relação à troca e uso de inteligência existente para combater ameaças terroristas.

Embora seja um mecanismo dedicado dentro das estruturas da EU, o Centro de Análise de Inteligência da UE, INTCEN e até certo ponto, também o Centro de Satélites da UE, existe um

[315] Esta diretiva foi transposta para o direito nacional pela Lei n.º 59/2019, de 8 de agosto, que aprovou as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais.

[316] Vide também o Regulamento (UE) 2016/681 do Parlamento e do Conselho, 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, e a Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015 relativo ao procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade de informação.

intercâmbio de informações entre autoridades de inteligência nacional, de forma voluntária e *ad hoc*, e em grande parte fora do quadro jurídico da UE. O que é conhecido sobre o intercâmbio de informações neste campo é necessariamente limitado, uma vez que grande parte dele é protegido do escrutínio público.

A ação coordenada a nível da UE limita-se, portanto, ao reforço do intercâmbio de informações sobre a aplicação da lei, com ênfase na melhor utilização do potencial do Serviço Europeu de Polícia (Europol)[317], como também pela Agência Europeia de Gestão da Cooperação Operacional nas Fronteiras Externas dos Estados-Membros da União Europeia (Frontex)[318].

A isenção de segurança nacional fornece um desafio metodológico devido à falta de uma delimitação clara entre as atividades de vigilância conduzidas por lei, fiscalização e para fins de segurança nacional.

Este delineamento, pouco claro, de "segurança nacional" também tem repercussões para a aplicabilidade do direito da UE, que depende da interpretação do propósito da isenção de segurança nacional e das características específicas dos vários programas de vigilância, realizados pelos serviços de inteligência. No entanto, as existências de tais programas permanecem em grande parte desconhecidos, mesmo com as revelações de Snowden, alguns contêm elementos que podem justificar a plena aplicabilidade da legislação da UE.

Por exemplo, quando as empresas da UE transferem dados para serviços de inteligência, incluindo os de países terceiros, alguns deles são considerados pela Diretiva de Proteção de Dados como controladores de dados que recolhem e processam dados para seus próprios fins comerciais. Qualquer subsequente atividade de processamento de dados relaciona se particularmente sobre as trocas mais eficazes de inteligência dentro e entre os Estados

[317] O sistema de informações da Europol (SIE) é a base de dados central de informações e informações criminais que abrange todas as áreas de criminalidade mandatadas pela agência, incluindo o terrorismo. Este sistema (SIE), para além de ser utilizados pelos funcionários e agentes de ligação dos Estados Membros bem como por peritos nacionais destacados na sede da Europol, alguns dos parceiros de cooperação da Europol podem armazenar e consultar dados através do centro operacional da Europol.
Quanto aos dados inseridos SIE permanecem sob o controlo total da entidade que os introduz e não podem ser alterados de alguma forma pela agência ou Estado Membro. Sendo que o proprietário é responsável por garantir a precisão e confiabilidade dos dados, verificar os prazos de armazenamento dos dados e garantir que os dados estejam atualizados. Por norma, os utilizadores da Europol e das unidades nacionais, têm acesso direto a todos os dados armazenados no sistema mas o proprietário dos dados pode limitar esse direito caso a caso. Disponível em https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system

[318]O apoio da Agência Europeia da Guarda Costeira e de Fronteiras (FRONTEX) nas fronteiras externas ajuda a garantir a liberdade de circulação sem controlos nas fronteiras internas contribuindo para o desenvolvimento da gestão das fonteiras na Europa assente em três grandes objetivos estratégicos: reduzir a vulnerabilidade das fronteiras externas; garantir a segurança e o bom funcionamento das fronteiras da UE e planear e manter as capacidades da Guarda Costeira e de Fronteiras europeias. Disponível em https://frontex.europa.eu/

Membros, pois podem prevenir ataques terroristas por parte de pessoas já conhecidas pelas autoridades nacionais, como era alegadamente o caso dos ataques perpetrados em 2014 (Bruxelas) e 2015 (Paris).

Outro exemplo, por meio do *Clube de Berna*[319] e seus derivados grupos de contra terrorismo (Counter Terrorist Group), um fórum de compartilhamento de inteligência, concentra-se especificamente em inteligência de contra terrorismo e abrange todos os Estados Membros da UE, bem como a Noruega e Suíça.

Quaisquer limitações dos direitos de privacidade juntamente com a proteção de dados pessoais devem ser examinadas de acordo com a legislação Europeia relativa às Diretivas de Proteção de Dados e a Carta. Tais limitações devem ser tratadas como exceções à proteção de dados pessoais, e portanto, sujeitas à interpretação restrita requerendo uma justificação adequada. A essência do direito de privacidade e proteção de dados pessoais deve ser respeitada. A exceção de "segurança nacional", não pode, portanto, ser vista como uma possibilidade de exclusão da aplicabilidade de Direito da UE. Como o revisor independente do terrorismo no Reino Unido colocou: "A segurança nacional continua a ser da responsabilidade única de cada Estado-Membro: mas sujeita a isso, qualquer legislação do Reino Unido que rege a intercetação ou comunicação de dados é provável ter que cumprir com a Carta da UE porque constituiria uma derrogação das diretivas da EU"[320].

Quando o direito da UE não se puder aplicar, outros instrumentos internacionais, se aplicaram, tais como a CEDH, a Convenção 108 de 1981 e o seu Protocolo Adicional de 2001.

1.2 A prática de recolha de dados pela comunidade de inteligência

Para analisar o trabalho dos serviços de segurança e informações na UE, como já foi abordado nesta investigação, relembramos uma breve descrição desses serviços e suas funções essenciais: "serviços de inteligência" são agências com foco em ameaças externas (eles têm um mandato estrangeiro), enquanto "Serviços de segurança" são agências com foco em ameaças internas, ou seja pelos serviços domésticos, com um mandato interno.

[319] Disponível em https://aboutintel.eu/the-club-de-berne/

[320] Relatório da Agência Europeia dos Direitos Humanos (FRA), 2017. Surveillence by intelligence services: fundamental rights safeguards and remedies in the EU. Vol. I: Member States´legal framework (consult. 26 set. 2021). Disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-voi-1_en.pdf

A este respeito a terminologia genérica refere-se a "serviços de inteligência" para ambos. Como referenciado no relatório da FRA[321], Born e Wills sugerem a seguinte definição de um serviço de inteligência: “Uma organização estatal que coleta, analisa e divulga informações relacionadas a ameaças à segurança nacional”. A linha entre ameaças “estrangeiras” e “domésticas” costuma ser confusa, como é o caso das atividades terroristas, que muitas vezes são de caráter transnacional, fruto dos grandes fluxos migratórios.

Como resultado, a estreita cooperação entre serviços com mandato nacional e serviços com mandato no estrangeiro é vital. Um relator especial da ONU para a promoção e proteção dos direitos humanos e liberdades fundamentais enquanto combate ao terrorismo, adotou a mesma abordagem, considerando que as práticas da ONU podem ser aplicadas a internos, externos, serviços civis e militares[322]. Os serviços de inteligência são organizados em diferentes agências com base no seu mandato. O quadro centra-se apenas nos serviços, e não nos órgãos de coordenação que possam existir nos Estados-Membros, tais como o Departamento de Informações de Segurança (DIS) em Itália ou o Coordenador Nacional de Inteligência em França, que faz parte da comunidade de inteligência francesa. Além disso, as diferenças entre atividades internas e externas não devem ser sobre enfatizadas, uma vez que a vigilância da comunicação digital não reconhece necessariamente as fronteiras geográficas.

Acima de tudo, a cooperação entre agências de aplicação da lei e agências de segurança nacional (serviços de inteligência), só pode acontecer sob a regra da Lei, se ambas agirem de acordo com os princípios do Estado de Direito, definindo estruturas legais claras e inequívocas.

Para além do principal objetivo dos serviços de inteligência consubstanciar-se na recolha, análise e disseminação de informações, por forma a auxiliarem os decisores políticos na tomada decisões e medidas para proteger a segurança nacional, também inclui a proteção da população e a salvaguarda do respeito pelos direitos humanos. Relembramos que qualquer serviço de inteligência encontra-se expressamente proibido de violar a Constituição ou as Leis internacionais de Direitos Humanos, estendendo-se não apenas à realização de ações no seu território nacional, mas também nas atividades no exterior.

1.3 Medidas de vigilância e gestão de dados pessoais

[321] Relatório da Agência Europeia dos Direitos Humanos (FRA), 2017. Surveillence by intelligence services: fundamental rights safeguards and remedies in the EU. Vol. I: Member States´legal framework (consult. 26 set. 2021). p.13 (58). Disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-voi-1_en.pdf

[322] *Idem.*

A recolha técnica é tradicionalmente distinta da recolha humana que ocorre no terreno.

Como anteriormente referenciado, as fontes de recolha de dados são diversificadas, mas a recolha automatizada de informações por meio de interceção e coleta de dados digitais – relacionados com a atividade de inteligência, baseia-se em quatro pilares principais: 1) criptografia, ou de-criptografia de comunicações; 2) inteligência de sinais (SIGINT); 3) imagens ou foto-inteligência (IMINT); e 4) inteligência digital. Na era digital, esses quatro pilares tendem a desaparecer, sendo fundidos em um único conceito, "inteligência de rede digital" (DNI).

De acordo com a Comissão de Veneza[323], "SIGINT é um termo coletivo referindo-se a meios e métodos para a intercetação e análise de rádio (incluindo satélite e telefone celular) e comunicações por cabo". Não obstante, as origens do SIGINT derivou dos serviços militares de inteligência. Na verdade, o SIGINT era tradicionalmente usado por serviços de inteligência militar e estrangeira para prevenir ações militares que punham em risco a segurança nacional.

A capacidade de intercetar comunicações é muito importante, porque dá uma visão sobre o que está a ser dito, planeado e considerado.

Com o desenvolvimento das comunicações digitais, as fronteiras nacionais, são mais difíceis de identificar, ou seja, as indicações do que é estrangeiro e do que é nacional. Além disso, as ameaças à segurança nacional não são apresentadas apenas por Estados, mas também por grupos terroristas e redes de crime organizado. Já que a luta contra o terrorismo levou a serviços de segurança (interna) a usarem o SIGINT.

Assim, as legislações nacionais deveriam descrever os tipos de recolha de dados disponíveis aos serviços de inteligência, os objetivos permissíveis para a recolha e análise de informações, as categorias de pessoas e atividades que podem estar sujeitas à recolha de informações, o limite de suspeita necessário para justificar o uso de medidas de recolha de dados que podem ser utilizados e os procedimentos para autorizar, supervisionar e rever o uso de medidas de recolha de informações. Para além do dever de estar publicamente disponível, quanto à descrição de dados pessoais que os serviços de inteligência podem conter e quais os critérios que se aplicam ao uso, retenção, exclusão e divulgação desses dados, é permitido ainda reter esses mesmos dados para os fins estritamente necessários para o cumprimento da sua missão[324].

---

[323] Relatório sobre a supervisão democrática sobre agências de inteligência de sinais. Adotada pela Comissão de Veneza na sua 102ª Sessão Plenária, de 20-21 de março de 2015. Study no. 719/2013. CDL-AD (2015) 011. II. Proteção dos direitos fundamentais. Segurança, terrorismo e direitos humanos. Disponível em https://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2015)011-e .

[324] De acordo com as boas práticas de recolha de informações, gestão e uso dos dados pessoais pelos serviços de informações (práticas 21 e 22). Disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services-voi-1_en.pdf

O relatório da FRA sugere ainda que se realizam avaliações regulares da relevância e exatidão dos dados pessoais que detêm, sendo obrigados a excluir qualquer informação que seja considerada imprecisa ou que deixe de ser relevante, para boas práticas de recolha de informações pelos serviços de inteligência, gestão e uso dos dados pessoais (prática 24).

1.4 Centro de Análise de Inteligência da União Europeia (EU INTCEN).

A criação da UE INTCEN[325] – ou Centro de Situação da EU (EU SITCEN) como era designado até 2012 – está intimamente ligado ao estabelecimento da Política Europeia de Segurança e Defesa (PESD) e à criação do cargo de Alto Representante em 1999[326]. O desenvolvimento das capacidades de gestão de crises da PESD e a implantação de missões civis e militares deixou claro que era necessária uma estrutura de análise de inteligência. Após o 11 de setembro de 2001, e as crescentes ameaças do terrorismo, também enfatizou a necessidade de uma análise de inteligência oportuna e precisa para apoiar a formulação de políticas da UE.

Em 2002, ano em que foi estabelecido o EU SITCEN, foram destacados membros dos serviços de inteligência dos estados para o SITCEN da UE.

Em 2005, a UE SITCEN foi reforçada com uma equipa de especialistas antiterroristas destacados pelos serviços de segurança dos Estados-Membros, permitindo fornecer ao Conselho avaliações de ameaças de terrorismo estratégico com base em inteligência de serviços nacionais.

Em 2007, o SITCEN da UE reforçou a sua colaboração com a Diretoria de Inteligência do Estado-Maior Militar da UE, concluindo uma concertação funcional, designada por Análise da Capacidade Única de Inteligência (SIAC). Visando que todas as avaliações de inteligência emitidas para os Estados-Membros são produtos conjuntos preparados de acordo com o SIAC.

Em 2011, o SITCEN da UE foi transferido para o Serviço Europeu de Ação Externa (SEAE), seguido no ano seguinte, de mudanças organizacionais e renomeado para Centro de Análise de Inteligência da UE (EU INTCEN).

As principais tarefas e funções do EU INTCEN centram-se essencialmente em fornecer informações exclusivas que não estão disponíveis abertamente, com base nas contribuições dos serviços de inteligência e segurança dos Estados-Membros, em fornecer avaliações e briefings

[325]Disponível em https://eeas.europa.eu/headquarters/headquartershomepage/search/site/EU%20INTCEN_en?search_token=o723U8OfUGuCIx6p-1rePhvLcUTgHe1WG3IBGatQGxA

[326] Disponível em https://eeas.europa.eu/headquarters/headquarters-homepage/3598/highrepresentativevice-president_en [consult. 20 set.2021].

e uma gama de produtos baseado em inteligência e fontes abertas para o Alto Representante /Vice-Presidente, ao SEAE e aos diversos órgãos de decisão da EU, em atuar como um único ponto de entrada da UE para informações classificadas provenientes dos serviços de inteligência e segurança dos Estados-Membros e apoiar o presidente do Conselho Europeu e do Presidente da Comissão Europeia no exercício das respetivas funções na área das relações externas.

Quanto às bases legais do EU INTCEN (sucessor do EU SITCEN), vem mencionado no artigo 4.º, n.º3 al. a), da Decisão do Conselho de 26 de julho de 2010 (2010/427/EU), que estabelece a organização e o funcionamento do Serviço Europeu de Ação Externa, servindo desta forma de base jurídica para a EU INTCEN, que assumiu as tarefas de inteligência da EU SITCEN.

2. Sistemas e serviços de informações congéneres

2.1 Alemanha

O BND (*Bundesnachrichtendienst*), o serviço de Inteligência Federal Alemão, é o responsável pela recolha e análise de informações de uma variedade de fontes secretas fora das fronteiras da Alemanha, funcionando ainda também como o principal órgão SIGINT.

Em 2016 foi aprovada uma reforma do BND[327], do qual resultou um reforço da monitorização pelo governo do principal serviço de inteligência da Alemanha, ao mesmo tempo em que lhe permitiu realizar certos tipos de atividades de vigilância.

Na sequência das revelações feitas pelo ex-analista da NSA, Snowden, diversos serviços de inteligência, incluindo o BND, cooperaram com a NSA a qual teria "espionado" os próprios aliados, levando à formação de uma comissão parlamentar a fim de elaborar uma reforma dos serviços de inteligência.

A recolha e o processamento de informações é o centro na sua estrutura organizacional, no entanto, não deixa de ser constituída por algumas unidades de apoio, nomeadamente as diretorias regionais que fornecem análises de inteligência sobre questões políticas, económicas e militares de países estrangeiros. A diretoria TE lida com o terrorismo, crime organizado e as razões e efeitos da migração. A diretoria TW trata do tráfico internacional de armas, armas NRBQ (armas nucleares, radiológicas, biológicas e químicas) e tecnologia militar. A diretoria

[327] Lei do BND. Disponível em https://www.gesetze-im-internet.de/bndg/BNDG.pdf [consult. 29 set.2021].

TA é a responsável pela SIGINT. A diretoria GU controla e coordena o processo de produção de informações e assegura o funcionamento da comunicação interna e externa. E a diretoria TI garante que todos os processos de comunicação necessários sejam confiáveis.

Recentemente o Tribunal Constitucional Federal de Karlruhe declarou inconstitucional a Lei BND[328], que tinha sido alterada no final de 2016[329], em relação à vigilância estratégica das telecomunicações no estrangeiro, bem como à monitorização dos jornalistas e suas fontes (apesar da sua comunicação estar protegida por lei).

De acordo com *Spiegel* os juízes do tribunal constitucional alemão esclareceram várias questões relacionadas com a vigilância e monitoramento indiscriminado, enunciando: "que os direitos básicos alemães como a liberdade de imprensa e o sigilo das telecomunicações não são direitos básicos; os direitos de defesa contra a vigilância das telecomunicações estendem-se também aos estrangeiros no estrangeiro; a vigilância da BND pela internet vai longe demais, não se limitando a fins suficientemente específicos e estruturados de forma a torná-la contornável e faltam medidas de proteção, por exemplo, para proteger jornalistas e advogados; a transmissão de resultados da vigilância das telecomunicações a outros serviços congéneres também deve de ser regulamentada de forma mais rigorosa e o controlo independente do BND deve ser ampliado" [330].

Resultado da declaração de inconstitucionalidade da atual versão que está em vigor desde o início de 2017, o governo alemão até ao final de 2021 de proceder à sua alterar, até lá os regulamentos em questão continuarão a ser aplicáveis.

Por fim, o tribunal sugeriu ainda a possibilidade de um desenho constitucional declarando que a monitorização da internet pelo BND não é fundamentalmente incompatível com a lei básica[331] (Lei Fundamental da Alemanha).

[328]Disponível em https://www.spiegel.de/netzwelt/netzpolitik/bundesverfassungsgerichtinternetueber wachung-des-bnd-verstoesst-gegen-grundrechte-a-351a9bcd-efd6-4028-8550-0f82b906246c [consult. 22 set.2021].

[329] A reforma de 2016 tinha sido aprovada permitindo ao BND usar dos meio disponíveis para garantir a segurança na Alemanha alegando: "de que outra forma se espera que o BND iria proteger contra o terrorismo, se não escutando conversas entre indivíduos fora do território?"

[330]Disponível em https://www.spiegel.de/netzwelt/netzpolitik/bundesverfassungsgerichtinternetueberwach ung-des-bnd-verstoesst-gegen-grundrechte-a-351a9bcd-efd6-4028-8550-0f82b906246c [consult. 22 set.2021].

[331] Como referenciado, veja-se a previsão normativa do artigo 10.º, n.º 1 da Lei Fundamental Alemã, que dispõem «a inviolabilidade da correspondência, das comunicações postais e das telecomunicações» e no seu n.º 2 prevê que «as limitações só podem ser ordenadas em virtude da lei, salvo se a limitação tiver por finalidade proteger a ordem fundamental livre e democrática ou a existência da Federação e de um estado federado, a lei pode determinar que a limitação não seja levada ao conhecimento do individuo atingido e que, em vez de seguir a via judiciária, o controlo seja efetuado por órgãos principais e auxiliares, nomeados pelos representantes do povo»

2.2 Espanha

O Centro Nacional de Inteligência (CNI ou abreviadamente designado por Centro) a par de outras instituições de inteligência europeias pautam-se pela transparência democrática, princípio básico das administrações públicas. Contudo, tanto pela natureza da informação obtida, como pelos métodos que utiliza para a obter, bem como pelo conteúdo das suas avaliações e análises, o segredo e a confidencialidade deve ser entendido como um método para ocultar as atividades prosseguidas pelos serviços, mas também como forma de garantir que certas fontes, questões, identidades, factos ou decisões não sejam de conhecimento de quem poderia usar a informação para atuar contra os interesses do Estado, visando desta forma contribuir para a manutenção da segurança nacional[332].

Quanto à designada "cultura de inteligência", o Centro Nacional de inteligência prossegue uma política de consciencialização pública com o objetivo de aprimorar o conhecimento da sociedade sobre a finalidade e as funções dos Serviços de inteligência, demonstrando a importância da análise e recolha de informações (inteligência) como ferramenta fundamental para a tomada de decisões estratégicas, tanto ao nível estadual quanto na esfera privada, num ambiente cada vez mais incerto e digital. O objetivo comum é que todos os atores sociais tomem consciência de que têm um papel ativo na salvaguarda da segurança e que só com o esforço de todos se pode garantir a segurança e defesa dos valores de um Estado de Direito Democrático.

No que concerne às disposições que regulam o CNI, a lei n.º 11/2002, de 6 de maio[333], regulamenta o Centro Nacional de Inteligência e a Lei Orgânica 2/2002, de 6 de maio regulamenta o controlo judicial prévio do CNI.

Como em todos os Estados Democráticos, os serviços de inteligência estão sujeitos a uma série de controlo e fiscalização. Neste sentido, os poderes do Estado exercem controlo sobre diferentes aspetos do CNI, nomeadamente o poder Executivo, o Legislativo e o Judiciário.

Quanto ao controlo Político, o governo estabelece os objetivos por meio de uma diretiva anual que delimita as atividades do Centro e através de um Comité do Executivo, do qual este acompanha e avalia o desenvolvimento dos objetivos e das atividades.

Por outro lado, o controlo parlamentar prevê que a Comissão que controla o orçamento e as despesas reservadas, seja também a que controla as atividades do Centro.

[332] Vide o sitio oficial do Centro Nacional de Inteligência (ESP). Disponível em https://www.cni.es/
[333] Ultima alteração a 24 de dezembro de 2008.

Já o controlo judiciário, tendo em consideração o artigo 18.º, n.º 3 da Constituição Espanhola, relativo à inviolabilidade das comunicações, é realizado pelo Magistrado do Supremo Tribunal, concedendo as autorizações prévias necessárias para o cumprimento das funções que lhes são atribuídas nos termos do artigo 12.º da Lei 11/2002 e do artigo Único da Lei Orgânica 2/2002, de 6 de maio. Assim, de acordo com estes dois diplomas, o Diretor do Secretário de Estado do CNI deverá solicitar ao Magistrado do Supremo Tribunal competente, nos termos da Lei Orgânica 2/2002, autorização para a adoção de medidas que afetem a inviolabilidade das comunicações, desde que tais medidas sejam necessárias ao cumprimento das funções do Centro. Este pedido deverá ser formulado por escrito e especificar as medidas solicitadas, os factos que fundamentam o pedido, objetivos que o motivam e motivos que orientam a adoção das medidas, a identificação da (s) pessoa (s) afetadas pelas medidas, se conhecidas, e designação do local onde devam ser executadas, e por ultimo a duração das medidas, que não pode ultrapassar as vinte e quatro horas no caso de afetação da inviolabilidade do domicílio e três meses para a intervenção ou interceção de correio, telégrafo, escutas telefónicas ou qualquer outro tipo de comunicação, havendo a possibilidade de prorrogação das medidas por períodos iguais sucessivos, se necessário[334]. A resolução fundamentada pelo Magistrado terá um prazo improrrogável de setenta e duas horas, de concessão ou não autorização e é classificada como secreta. No seguimento de todas as informações obtidas por esta autorização que não tenham relação com o objeto ou finalidades da mesma, o secretário de Estado e Diretor do CNI, ordena a imediata destruição desse material.

A título de curiosidade e com o intuito de reforçar o espirito e o código ético de um serviço de inteligência, reiteramos os princípios éticos mais relevantes (não desmerecendo outros igualmente importantes) de acordo com o Código Ético do CNI: o profissionalismo, a retidão, o espírito de sacrifício, a objetividade e a imparcialidade, a dedicação e esforço constante, a camaradagem sincera, a capacidade de liderança que sirva de exemplo aos seus subordinados com humildade e espírito de equipa, a honra, a lealdade e a pronta disponibilidade para as missões que lhes sejam exigidas contribuindo assim para o prestígio da instituição e do Estado.

2.3 Brasil

Gostaríamos de assinalar primeiramente o contributo doutrinário imprescindível do professor e consultor do Senado Federal, Joanisval Gonçalves para a realização desta

[334] Cf. o artigo Único, 2 (a, b, c e d).

investigação e oportunamente considerável neste espaço que nos ocupa a respeito do direito comparado no Brasil.

Importa assim, enquadrar sumariamente o seu sistema de inteligência. Neste sentido, após a extinção do Serviço Nacional de Informações (SNI) em 1964, a atividade de inteligência no Brasil sofreu um período conturbado e de reformas que culminaram na elaboração da Lei n.º 9.883, de 7 de dezembro de 1999, que instituiu o Sistema Brasileiro de inteligência (SISBIN) e criou, como seu órgão central, a Agência Brasileira de Inteligência (ABIN) através do Decreto n.º 4.376, de 13 de setembro de 2002, esta última constituindo o atual fundamento normativo da atividade de inteligência no Brasil, dispondo da organização e do funcionamento do SISBIN.[335]

Além desta legislação, o Brasil conta também com uma Política Nacional de Inteligência (PNI) fixada em 2016 por meio do Decreto n.º8.793, de 29 de junho, bem como a aprovação da Estratégia Nacional de Inteligência (ENINT), anexo pelo Decreto (sem número) de 15 de dezembro de 2017 "*servindo de referência para a formulação do PNI, consolidando desta forma os conceitos e identificando os principais desafios para a atividade de inteligência, definindo eixos estruturantes e objetivos estratégicos*"[336].

Um outro instrumento normativo é a Lei n.º12.527, de 18 de dezembro de 2011, que se traduz na Lei de Acesso à Informação (LAI), e o seu regulamento, Decreto n.º 7.74, de 16 de maio de 2012 e ainda o Decreto n.º 7.845, de 14 de novembro de 2012 que regulamenta os procedimentos para credenciação de segurança e tratamento de informação classificada. A LAI teve, portanto, um impacto preponderante nos serviços de inteligência, na circunstância de possibilitar alternativas para lidar com a disponibilização de informações cobertas sob sigilo a qualquer interessado[337], sem a necessidade justificativa para o pedido de acesso[338].

Assim, conforme o disposto do art.2.º§1.º da Lei n.º 9.883, o SISBIN é responsável pelo processo de obtenção, análise e disseminação da informação necessária ao processo decisório do poder executivo, bem com da salvaguarda da informação contra o acesso de pessoas ou órgãos não autorizados, enquanto a ABIN, órgão da Presidência da República, tem a seu cargo, planear, executar, coordenar, supervisionar e controlar as atividades de inteligência, sob as diretrizes delineadas superiormente.

[335] Cf. Joanisval Brito Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, cit. p.139.
[336] *Idem*, p.140.
[337] Cf. Art.ºs 23.º a 26.º da LAI.
[338] Cf. Art.º10.º da LAI.

Aspeto importante é a questão que Joanisval Gonçalves levanta sobre o controlo da atividade de inteligência - Se os órgãos de Controlo (externo) são adversários ou aliados?

Como refere o autor, não deixa de ser um paradoxo. A relação, entre órgãos de fiscalização (controladores) e os serviços de inteligência (controlados) cria dificuldades na comunicação e dificulta o controlo. Mormente "se as partes já se encontrarem na relação influenciadas por preconceitos ou temores um do outro"[339].

A consequência deste antagonismo será indubitavelmente marcada pela ineficiência da atividade de inteligência e a ineficácia na fiscalização.

Assim, na perspetiva do controlo e fiscalização (externa) da atividade de inteligência, o mais relevante para a democracia é exercida pelo Poder Legislativo, constituído pelos líderes da maioria e da minoria na Câmara dos Deputados e no Senado Federal, assim como os Presidentes das Comissões das Relações Exteriores e Defesa Nacional da Câmara dos Deputados e do Senado Federal. No âmbito externo podemos ainda verificar um controlo exercido pelo Judiciário, o qual cabe aos magistrados um controlo prévio – quando autorizam determinadas operações, e também um controlo *à posteriori*, ao julgarem ações em que a comunidade de inteligência se encontre no polo passivo [340].

Para além deste controlo (externo) exercido pelo Poder legislativo, encontramos também um controlo interno, realizado na esfera do Poder Executivo, exercido pela Câmara das Relações Exteriores e Defesa Nacional do Conselho do Governo.

Concluindo esta alusão comparativa do Direito Brasileiro relativo à previsão Constitucional dos serviços de inteligência, à semelhança do que se passa em Portugal, a Carta de 1988 (Constituição da República Federativa do Brasil), também não faz qualquer menção a um tão importante órgão de estado na preservação da democracia, nem ao papel da atividade de inteligência para a defesa do Estado e da sociedade. Verifica-se, portanto, a falta de previsão constitucional, atribuindo à legislação infraconstitucional uma efêmera previsão normativa das competências e atribuições da ABIN e dos demais órgãos do SISBIN.

Joanisval Gonçalves refere inclusive na falta de uma claro mecanismo de controlo da atividade de inteligência, particularmente no controlo externo exercido pelo Parlamento e também na fiscalização pelo Congresso, estando os serviços de inteligência sujeitos não só a

[339] Cf. Joanisval Gonçalves, Políticos e Espiões. O Controle da Atividade de Inteligência. 2ª Ed. 2019, *op.cit*. p.59.
[340] Presumimos que o autor se queira referir à circunstância de os agentes de inteligência violarem as disposições legais estabelecidas atendendo aos princípios da proporcionalidade, adequação e exigibilidade das suas competências.

desvios de conduta, mas vulneráveis a mudanças conjunturais na sua estrutura, organização e missões.

Por fim, relativo aos direitos e garantias fundamentais previstos na Carta de 1988, no seu art. 5.º, XII, este enforma que todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, considerando a inviolabilidade e o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefónicas, salvo, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal[341].

Assim, concluímos também que a restrição enunciada no referido artigo 5.º da Lei Fundamental Brasileira circunscreve-se no âmbito de um processo penal, não obstante o facto de a atividade de inteligência ter distintas categorias, conforme descreve Joanisval Gonçalves. O autor descreve então, como atividade de Inteligência as seguintes caraterísticas: "proactiva; visão de futuro; compreensão do fenómeno, suas causas, consequências e de como enfrentar o problema por meio de atuações específicas; não se preocupa com a produção de prova; não se preocupa em buscar a verdade e sim a realidade; assessoria qualificada produtora de conhecimentos e; pode ser de natureza exploratória e sistemática"[342]. Por outro lado, a Investigação Criminal destaca-se: "por ser reativa; visão de passado e presente; objetiva esclarecera a autoria e comprovar a materialidade; ocupa-se da produção de prova; preocupa-se com a busca da verdade; não é atividade de assessoria e em regra é exploratória"[343]

[341] Cf. Joanisval Gonçalves, "Conhecimento e Poder – A atividade de inteligência e a Constituição Brasileira (1988)."Disponível em https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/outras-publicacoes/volume-iii-constituicao-de-1988-o-brasil-20-anos-depois.-a-consolidacao-das-instituicoes/segur anca-publica-e-defesa-nacional-conhecimento-e-poder-a-atividade-de-inteligencia-e-a-constituicao-brasileira

[342] Cf. Joanisval Gonçalves, Atividade de inteligência e legislação correlata. 6ª Ed. 2018, *op.cit.* p.48. O autor reproduz esta distinção, segundo um quadro em que distingue entre atividade de inteligência e investigação criminal, através de uma monografia apresentada ao Departamento de Estudos da Escola Superior de Guerra, como requisito à obtenção do diploma do curso de Altos Estudos de Política e Estratégia, Paulo Roberto Batista de Oliveira.

[343] *Ibidem.*

CONCLUSÃO

Considerando a génese desta investigação, estamos longe de esgotarmos a profundidade do tema bem como a controvérsia gerada em torno da utilização dos designados metadados pelos serviços de informações.

Na circunstância por exemplo da ingerência das autoridades públicas nas comunicações, colocar em conflito um direito fundamental com outros direitos comunitários, só seria autorizada para a realização da justiça, da descoberta da verdade "material" e restabelecimento da paz jurídica comunitária, ou seja, no âmbito e de acordo com os valores que ao processo penal incumbe realizar. Não obstante ainda da abundante jurisprudência constitucional convergir no sentido em que, fora de um processo penal, vigora uma proibição absoluta de ingerência das autoridades públicas nos meios de comunicação.

Observamos então que durante a época ditatorial que se viveu no passado face as caraterísticas repressoras que a PIDE/DGS desenvolvia até à revolução de abril de 1974, vigorava uma redundância legislativa que contribuía claramente para um abuso dos poderes punitivos e de perseguição criminal do Estado, e que de facto não se tratava verdadeiramente de um serviço de informações, mas antes um organismo repressor e opressor, utilizado por um regime de cariz autoritário, com fins político-partidários e desta forma descredibilizando a atividade dos órgãos de inteligência, tornando-os vulneráveis.

Por se tratar de uma matéria que pela sua natureza, demonstra uma certa complexidade, como os metadados e a relação com a atividade de produção de informações prosseguida pelos serviços de informações, poder-se-á traduzir no entanto numa medida preventiva (constatando uma restrição de certos direitos fundamentais, em particular, os direitos à reserva da intimidade da vida privada e o direito à inviolabilidade das comunicações) que poderá ser aplicada à margem do processo penal, numa fase premonitória que se destina sobretudo a prevenir algum género de crimes com especial gravidade (terrorismo, espionagem, criminalidade altamente organizada e violenta).

No fundo seria atribuir um reforço de competências aos serviços de informações de forma a instituir um sistema preventivo de produção de informações que permitiria detetar ameaças e situações de risco que afetassem os valores fundamentais da comunidade.

A respeito das questões suscitadas na introdução ao tema proposto, tomámos como ponto de partida a análise de dois acórdãos do Tribunal Constitucional, no âmbito da interpretação e alcance do artigo 34.º n.º 4 da Constituição da República Portuguesa.

Entendemos assim, ainda que não sejamos conclusivos na sua interpretação, apesar de a norma comportar uma medida de exceção quanto às restrições legalmente estabelecidas em matéria de defesa de direitos, liberdades e garantias perante a informática. O legislador constitucional não previu que pudesse existir um dia a necessidade de combater determinadas ameaças, logo num plano preventivo, com recurso a medidas restritivas que tradicionalmente, apenas seriam admitidas no âmbito de um processo penal em curso e eventualmente não poderia fazer essa previsão, uma vez que a tecnologia encontrava-se num estado embrionário na última revisão constitucional.

Daqui decorre também a possibilidade da realização da tal revisão constitucional face a esta medida de exceção, que deveria encontrar a sua fonte de legitimação de forma expressa e inequívoca na Constituição. Caso contrário, à autorização (exceção) prevista no n.º 4 do artigo 34.º da Constituição bastaria a interpretação de uma redução teleológica de forma a abranger a atividade de recolha de dados (metadados) pelos Serviços de Informações no âmbito da prevenção de formas bastante gravosas de criminalidade.

Neste sentido acompanhamos a tese de que a atividade desenvolvida pelos serviços de informações, teria de ser tida em conta na relação de complementaridade com o processo penal, ou seja, apoiado ainda na ideia de uma verdadeira cooperação institucional entre os órgãos de polícia (no âmbito do processo criminal) e os serviços de informações (no momento prévio de recolha de informações) em nome da prevenção criminal e do processo penal.

Uma outra questão seria o da conformidade da ingerência ou acesso aos metadados com o princípio da proporcionalidade, na medida em que, esta seria adequada face ao fim a que se destinava. Dado o complexo rastreio e monitorização das pegadas digitais face aos recursos disponíveis, bem como as atribuições diferenciadas dos diversos organismos policiais, consideramos que as medidas seriam necessárias para que os Serviços pudessem atuar no âmbito da prevenção criminal, pois o acesso a este tipo de informação permitiria estabelecer conexões entre informações dispersas com vista à formação da convicção de elementos vitais na constituição de uma cadeia informacional coerente.

A propósito ainda da observância do princípio da proporcionalidade, levantou-se a questão da concordância prática e combinação de outros bens jurídicos em conflito, de forma a evitar o sacrifício (total) de uns em relação a outros. Assim, podemos concluir a este respeito que não podemos arredar-nos de delimitar, no acesso aos metadados dos cidadãos, um fundamento preciso e determinado na lei, impondo naturalmente os requisitos da necessidade, exigibilidade e proporcionalidade (ou proibição do excesso).

Não olvidamos as opções existentes atualmente sem o recurso de acesso aos metadados e às comunicações, encontrando-se limitadas no tempo e no espaço. Como referimos, através da OSINT podem tanto os OPC como os serviços de informações recolher uma enorme quantidade de informação, de modo a construir uma fonte credível e uma base de dados, mas não suficiente. Necessariamente precisariam de tempo, assim como de uma espécie de sistema de filtro de informação (algoritmo avançado) que pudesse tratar e selecionar a informação relevante, a fim de prever crimes como o terrorismo, a espionagem e a criminalidade organizada e violenta transnacional.

Posto isto, com vista à viabilização de dotar os Estados de mecanismos de combate à prevenção e luta contra este tipo de criminalidade grave, urge a necessidade de uma resposta integrada, mobilizada e coordenada numa cooperação de todos os organismos e estruturas nacionais.

Assente num código ético rigoroso, seja qual for a categoria de inteligência – militar, estratégica ou policial – a produção de informações deverá ser conduzida por princípios norteadores, através de leis, regulamentos adequados e de um sistema de controlo democrático regular e eficiente.

Quanto à fiscalização e controlo judicial da atividade dos serviços de informações, constatamos que decorre atualmente, através de instrumentos legislativos como: a Lei Orgânica n.º 4/2017, de 25 de agosto; a Lei n.º 9/2007, de 19 de fevereiro; e da Resolução do Conselho de Ministros n.º 188/2017, de 5 de dezembro, a preocupação de um efetivo controlo democrático, não fazendo cair sobre esta melindrosa atividade administrativa do Estado qualquer sombra ou obscuridade.

Não obstante do controlo administrativo (interno) e do controlo judicial (externo), podemos ainda acrescentar ao controlo externo o papel da comunicação social, onde desempenham um papel fundamental de manter o cidadão informado e de formar opinião pública, quem são os serviços de informações e o que fazem, exercendo em paralelo um papel de "controladores" da atividade de inteligência.

Para além dos órgãos e mecanismos de fiscalização e controlo formais, que vão desde o controlo executivo (governo), o controlo legislativo (orçamentário, regulamento do centro de dados, comissões de fiscalização, conselhos de fiscalização), o controlo administrativo e judicial (comissão de controlo prévio), possamos acolher também os órgãos de comunicação social a desempenhar uma função de controlo informal monitorando as atividades dos serviços de informações.

Já a clarificação da distinção entre a recolha de informações prosseguida pelos serviços de inteligência (*intelligence*) por um lado e a recolha de informações no âmbito de uma investigação criminal, por outro foi também merecedora da nossa atenção. A primeira envolvendo dados e a produção de conhecimento com o objetivo de assessorar o processo decisório, quer ao nível estratégico na prossecução e definição de estratégias de combate à criminalidade altamente organizada, espionagem e terrorismo, quer na adoção de medidas concretas no âmbito de outros quadros funcionais atuando num plano que antecede a atividade policial de controlo de perigos. A segunda pressupõe a função policial, quando direcionada à adjetivação penal, elementos factualmente expressos, indutores de uma objetivação comportamental que afastam o essencial dos elementos de incerteza e de fluidez na referenciação concreta que observamos nas situações de risco, incerteza e ignorância como correspondendo ao espaço próprio da atividade de produção de informações.

Por último, no capítulo terceiro, analisamos um relatório da agência europeia dos direitos fundamentais bem como outros relatórios temáticos relacionados com os serviços e agências de inteligência, formais e informais, e ainda, perspetivando uma ação coordenada da UE, no reforço e intercâmbio de informações entre as várias agências de modo a prevenirem ataques terroristas e a subsequente atividade de processamento de dados.

Analisamos também os sistemas e serviços de inteligência congéneres, nomeadamente da Alemanha por onde "vamos beber" muito do nosso Direito; da Espanha por se encontrar na península ibérica e ser nosso vizinho, e, do Brasil pelas ligações que nos unem. De um modo geral, no domínio específico que aqui nos ocupa, todos estes ordenamentos jurídicos, com exceção do último, as Constituições vigentes dos Estados-Membros parecem encontrar-se preparadas para admitir a interceção de comunicações privadas com finalidades exclusivamente preventivas. Reforçando uma vez mais a solução de se proceder a uma revisão constitucional no nosso ordenamento jurídico.

Não obstante estarmos a viver tempos pandémicos que fragilizaram a economia e estabeleceram uma nova hierarquia de prioridades, reconhecemos que a recuperação económica, que irá ter lugar com o plano de recuperação e resiliência, é urgente para o nosso

país, contudo, uma revisão constitucional abrangendo matérias como estas ficam "naturalmente" secundarizadas ou até mesmo vistas como marginais. No nosso entendimento, sem olvidarmos o tão famoso ditado popular «de que é melhor prevenir que remediar», uma revisão constitucional com este tema, poderá nunca ser aceite, mas decerto, que será continuadamente discutida, até porque vivemos num mundo cada vez mais globalizado, e no qual o papel dos serviços de inteligência tem uma relevância fundamental na estabilidade política e económica.

O crescimento de forças partidárias, nomeadamente de extrema-direita poderão de alguma forma precipitar e crispar esta discussão, desta forma, caso por este meio este debate tenha lugar, no nosso humilde entendimento, este ponto de partida poderá levar a um desenquadramento e a uma politização de um tema que deve ser visto com a moderação necessária sem conservadorismos extremos, sem populismos e acima de tudo sem o aproveitamento enviesado partidário.

REFERÊNCIAS BIBLIOGRÁFICAS

Fontes documentais/ Jurisprudência

RIBEIRO, Lino Rodrigues. **- Ac.TC n.º 403/2015 de 17/09/2015 – Proc. N.º 773/15**, pp. 8245-8279. [Em linha]. (Consult. 30 Jun. 2021). Disponível em https://dre.pt/home/-/dre/70300353/details/maximized?p_auth=OsYd65lz.

RIBEIRO, Lino Rodrigues. **- Ac. TC n.º 464/2019 de 21/10/2019 – Proc. N.º 26/2018,** pp. 5-124 [Em linha]. (Consult. 30 Jun. 2021). Disponível em https://dre.pt/home/-/dre/125515884/details/maximized,

Acórdão Tele 2 Disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A62015CJ0203#

Acórdão Digital Rights of Ireland Disponível em https://eur-lex.europa.eu/legal-content/pt/TXT/?uri=CELEX%3A62012CJ0293

Manual de Legislação Europeia sobre a Proteção de Dados. [consult. 6 julh. 2021]. Disponível em http://publications.europa.eu/resource/cellar/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1.0017.03/DOC_2

Relatório da Agência Europeia dos Direitos Humanos, 2017, ***Surveillence by intelligence services: fundamental rights safeguards and remedies in the EU***. *Vol I: Member States´legal framework*. ISBN 978-92-9491-820-8. Disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligenceservices-voi-1_en.pdf.

TECHNICAL REPORT: ***Intelligence and Security Legislation for Security Reform.*** United Kingdom's Security Sector Advisory Team, RAND Europe, Cambridge, June 2005. Greg Hannah, Kevin O'Brien, Andrew Rathmewll. Disponível em https://www.rand.org/pubs/technical_reports/TR288.html (***sobre a obtenção do Dado Negado***)

Referências Bibliográficas

ABRANTES, António Manuel, Academia Edu [em linha]. Revista do Ministério Público 156 (Out. – Dez. 2018). P. 157-208- [Consult.25 Jan. 2021]. **O acesso a dados de tráfego pelos Serviços de Informações à luz do direito fundamental à inviolabilidade das comunicações**. Disponível em https://arquitectura-ucp.academia.edu/Ant%C3%B3nioManuelAbrantes

ALEXY, Robert, **Teoria dos Direitos Fundamentais**. Malheiros Ed. Ltda., 5.ª Edição, 2008. ISBN 978-85-7420-872-5

ANDRADE, Manuel de Costa, **Sobre as Proibições de Prova em Processo Penal**. Coimbra Editora, 1992. ISBN 972-32-0613-7

ÂNGELO, Fernando Cavaleiro, **DINFO: A Queda do Último Serviço Secreto Militar** – Alfragide: Casa das Letras, 2020. ISBN 978-989-660-816-3

BECCARIA, Cesare – **Dos Delitos e das Penas, 4ª ed.** Lisboa: Edição da Fundação Calouste Gulbenkian, 2014. ISBN 978-972-310-816-3

BRANCO, Carlos Castelo – **A Prova Ilícita: Verdade ou Lealdade?.** Coimbra: Almedina (Casa do Juiz), 2018. ISBN 978-9872-40-7555-6

BRITO, Maria Beatriz Seabra, **Novas tecnologias e legalidade da prova em processo penal. Natureza e enquadramento do GPS como método de obtenção de prova**. Coordenação: Tereza Beleza; Frederico de Lacerda da Costa Pinto. Coimbra: Almedina. Outubro, 2018. ISBN 978-972-40-7640-0

BELEZA, Teresa Pizarro., Pinto, Frederico De Lacerda Da Costa Pinto, **Prova Criminal e Direito de Defesa.** 8.ª Reimp. Coimbra: Almedina, 2019. ISBN 978-972-40-4090-5

CANOTILHO,J.J Gomes; MOREIRA, Vital, **Constituição da República Portuguesa Anotada Artigos 1º a 107º** - 4ª ed. Coimbra: Coimbra Editora, 2007. ISBN 978-972-321-1462-8.

CANOTILHO, J.J Gomes, **Direito Constitucional e Teoria da Constituição.** 7ª Ed. 17ª (reimp). Coimbra: Edições Almedina. ISBN 978-972-40-2106-5

CARDOSO, Pedro, **As Informações em Portugal**. 2ª Ed. Gradiva – Publicações, Lda./Instituto da Defesa Nacional. 2004. ISBN 072-662-961-6

CASTRO, Catarina Sarmento, **Direito da Informática, Privacidade e Dados Pessoais.** Coimbra: Edições Almedina, 2005. ISBN 978-972-40-2424-0

CASEMIRO, Sofia, **Liberdade e Segurança no Combate ao Terrorismo: Quis Custodiet Ipsos Custodes? Uma perspetiva Jurídica**. NAÇÃO E DEFESA – Terrorismo e Violência Política. Ed. Instituto de Defesa Nacional. ISSN 0870-757X. N.º 152 (2019), p.23-38.

COELHO, Carlos Montez, **"As informações em Portugal: Reflexão crítica sobre as secretas e a Constituição**", [Consult. 05 set.2021]. - Direito, Segurança e Democracia, n.º 1, Maio 2021, CEDIS Working Papers. Disponível em https://cedis.fd.unl.pt/wp-content/uploads/2021/06/DISED_2021_MAIO-01.pdf. ISSN 2184-0776. N.º 1 (2021), pp.24.

CORREIA, Eduardo, **Direito Criminal**. **Reimp.** Coimbra: Edições Almedina, S.A, 2016. ISBN 978-972-400-123-4

COSTA, Carla, **As alterações legislativas e as estatísticas criminais** – Revista Semestral de Investigação Criminal, Ciências Criminais e Forenses. Investigação Criminal N.º 7, 2014, pp.35-51. ISSN 1647-9300

D'AGOSTINO, Francesco, **Direito e Justiça - Introdução ao Estudo de Direito. 1ªed.** Cascais: Princípia Editora, Lda, 2014. ISBN 978-989-716-112-4

DIAS, Jorge Figueiredo, **Direito Penal: Tomo I. 2ª ed. 2ª Reimp**. Coimbra: Coimbra Editora, S.A, 2012. ISBN 978-972-322-108-4

DIAS, Jorge Figueiredo, **Clássicos Jurídicos. Direito Processual Penal. 1ª Ed.1974**. Coimbra: Coimbra Editora, S.A, 2004. ISBN 972-32-1250-1

_____Sobre a revisão de 2007 do Código de Processo Penal Português, *Revista Portuguesa de Ciência Criminal*, Ano 18, n.ºs 2 e 3, Abril-Setembro 2008, Coimbra Editora. Pp. 367-385; ISNN: 0871-8563

DIAS, Augusto Silva; PEREIRA, Rui Soares, **Sobre a Validade de Procedimentos Administrativos Prévios ao Inquérito e de Fases Administrativas Preliminares no Processo penal**. Coimbra: Ed. Almedina 2018. ISBN 978-072-40-7531-0

DULLES, Allen W., **The Craft of Intelligence**. Lyons Press, 2016. ISBN 978-1-4930-1879-6.

ESTEVENS, João, **"A construção da cooperação em intelligence na União Europeia"**. In Janus.net, e-journal of international relations. Vol. 11, Nº 2 [Em linha] (Consult. 27 Ago.2021), pp. 93-108. Disponível em https://doi.org/10.26619/1647-7251.11.2.6 .

Faculdade de Direito da Universidade de Coimbra, **Direito Penal Internacional para a Proteção dos Direitos Humanos.** In: Simpósio da Faculdade de Direito da Universidade de Coimbra. Coimbra: Fim de Século – Edições, Sociedade Unipessoal, Lda., 2003. ISBN 972-754-201-8

FAZENDEIRO, Ana, **Regulamento Geral sobre a Proteção de Dados** – Coimbra: 3ª ed., Almedina, 2018. ISBN 978-972-40-7629-4

FERREIRA, Eduardo Viegas, **Prevenção do crime na União Europeia** – Revista Semestral de Investigação Criminal, Ciências Criminais e Forenses. Investigação Criminal N.º 7, 2014, pp.62-71. ISSN 1647-9300

FERRAJOULI, Luigi, **As Garantias da prova como fonte de legitimação da jurisdição**. In: Um juiz pela democracia: um livro de homenagem ao Perfecto Andrés Ibánez /diretores Guilhermo Portilla Contreras, Fernando Velásquez. (Coord: Easther Pomares Cintas, Juan Luis Fuentes Osori).1ª Ed. Dykinson. ISBN 978-84-1324-412-9

FONTES, José, **A Constituição e os Serviços de Informações. "Segurança e Defesa"** [Em linha]. Nº 15 (Out.-Dez. 2010), p. 1-7. [Consult.25 Jan.2021]. Repositório aberto. Universidade Aberta. Disponível em https://repositorioaberto.uab.pt/handle/10400.2/1788

GONÇALVES, Joanisval Brito, **Atividade de inteligência e legislação correlata**. 6ª ed. Impetus, Niteoy, RJ 2018. ISBN 978-857-626-983-0

_____Políticos e Espiões. O Controlo da Atividade de Inteligência. 2ª Ed. Impetus, Niteoy, RJ 2019. ISBN 978-857-626-995-3

GOUVEIA, Jorge Bacelar, **Direito da Segurança. Cidadania, Soberania e Cosmopolitismo.** 1ª Ed. Coimbra: Almedina, 2018. ISBN 978-972-40-7492-4

_____Manual de Direito Constitucional. Vol. I, 5ª ed. Coimbra: Almedina, 2014. ISBN 978-972-40-5393-4

_____Textos Fundamentais de Direito Internacional Público. 2ª Ed. Rev. e actualizada. 2ª(reimp). Coimbra: Almedina SA, 2014. ISBN 978-972-40-5584-8

_____Manual de Direito Constitucional. Vol. II, 5ª ed. Coimbra: Almedina, 2013. ISBN 978-972-40-5394-3

_____Legislação de Direito Constitucional. 3ª Ed. Rev. e actualizada. QuidJuris – Sociedade Editora Ld.ª, 2013. ISBN 978-972-724-634-2

GOUVEIA, Jorge Bacelar; PEREIRA, Rui, **Estudos de Direito e Segurança**. Coimbra: Almedina, 2007. Depósito Legal n.º 256188/07

GRECO, Luís; GLEIZER, Orlandino, "***A infiltração on-line no processo penal - Notícia sobre a experiência Alemã***." Revista Brasileira de Direito Processual Penal, Porto Alegre, Vol.5, n.º3, pp.1483-1518, set-dez.2019. [consult. 09 set.2021]. Disponível em http://doi.org/10.22197/rbdpp.v5i3.278

MACHADO, Mariana Gomes, **O acesso aos metadados pelos serviços de informações da República Portuguesa á luz da Lei e da Constituição**. Coimbra. Almedina, 2019. ISBN 978-972-40-8199-1

MENDES, Paulo de Sousa, **Lições de Direito Processual Penal**. 5.ª Reimp. Coimbra: Almedina, 2018. ISBN 978-972-40-5205-2

MIRANDA, Jorge; MEDEIROS, Rui, **Constituição Portuguesa Anotada, Vol I**, 2.ª ed. Revista. Lisboa: Universidade Católica Editora, 2017. ISBN 978-972-540-541-3

MIRANDA, Jorge, **As Constituições Portuguesas.** 6ª Ed. Cascais: Princípia Editora ldª, 2013. ISBN 978-989-716-106-3

Manual de Direito Constitucional - Tomo IV: Direitos Fundamentais. 5ª ed. Coimbra: Coimbra Editora, 2012. ISBN 978-972-332-010-0

GODOY, Arnaldo Moraes, **Métodos de Trabalho do Direito Constitucional**, de Friedrich Müller. Uma Resenha. [Consult. 15 Fev. 2021]. Academia Edu. Disponível em https://www.academia.edu/38024664/M%C3%89TODOS_DE_TRABALHO_DO_DIREITO_CONSTITUCIONAL_DE_FRIEDRICH_M%C3%9CLLER_UMA_RESENHA

NEVES, Rita Castanheira, **As ingerências nas comunicações eletrónicas em processo penal**. 1ª ed. Coimbra: Coimbra editora, 2011. ISBN 978-972-32-1942-5

NUNES, Duarte Alberto Rodrigues, **Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime.** 1ª Ed. Coimbra: Gestlegal, 2018. ISBN 978-989-54076-4-4

NUNES, Paulo Viegas, **Sociedade em Rede, Ciberespaço e Guerra de Informação.** Contributos para o enquadramento e construção de uma estratégia nacional da informação. 2.ª ed. 2016. Instituto de Defesa Nacional. ISBN 978-972-9393-34-1

PEREIRA, Júlio, Vigilância Vídeo, Interceção Preventiva de Comunicações e Contraterrorismo. Nação e Defesa – **Terrorismo e Violência Política**. Ed. Instituto de Defesa Nacional. ISSN 0870-757X. N.º 152 (2019), p.39 - 47.

RAMALHO, David Silva, **Métodos Ocultos de investigação Criminal em Ambiente Digital.** Coimbra: Almedina, 2009. ISBN 978-972-10-70000-1

RAMOS, Armando Dias, **Prova Digital em Processo Penal: O Correio Eletrónico**. 2.ª Ed. Lisboa. Chiado Editora, 2017. ISBN 978-989-51-2383-4

RODRIGUES, Anabela Miranda; MOTA, José Luís Lopes, **Para uma Politica criminal Europeia: "Quadro e Instrumentos jurídicos da Cooperação Judiciária em Matéria Penal no Espaço da União Europeia".** Coimbra: Coimbra Editora, 2002. ISBN 972-32-1095-9

RAMOS, Rui Manuel Gens de Moura, **Tratado da União Europeia e Tratado sobre o Funcionamento da União Europeia**. 5º. Ed. Coimbra. Coimbra Editora. Fevereiro 2015. ISBN 978-972-32-2316-3

SANTOS, Gil Moreira, **Princípios e Prática Processual Penal**, 1.ª Ed. Coimbra. Coimbra Editora, 2014. ISBN 978-972-32-2202-9

SILVA, Germano Marques da, **Direito Penal Português. Vol. I: Introdução e Teoria da Lei Penal. 3ª Ed.** Lisboa. Verbo, 2010. ISBN 978-972-223-012-4.

_____Direito Processual Penal Português. **Vol. I.** Noções e Princípios Gerais; Sujeitos Processuais; Responsabilidade Civil conexa com a Criminal; Objeto do Processo. Lisboa: Universidade Católica Editora, 2017. ISBN 978-972-540-566-6

_____Curso de Processo Penal. Vol. II. 5ª Ed. Revista e atualizada. Lisboa. Verbo, 2011. ISBN 978-972-223-043-8

SIMÕES, Pedro, **Os Serviços Secretos em Portugal. Os serviços de informação e a comunicação social**. Lisboa: Prefácio, 2002. ISBN 972-8563-82-5

VALENTE, Manuel Monteiro Guedes; PRADO, Geraldo; GIACOMOLLY, Nereu José; SILVEIRA, Edson Damas, **Prova Penal. Estado Democrático de Direito**. Letras e Conceitos, Ld.ª, 2015. ISBN 978-989-8823-01-4

VALENTE, Manuel Monteiro Guedes, **Cadeia de Custódia da Prova.** Coimbra: Edições Almedina, S.A, 2019. ISBN 978-972-40-8191-5

_____Teoria Geral do Direito Policial, 5ª ed. Coimbra: Edições Almedina, S.A. 2017. ISBN 978-972-407-017-9

_____Direito Penal: Fundamentos Político-Criminais. Reimp. Lisboa: Edição de Autor, 2017-. ISBN 978-972-991-181-1

_____Direito Penal do Inimigo e o Terrorismo: O «Progresso ao Retrocesso». 2ªed. Reimp. Coimbra: Edições Almedina, S.A, 2018. ISBN 978-972-407-146-6

_____Escutas Telefónicas. Da excecionalidade à vulgaridade. 2ª Ed. Coimbra: Edições Almedina, S.A. 2008. ISBN 978-972-240-358-33

_____Direito Processual Penal: Da Sociedade Internético-Personocêntrica. Lisboa. 2020. ISBN 978-972-99118-2-8

ZIEMBOWICZ, Rodrigo Luís (2021). **Estimular e proteger o Desenvolvimento Econômico diante da Criminalidade Organizada**. In: Manuel Monteiro Guedes Valente (Coord.).

Criminalidade Organizada Transnacional – Corpus Delictii III. Coimbra: Almedina, pp. 87-138.