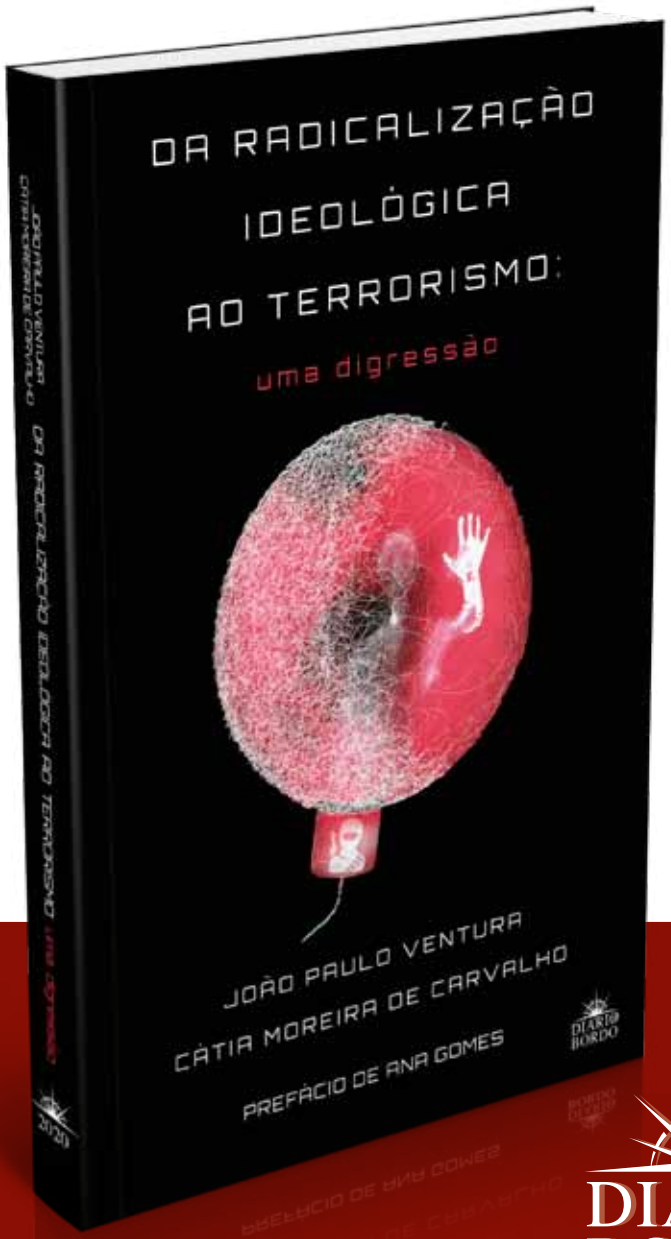
Segurança e Defesa

COORDENAÇÃO

JOSÉ MANUEL ANES

JOÃO GOMES CRAVINHO
AGOSTINHO COSTA
ANTÓNIO BRÁS MONTEIRO
FRANCISCO VILHENA DA CUNHA
HENRIQUE GOUVEIA E MELO
JOÃO GONÇALVES PEREIRA
JORGE PEREIRA LOURENÇO
JOSÉ ALBERTO PEREIRA
LUÍSA PROENÇA
MANUEL GOMES FERREIRA
MANUEL PEDROSA DE BARROS
PAULO MIGUEL SANTOS MONIZ

DIÁRIO DE BORDO



DIÁRIO DE BORDO

Cidadania e Conhecimento

REFLEXÕES
Segurança e Defesa

DIÁRIO DE BORDO

ÍNDICE

A DEFESA EUROPEIA E A PRESIDÊNCIA PORTUGUESA DO CONSELHO DA UNIÃO EUROPEIA

JOÃO GOMES CRAVINHO
Ministro da Defesa Nacional

Portugal irá assumir a Presidência do Conselho da União Europeia (UE), pela quarta vez, a 1 de janeiro de 2021, depois de o ter feito em 1992, 2000 e 2007. O contexto em que decorre a presidência portuguesa é o de um novo quadro internacional marcado por uma alteração dos alinhamentos e equilíbrios geopolíticos. O contexto geoestratégico na Europa deteriorou-se, com o surgimento de novas e importantes ameaças na sua vizinhança. Vimos também aumentarem os riscos resultantes de emergências complexas tornadas mais frequentes e mais intensas pelo efeito das mudanças climáticas e da globalização. O impacto da pandemia da COVID-19 tem sido um teste particularmente exigente à capacidade de resiliência dos Estados membros, mas também à coordenação e entreajuda no quadro da UE, tornando ainda mais clara a necessidade de se melhorar a capacidade da resposta europeia a este tipo de emergências, na qual os militares e as estruturas e meios da Defesa desempenham um papel indispensável. Por tudo isto, torna-se urgente que a União Europeia reforce o seu papel como ator global e produtor de segurança, investindo na defesa, no desenvolvimento de capacidades e na prontidão operacional, em complementaridade com a NATO, que permanece o pilar da defesa coletiva da Europa.

Deste modo, guiado por uma visão ambiciosa para o futuro da política europeia de defesa como uma produtora credível de segurança regional e global, o Ministério da Defesa Nacional definiu as grandes prioridades da Presidência portuguesa para a Política Comum de Segurança e Defesa (PCSD) da UE. Assim, daremos prioridade ao reforço da **Parceria UE-África para a Paz e Segurança**, defendendo uma visão abrangente e coordenada da atuação europeia no continente, em parceria e diálogo político com as organizações regionais africanas e as Nações Unidas. Discutiremos propostas concretas para uma maior eficácia das missões e operações militares da PCSD no continente, onde decorrem 5 destas missões (de um total de 6). Promoveremos o reforço da **Estratégia da UE para a Segurança Marítima**, advogando que o foco da ação europeia neste campo deve ser no Golfo da Guiné. É nesta região que se concentraram 90% dos ataques armados de pirataria, em 2019, e é nela que decorre o teste do conceito muito importante de Presenças Marítimas Coordenadas, fundamental para garantir uma mais eficaz e permanente presença militar naval europeia em espaços marítimos vitais. Em função da experiência desenvolvida no Golfo da Guiné, a União Europeia poderá a prazo começar a ter uma presença no mar, algo que é imprescindível atendendo às ambições da Identidade Europeia de Defesa. Trabalharemos para uma **relação UE-NATO** mais ambiciosa e com resultados tangíveis, e acreditamos que há diversos campos de trabalho em que isto se pode materializar. Outra grande prioridade da Presidência será a construção de uma **Europa mais resiliente** e, portanto, melhor preparada para responder a emergências de todo o tipo, das emergências sanitárias, como as pandemias, até às causadas por desastres naturais. Uma Europa mais resiliente passa também, necessariamente, pela criação de uma verdadeira **Economia europeia de Defesa**, onde as pequenas e médias indústrias de defesa, focadas na inovação tecnológica, devem ter um papel importante.

Todas estas importantes dimensões da Defesa europeia deverão encontrar expressão num novo documento orientador, a chamada Bússola Estratégica (BE), que a União Europeia irá elaborar durante os próximos 18 meses. A Bússola vai construir uma ponte entre a PCSD e a Estratégia Global da UE, de 2016, sem pôr em causa o nível de ambição desta estratégia. Ela visa reforçar a coerência estratégica das várias iniciativas da UE em matéria de segurança e defesa, como as operações e missões militares da PCSD, a

Revisão Anual Coordenada de Defesa (CARD), a Cooperação Estruturada Permanente (PESCO) ou o Fundo Europeu de Defesa (FED). Durante o seu semestre, Portugal irá orientar a discussão das principais linhas de orientação da Bússola Estratégica, apoiando o papel de coordenação do Serviço Europeu de Ação Externa.

Estes são em síntese os nossos principais objetivos e as linhas de ação que serão seguidas durante a presidência, aos quais voltarei mais adiante. Parece-me, porém, relevante, desde já, afastar algumas falsas dicotomias que devemos ultrapassar no nosso caminho para uma mais eficaz política europeia de Defesa.

A primeira destas falsas dicotomias que precisamos ultrapassar é a do chamado *soft power* europeu, supostamente assente na Europa como potência puramente civil versus uma política comum de segurança e defesa. Para isso importa responder à pergunta: porque deve a União Europeia envolver-se na defesa e desenvolver capacidades militares? A verdade é que nós, europeus, prezamos muito justamente a paz, depois de séculos de grandes guerras no nosso continente. Em Portugal, como em muitos outros países europeus, a Constituição determina que se procure que a primeira resposta aos conflitos seja a resolução pacífica dos mesmos. No entanto, como europeus, também precisamos de capacidades militares para garantir a nossa segurança. Precisamos delas para dissuadir a agressão externa e para ajudar outros a defenderem-se. Precisamos de capacidades militares para ajudar a responder a desastres naturais e outras emergências complexas, como a pandemia Covid-19. Para tal, é também necessário construir uma cultura estratégica partilhada europeia que reconheça esta realidade e que saliente a promoção dos nossos valores, bem como dos nossos interesses. Procurar a paz a qualquer custo deixar-nos-ia vulneráveis a qualquer autocrata agressivo que apareça. Isso seria uma desistência tanto dos valores como dos interesses europeus, e não garantiria, em última análise, a paz.

A segunda falsa dicotomia que devemos ultrapassar é entre uma economia europeia de defesa mais integrada versus a soberania nacional de cada Estado Membro. A verdade é que os Estados europeus são soberanos em relação à sua Defesa Nacional, porém ser soberano não deve significar

recusar a cooperação e as alianças que sejam do interesse nacional. Assim, considero que se não fizermos alguns dos grandes investimentos necessários para mantermos as nossas capacidades de Defesa atualizadas através de um esforço coordenado ao nível europeu, muitos deles não serão possíveis apenas a nível nacional. Em segundo lugar, é igualmente vital assegurar que estes projetos europeus sejam inclusivos ao nível da geografia europeia e diversificados, nomeadamente, através de uma melhor e maior participação das PME, as quais representam uma grande percentagem deste sector em toda a Europa. com estas características, estes investimentos em defesa serão mais sustentáveis. As PMEs são os principais motores da inovação e a chamada "reindustrialização" europeia não pode sufocar a concorrência e a inovação, fundamentais para melhorar o desempenho europeu em sectores tecnológicos críticos como a robótica, sistemas não tripulados, inteligência artificial e *big data*, bem como o domínio do espaço e as capacidades ciber. Em suma, o investimento na Defesa pode ser um importante contribuinte para a recuperação económica europeia após a enorme crise causada pela pandemia (e cujo impacto ainda não conhecemos plenamente), bem como para uma economia europeia mais inovadora, tecnologicamente avançada e resiliente.

A terceira falsa dicotomia que importa desmentir consiste no preconceito de que existe uma contradição entre a NATO e o aprofundamento de uma política europeia de defesa. Esta perceção tem sido alimentada recentemente por uma interpretação incorreta do significado do conceito de autonomia estratégica da UE. Defendo que este conceito deve ser entendido não como autonomia para os Europeus fazerem menos na NATO, mas sim como autonomia para a UE fazer mais. Na NATO e independentemente da NATO. Durante décadas, a NATO foi realmente a única organização da Defesa Europeia, e ela continua hoje a dar um contributo vital e indispensável para a UE. No entanto, a UE deverá continuar a trabalhar para poder atuar por si numa crise de segurança se não houver consenso ou disponibilidade na NATO para o fazer. Ao mesmo tempo para mim é evidente que a PCSD pode e deve ser também uma forma de melhorar a eficácia da contribuição europeia para a NATO. O que isto também significa é que temos de continuar a melhorar os mecanismos de cooperação entre a NATO e a UE. Juntos somos mais fortes. Isto interessa à NATO, interessa à UE, e interessa a Portugal. Esta é não só uma prioridade nacional como

uma prioridade do Trio da Presidência da UE, no qual temos trabalhado muito proximamente com a Alemanha e a Eslovénia.

Chegam-nos agora, dos Estados Unidos, notícias favoráveis a que este desenvolvimento da defesa europeia seja feito em estreita articulação com os nossos parceiros transatlânticos. Se é verdade que deveremos contar que os Estados Unidos permanecerão centrados na sua própria recuperação sanitária e económica, poderemos seguramente contar com um parceiro que saberá valorizar e potenciar os esforços que os Europeus têm em curso para contribuir mais ativamente para a segurança do espaço Euro-Atlântico. A presidência portuguesa irá procurar dar o seu contributo para potenciar este novo contexto.

Vivenciamos hoje uma convergência de um fenómeno poderoso, mas conjuntural, a pandemia, com mudanças profundas na geopolítica e geoeconomia mundiais. Esta é a era das alterações climáticas, das revoluções tecnológicas, cujas consequências se revelarão passo a passo, e é também a era da ascensão da China e do reposicionamento dos Estados Unidos e da própria Europa. É uma era de transição, e em que sabemos apenas que as nossas certezas do passado valem pouco para as décadas que se seguem. Assim, poder contar com os nossos aliados tradicionais, como os EUA ou o Reino Unido, torna-nos mais resilientes para podermos enfrentar estas mudanças.

Retomando o tema central, das oportunidades e prioridades que temos no âmbito da Presidência Portuguesa da UE para melhor as especificar, o Ministério da Defesa Nacional tem trabalhado estreitamente com o Ministério dos Negócios Estrangeiros e no âmbito do Trio de presidências, para que sejam tomadas importantes iniciativas concretas a respeito de cada uma delas. Destacaria especialmente a já referida Bússola Estratégica, que deverá centrar-se em quatro áreas: (1) gestão de crises, (2) resiliência, (3) desenvolvimento de capacidades e (4) parcerias. Este processo iniciou-se com a primeira avaliação conjunta das ameaças à União Europeia, com contributos nacionais coligidos e organizados pelo EU IntCen, o Centro de Inteligência e de Situação da União Europeia, que deverá agora formar a base de um entendimento comum à escala da União. Portugal dará a devida prioridade a este processo, a partir de janeiro, o qual deverá vir a

ser concluído no início de 2022, durante a Presidência francesa.

Três outros dossiers têm merecido particular empenho de Portugal, em apoio à Presidência alemã e ao Serviço Europeu de Ação Externa. O primeiro, concluído recentemente, em termos de princípios orientadores, referente à importante questão da participação de Estados terceiros na PESCO em matéria de Defesa e que será importante implementar; e outro, também concluído no final da presidência alemã, relativo à aprovação do novo Mecanismo Europeu de Apoio à Paz. Este mecanismo que deverá entrar em vigor em 2021 visa responder a necessidades fundamentais na nossa cooperação em matéria de segurança e estabilidade com alguns países, nomeadamente, em África. O terceiro dossier, diz respeito à definição do quadro regulamentar para o inovador Fundo Europeu de Defesa, que entrará em vigor durante a nossa Presidência.

Para além do necessário acompanhamento destas matérias, o próximo semestre contará com um papel ativo de Portugal no seio da União Europeia no que toca às prioridades acima enunciadas, nomeadamente, ao reforço da Parceria UE-África em matéria de Paz e Segurança.

A crescente instabilidade existente em partes do continente africano representa um rude golpe na ambição de as sociedades africanas melhor participarem no desenvolvimento global do século XXI e é uma fonte de insegurança na relação entre africanos e europeus. A parceria europeia com África deverá centrar-se na mobilização dos recursos de que a UE dispõe para contrariar aquela tendência em diálogo com os nossos parceiros no Sahel, na África Subsariana, na orla do Mediterrâneo e no Atlântico. A defesa é uma dimensão essencial dessa parceria com África. Durante a presidência portuguesa, e tendo como referência as missões militares no âmbito da PCSD, iremos procurar torná-las mais robustas e coordená-las com missões civis já implantadas em África. Esta iniciativa terá um real impacto, uma vez que cinco das seis missões militares da UE estão no continente africano, e das onze missões civis da UE também cinco se encontram naquele continente. O reforço do diálogo entre a UE e as organizações regionais e sub-regionais de segurança em África é, por isso, muito importante, e faz particular sentido num contexto em que a competição geopolítica nesse continente avança. É nosso entendimento que só com um

diálogo reforçado com parceiros regionais mais empenhados e capacitados, poderemos assegurar que os nossos interesses comuns são salvaguardados. Para este efeito pretendemos organizar em Lisboa, à margem da reunião informal de ministros da Defesa da UE uma reunião com a União Africana e as organizações sub-regionais mais diretamente implicadas nos temas da segurança, como a CEDEAO, a SADC, a CEEAC e o IGAD.

A Segurança Marítima será igualmente prioritária. A segurança da Europa encontra-se profundamente dependente de dinâmicas que ocorrem no mar, e em particular no Atlântico por onde transita boa parte dos 90% do comércio externo da UE e 40% do comércio interno da UE que são transportados por via marítima. Portugal, pela sua situação geopolítica euro-atlântica tem aqui um interesse e um conhecimento particulares, sendo tradicionalmente ativo nos mares africanos, nomeadamente no Golfo da Guiné, com a presença de um navio patrulha da Marinha Portuguesa cooperando com São Tomé e Príncipe, e outras iniciativas. Durante a presidência portuguesa da UE iremos procurar que o diálogo em torno deste espaço se densifique, pelo que será promovido um encontro entre os ministros da defesa da UE e os ministros da defesa do G7 ++ Amigos do Golfo da Guiné. Ainda neste âmbito será apresentado oficialmente o Centro do Atlântico, uma iniciativa liderada por Portugal que se centra na segurança cooperativa e tem particular enfoque na segurança marítima. Paralelamente, intensificar-se-ão as Presenças Marítimas Coordenadas da UE, para garantir uma melhor coordenação da presença militar da União e de outros parceiros regionais, nomeadamente no Golfo da Guiné.

Em terceiro lugar, Portugal assume o reforço das relações UE-NATO como uma prioridade nacional, como já referi. Um maior envolvimento dos 27 no debate sobre a autonomia estratégica da Europa tem resultado numa visão articulada com a NATO, traduzida na criação de capacidade europeia para dar resposta às tensões e conflitos que afetam, quer o espaço da Aliança Atlântica, quer os espaços geográficos normalmente fora da área de atuação da NATO. Queremos uma relação UE-NATO mais ambiciosa e com resultados tangíveis, centrada em matérias como a segurança marítima, as ameaças híbridas, a mobilidade militar e a defesa verde, mas também na resposta a emergências complexas, nomeadamente aproveitando as *task forces* criadas na UE e na NATO para acompanhar o contributo militar ao

combate à pandemia de Covid-19. A entrada em funções da Administração Biden representa uma oportunidade de aprofundar o diálogo quanto à Identidade Europeia de Defesa e o pilar europeu da NATO.

Em quarto lugar, teremos o objetivo da promoção de uma Economia Europeia de Defesa forte, assente numa cooperação mais profunda em matéria de desenvolvimento de capacidades, para alcançar a liderança tecnológica e industrial na UE. Em abril, no Porto, a Agência Europeia de Defesa realizará, em parceria com o Ministério da Defesa Nacional, um evento de alto nível que abordará o impacto das tecnologias disruptivas na defesa. Organizaremos também um seminário internacional, em maio, em Lisboa, pensado para alavancar a Base Tecnológica e Industrial de Defesa Europeia, densificando laços à escala europeia. Uma prioridade absoluta para Portugal é que o futuro FED garanta um estímulo adequado à participação de PMEs, permitindo assim uma real difusão dos benefícios e oportunidades deste novo programa.

Refiro, ainda, uma prioridade transversal centrada no reforço da resiliência para a resposta a emergências complexas, seja em território europeu ou junto dos nossos parceiros, como sendo as alterações climáticas e os seus efeitos multiplicadores na intensidade e frequência das catástrofes naturais, assim como as emergências sanitárias, como é o caso da pandemia em que vivemos. Na melhoria da resposta europeia a todos os tipos de emergências, a defesa e os militares têm um papel indispensável, dadas as suas capacidades e recursos humanos únicos na abordagem de ambientes de alto risco, incluindo, nomeadamente, elevada prontidão e capacidade logística.

A integração no programa da nossa Presidência de questões relativas à defesa verde e à necessária atualização do planeamento estratégico de defesa face às pressões sociais que as alterações climáticas impõem, permite apostar na resiliência e numa gestão de riscos mais eficaz. É este o objetivo subjacente ao trabalho que nos propomos fazer quanto à melhoria da coordenação entre estruturas militares e civis da UE.

A pandemia COVID-19 tem sido um teste à resiliência dos Estados-Membros da UE, mas também à capacidade da UE de coordenar a assistência mútua

em situações complexas de emergência. Portugal foi um dos iniciadores da partilha de lições aprendidas entre Estados-Membros e defendeu a criação de uma *task force* no Serviço Europeu de Ação Externa para avaliar a resposta das Forças Armadas dos Estados-Membros à pandemia, identificar lacunas, desafios e boas práticas, bem como formas de melhorar a cooperação mútua em resposta a emergências complexas. A Presidência pretende desenvolver o trabalho desta *task force*, bem como operacionalizar a utilização das capacidades militares dos Estados-Membros em apoio do Mecanismo de Proteção Civil da União Europeia.

Para terminar, gostaria de sublinhar que o esforço de construção de uma cultura estratégica europeia partilhada deverá começar pelo reconhecimento de que as transformações em curso na geopolítica global tornaram a União Europeia mais indispensável do que nunca. A criação de uma Defesa Europeia tem sido um processo demorado, complexo e repleto de desafios. Ainda hoje, apesar dos importantes avanços que têm ocorrido nesta política, é por vezes difícil, e pode ser frustrante, encontrar um acordo eficaz por unanimidade entre um grupo de 27 países com sistemas nacionais de defesa tão díspares. Mas não há alternativa. Uma tarefa decisiva desta cultura estratégica europeia será, portanto, construir pontes entre as prioridades estratégicas dos diferentes Estados Membros, e realçar que precisamos de investir na modernização das nossas capacidades militares para defender os nossos valores, bem como os nossos interesses no mundo do século XXI.

OPERAÇÕES CONJUNTAS ENTRE FORÇAS ARMADAS E POLICIAIS – entre Cila e Caríbdis –

AGOSTINHO COSTA
Major-General
Vice-Presidente do Centro de Estudos EuroDefense – Portugal
Membro do Grupo de Reflexão Estratégica sobre Segurança (IDS/FD-UNL)

1. PREAMBULO

O tema em epígrafe tem estado na ordem do dia também no plano nacional, em particular a partir da onda de ataques terroristas registada um pouco por toda a União Europeia. Teve o seu ponto inicial no ataque ao jornal satírico francês Charlie Hebdo, em 7 de janeiro de 2015 e como episódios mais recentes, em certa medida relacionados com o primeiro por envolverem as caricaturas do profeta Maomé, o assassinato do professor Samuel Paty em Paris, em 16 de outubro e o atentado perpetrado num tempo católico de Nice, em 29 de outubro de 2020.

A ameaça do terrorismo, particularmente o de matriz jihadista e, mais recentemente, as questões associadas à implementação dos três primeiros estados de emergência, que vigoraram entre 19 de março e 2 de maio de 2020, em resposta à crise pandémica provocada pelo novo coronavírus

SARS-CoV-2, trouxeram à colação a questão do emprego das forças armadas na ordem interna, para além do vulgarmente referido por "outras missões de interesse público". Importa salientar que o seu emprego neste contexto enquadra-se no estipulado pela Lei de Defesa Nacional (Lei Orgânica n.º 1 -B/2009, de 7 de julho) alterada em 29 de agosto de 2014, que no tocante às Missões das Forças Armadas estabelece, respetivamente, nas alíneas e) e f) do Art.º 24º que: "*Nos termos da Constituição e da lei, incumbe às Forças Armadas: e) Cooperar com as forças e serviços de segurança tendo em vista o cumprimento conjugado das respetivas missões no combate a agressões ou ameaças transnacionais; f) Colaborar em missões de proteção civil e em tarefas relacionadas com a satisfação das necessidades básicas e a melhoria da qualidade de vida das populações*."

Em 28 de fevereiro de 2020, após quase dois anos de negociação entre o CEMGFA e a Secretária-Geral do Sistema de Segurança Interno, realizou-se a assinatura de um protocolo entre os ministérios da defesa nacional e da administração interna, relativo à "articulação operacional entre as Forças Armadas e as Forças e Serviços de Segurança contra as ameaças transnacionais". Não obstante a assinatura do protocolo, que teve ampla cobertura mediática, ficou em aberto uma questão essencial – a das regras de empenhamento dos militares, i.e., do emprego da força.

O texto do protocolo não é do conhecimento público, contudo, os seus efeitos práticos parece terem ficado bem patentes no incidente ocorrido em 31 de março de 2020, entre agentes da PSP e uma força do Exército empenhada na desinfeção de um lar em Vila Real, que culminou com a identificação do comandante da força militar por parte dos elementos policiais. Este facto foi causador de mal-estar no meio castrense, como atestam as declarações do Chefe do Estado-Maior do ramo na Assembleia da República. A leitura que o Diretor Nacional da PSP fez dos acontecimentos é também expressiva da divergência de pontos de vista sobre a matéria.

Esta ocorrência torna legítimo equacionar-se se a assinatura do protocolo não terá contribuído para adensar os equívocos sobre a matéria, legitimando uma atitude por parte da PSP que nas circunstâncias anteriores não lhes teria certamente ocorrido. Uma primeira ilação se poderá retirar deste incidente – a ação conjunta entre forças armadas e de polícia civil não é

uma questão resolúvel apenas através da assinatura de um protocolo e a situação hoje aparenta ser bem mais complexa do que no antecedente.

2. ENQUADRAMENTO

A questão em apreço não é, portanto, de mera coordenação, que possa subsumir-se à vontade política dos ministérios das respetivas tutelas, ou à vontade de cooperação entre duas personalidades no vértice das instituições militar e policial. A existência, no quadro da segurança interna, de um plano com propósito semelhante, o "Plano de Coordenação, Controlo e Comando Operacional das Forças e Serviços de Segurança (Deliberação n.º 230/2006, de 18 de maio)", delineado para desconflituar a ação operacional entre a GNR e a PSP, é já por si um indiciador das dificuldades existentes no seio do próprio MAI, em articular duas forças com missões semelhantes e que não raras vezes se vêm envolvidas em questões quixotescas de disputa pela prevalência territorial.

Sendo mais fácil a um cidadão cruzar-se com uma patrulha combinada da GNR com elementos da Guarda Civil espanhola, dos Carabinieri italianos ou da Gendarmerie francesa, ou da PSP com os seus congéneres das polícias nacionais daqueles países, do que encontrar uma patrulha mistas da GNR e PSP, será espectável que se não for devidamente equacionado um racional que enquadre e sustente a real necessidade da ação conjunta entre as forças militares e policiais na segurança interna, estaremos sempre no domínio do que os anglo-saxónicos designam por *wishful thinking*.

Acresce que durante o período da atual segunda república não existe, neste domínio, um referencial para o sistema de segurança interna português, dada a clara divisão de trabalho existente entre militares e polícias, ainda muito assente na conceção realista da segurança. Persistem ainda alguns fantasmas do Estado Novo, que importa lembrar teve a sua génese na ditadura militar imposta pelo golpe do 28 de maio de 1926. Por outro lado, estão praticamente reduzidas ao ciclo dos historiadores, as particularidades e vicissitudes do modelo de segurança interna da monarquia constitucional, um período onde o Exército foi amplamente empregue na ordem interna, facto que em boa parte inspirou a reforma encetada em 1867 pelo então

ministro do reino Martens Ferrão, pese embora não tenha sido consomada na totalidade em virtude da instabilidade política da época.

Importa, no entanto, salientar que nas circunstâncias atuais o tema não é completamente alheio ao conhecimento e experiência tanto das forças armadas como das polícias, nomeadamente da GNR e PSP, em virtude da sua vasta experiência em operações multinacionais. Consequentemente, para responder à questão central de "como articular operações conjuntas entre forças armadas e policiais no território nacional?", a referência adequada é a da experiência recolhida e lições aprendidas nas missões internacionais em que Portugal tem tomado parte e onde tem sido possível obter vasta experiência sobre a matéria. Será, pois, esse o referencial de análise para a abordagem do assunto.

3. DESAFIOS DAS ALTERAÇÕES NO AMBIENTE SEGURANÇA

Poder-se-á argumentar que, no essencial, os conflitos armados e as crises que as antecedem não mudaram na sua essência e que os princípios da guerra se lhes aplicam no essencial, atentos os desenvolvimentos tecnológicos que têm produzido alterações substanciais na conduta das operações.

A guerra resume-se sempre a uma oposição entre vontades, onde os interesses em causa justificam o recurso à força. Consoante o seu grau de relevância, assim as guerras assumem um caráter limitado ou total. Os fins-últimos da guerra continuam orientados para a destruição do Inimigo, ou da sua vontade de combater. Em síntese, no plano dos propósitos da guerra, poderá não se ter verificado uma alteração substancial, contudo, o contexto em que se processa e no domínio dos processos têm-se verificado alterações substanciais.

Da prevalência dos desígnios do Estado transitou-se para a centralidade na proteção das pessoas, que consubstancia uma mudança de perspetiva sobre a soberania, onde a responsabilidade de proteger (R2P) representa mais do que uma máxima, mas antes uma mudança de paradigma, onde a dimensão da segurança humana ganha prevalência em relação à da segurança do

Estado. Por outro lado, o ambiente de segurança espelha as antinomias do tempo atual, onde as interpretações analíticas de causa-efeito são insuficientes para a compreensão dos fenómenos securitários. Questões como o terrorismo, as redes de criminalidade organizada transnacional, nas suas diferentes variantes, das relacionadas como as diferentes formas de tráfico ao cibercrime, estão na ordem do dia. A proliferação de atores não estatais motivados por agendas políticas ou pelo propósito de encaixe económico, potenciados pelos meios facultados pela globalização e embrenhados na estrutura social, ou operando a partir de santuários em Estados falhados, todos, no seu conjunto, conferem ao atual ambiente de segurança uma das suas características principais – a complexidade.

Em síntese, o ambiente de segurança caraterizado por uma multiplicidade de atores, pluralidade de interesses e formas diversificadas de atuação, por regra assimétricas e frequentemente empregues de forma concorrencial, consubstancia uma matriz de conflitualidade designada por conflitos híbridos, ou de 4ª geração. Integra-se no atual clima de competição estratégica entre grandes potências como forma de equilibrar as respetivas assimetrias de potencial estratégico, em particular como manobra destinada a eximirem-se à ação estratégica da superpotência ainda dominante nos planos militar e tecnológico – os EUA.

Por regra as formas híbridas de conflitualidade processam-se em patamares abaixo do limiar da ação estratégica direta. Procuram manter-se em níveis de intensidade insuficientes para justificar a ativação de mecanismos de resposta que impliquem o envolvimento direto da força militar. Visam a paralisia do processo de decisão das organizações de defesa coletiva e, sobretudo, pretendem coartar a liberdade de ação estratégica dos EUA, atenta a dimensão global dos seus interesses.

Neste contexto, assume especial relevância a batalha no campo das perceções, travada pelas operações de informação e operações psicológicas, fazendo recurso às diferentes plataformas de comunicação orientadas para moldar as opiniões públicas. Não obstante o prolongado hiato de quase duas décadas da guerra global de contraterrorismo liderada pelos EUA, as operações multinacionais têm representado a principal forma de intervenção da comunidade internacional em prol da paz e segurança, seja

num contexto de estabilização pós-conflito, ou das diferentes vertentes de apoio à paz sob a égide das Nações Unidas. Contudo, em todas persiste um ponto comum – os desafios à segurança não cessam após a conclusão das operações de combate. Todos recordamos o discurso de George W. Bush a bordo do porta-aviões USS Abraham Lincoln, em 1 de maio de 2003, declarando a "missão cumprida", numa euforia que os acontecimentos naquele teatro de operações, durante os anos seguintes, se encarregariam de refrear.

Emergiram desafios à segurança de outra natureza, sejam os relacionados com movimentos de insurgentes, terrorismo, tumultos civis e diversas formas de criminalidade organizada, delinquência comum, ou a utilização do território como santuário por parte de outros atores, entre outras ameaças. No seu conjunto, conferem à situação uma dimensão de complexidade que extravasa a exclusiva capacidade de intervenção das forças armadas, por regra dimensionadas para o emprego da força máxima, com base na dualidade amigo/inimigo.

Consequentemente, nas circunstâncias aduzidas (operações de apoio à paz, de estabilização pós-conflito, de gestão de crises, etc.) as forças armadas passaram a ter de defrontar estes desafios à segurança, colocando-se com o dilema de terem de recorrer ao emprego desproporcional da força ou, em alternativa, optarem por uma postura de paralisia. Este hiato securitário, perante questões de segurança que tanto podem ser pré-existentes como emergirem na sequência das operações de combate, ou em virtude da forma como a fase de estabilização estiver a ser conduzida, representa um dado sério que requer respostas com efetividade. Estes constrangimentos estiveram bem patentes na anarquia vivida no Kosovo, em 1999, após a retirada das autoridades sérvias e no Iraque após as instituições do Estado terem sido deliberadamente dissolvidas pelas forças ocupantes, em 2003. As pilhagens, o caos e o clima de impunidade foram factos que permanecem bem presentes na nossa memória coletiva.

Talvez o exemplo mais elucidativo deste contexto securitário foi a emergência do autointitulado estado islâmico, exemplo paradigmático de um efeito emergente da estratégia conduzida pelo ocidente no combate à Al-Qaeda no Iraque, através do apoio as fações sunitas e grupos armados que viriam

a criar condições para a emergência do califado, que Abu Bakr al-Baghdadi decretou em 29 de junho de 2014 na mesquita de Mosul, no Iraque. Trata-se de um fenómeno que teve repercussões à escala global, abrindo um novo capítulo no terrorismo, agora em modo *franchising* e que não se extinguiu com o colapso do Daesh.

As operações multinacionais processam-se assim em contextos para os quais já não são suficientes as teorias explicativas de base analítica, assentes em lógicas de causa-efeito, atestando que os diferentes atores num teatro de operações se comportam como variáveis interdependentes de um sistema complexo e adaptativo, cujo controlo está para além da capacidade do comando da operação, tanto nos planos político, como estratégico, operacional e tático.

No quadro explicativo, a aplicação da teoria dos sistemas às operações militares, em linha com a COPD da NATO, consubstancia a aplicação daquela teoria ao planeamento e condução das operações. Trata-se de um documento de referência na formulação da doutrina da Aliança Atlântica que deve merecer particular atenção por parte de quem tem a responsabilidade pelo planeamento nos níveis político, político-estratégico e operacional, tanto das operações militares como das forças de segurança, atentas as necessárias adaptações.

O hiato securitário, a abordagem sistémica e, sobretudo, o imperativo de conquistar as mentes e os corações das populações locais constituem requisitos para o sucesso e concorrem para mitigar o impacto negativo que as baixas civis, frequentemente apelidadas como danos colaterais, têm nas opiniões públicas. A necessidade de conferir versatilidade ao emprego da força emerge assim como um importante requisito para a efetividade (eficácia e eficiência) da operação multinacional. Apresenta-se ainda como um catalisador da transformação processada nas operações em apreço, que teve início na da Bósnia-Herzegovina (SFOR). Recolheu ensinamentos dos anos anteriores em que a ONU procurou manter a paz no território (UNPROFOR). Pela primeira vez uma operação passou a poder contar com as capacidades necessárias para o emprego versátil da força.

O *litmus test* desta operação, bem como das que lhe sucederam, primeiro

no Kosovo (KFOR e EULEX) e depois no Afeganistão (ISAF), foi o desenho de uma estrutura com capacidade para emprego da força em todo o espectro, cuja versatilidade foi assegurada pelo conjunto de unidades das forças armadas (força máxima), forças de polícia de matriz gendármica (força intermédia) e de polícia civil (força mínima), ficando assim apta para dar resposta cabal às várias tipologias de desafios à segurança.

4. ENTROPIAS À COOPERAÇÃO ENTRE FORÇAS ARMADAS E POLICIAIS NAS MISSÕES INTERNACIONAIS

A resistência à mudança é uma reação expectável, muito mais por parte de instituições com fortes culturas organizacionais, práticas enraizadas e estruturas orgânicas fortemente hierarquizadas, como são tanto as forças armadas como as policiais.

As dificuldades na implementação deste modelo não se subsumem apenas às forças armadas, onde em alguns quadrantes se regista algum desconhecimento sobre a tipologia das missões cometidas às polícias, aliado a um paroquialismo enraizado numa ideia de prevalência do múnus militar nas operações sob comando das forças armadas. Também se regista oposição em submetê-las a um *downgrade* de atuação, que comporte algo menos do que o emprego da força máxima, bem tipificado no epítetos *overwhelming force* e *shock and awe* que norteiam a doutrina de atuação das forças armadas dos EUA, considerados como forma de alcançar uma vitória simultaneamente rápida e com mínimo de baixas.

Regista-se também resistência por parte das estruturas de polícia civil, uma vez que a dicotomia gendarmeries/polícias civis consubstancia modelos de organização policial distintos nos países integrantes das operações multinacionais. Os do Norte da Europa, por exemplo, não dispõem desta capacidade, com a honrosa exceção da Marechaussee na Holanda. Este facto acarreta limitações não só no plano formal, mas também no informal. Decorrem tanto da falta de experiência como do tipo de práticas de atuação policial enraizadas naqueles países, que justificam as objeções que colocam ao emprego conjunto das polícias civis com as forças armadas.

Estão assim em vantagem os países que têm forças policiais de matriz gendármica e, em particular, aqueles que reúnem experiência de as empregar no quadro da segurança interna conjuntamente com as forças armadas, como é o caso da Itália, onde as forças armadas têm um historial de colaboração com os Carabinieri no combate às Máfias do Sul do país. Não admira, portanto, que desde meados da última década do século passado a Itália se tenha destacado na liderança dos principais avanços e inovações que se verificaram neste domínio.

Outra questão a tomar em consideração é o facto de a atuação das forças armadas se enquadrar no quadro do Direito Internacional Humanitário ou dos Conflitos Armados, ao passo que a das polícias obedece ao Direito Internacional dos Direitos Humanos, o que não sendo impeditivo da atuação conjunta não pode, no entanto, deixar de ser tido em conta.

Também no plano da dependência funcional, as unidades policiais de matriz gendármica, por regra, inserem-se na estrutura de comando militar, tornando a coordenação da sua atuação conjunta com as forças armadas mais facilitada, ao passo que as de polícia civil ficam, normalmente, subordinadas a cadeias de coordenação distintas, inseridas na estrutura civil da missão. Em síntese, mesmo no quadro das missões internacionais uma ação que acarrete o emprego concomitante do conjunto destas forças não deixa de se revestir de complexidade.

5. AJUSTAMENTOS ESTRUTURAIS, ACERTOS NAS FUNÇÕES E ALTERAÇÕES NOS PROCESSOS COM VISTA AO EMPREGO VERSÁTIL DA FORÇA.

A Implementation Force (IFOR) da NATO, na B-H, iniciou-se em janeiro da 1996 com o propósito de pôr cobro ao conflito étnico que perdurava naquele Estado da antiga Jugoslávia desde 1992, com um extenso registo de atrocidades e todo o tipo de atropelos aos Direitos Humanos. Seguiu-se a uma campanha aérea da NATO destinada a obrigar as partes a sentarem-se à mesa das negociações, tendo culminado com o Acordo de Dayton, em 21 de novembro de 1995.

É pertinente relembrar que os esforços de mediação do conflito foram inicialmente protagonizados pela European Community Monitor Mission (ECMM), uma missão civil composta por um misto de militares e diplomatas que durante o primeiro semestre de 1992, durante o período da presidência portuguesa do Conselho Europeu, teve um desempenho assaz relevante. No essencial, o plano então gizado pelo chefe da missão, o embaixador José Cutileiro, prognosticou as linhas gerais acordadas em Dayton. A partir do segundo semestre daquele ano o protagonismo transitou para as Nações Unidas que alargaram àquele território o âmbito da ação da operação de manutenção de paz da Croácia (UNPROFOR).

Os elementos policiais seguiam aqui uma lógica de atuação próxima da dos observadores militares, com a diferença que estes monitorizavam as atividades das forças beligerantes, zelando pelo cumprimento do cessar-fogo e aqueles monitorizavam a ação das polícias locais. Atuavam desarmados e em funções de observação da situação no terreno, assegurando o correspondente reporte para a direção da CIVPOL junto da estrutura civil da missão.

A UNPROFOR marcou um ponto de viragem nas missões de manutenção de paz, nomeadamente após os trágicos acontecimentos em Srebrenica, que marcam o epílogo das ambiguidades do modelo preconizado pelas Nações Unidas. No caso em apreço eram adensadas pelo paradoxo da força de manutenção de paz estar inserida num território onde estava em curso uma situação de guerra, com a ação limitada por regras de empenhamento ambíguas e sem efetiva capacidade de combate, com uma parte dos seus elementos desarmados.

A IFOR, por seu turno, seguiu uma lógica de imposição da paz, com regras de empenhamento muito mais amplas e claras e forças armadas dotadas de uma tipologia de capacidades mais robusta em relação à missão da ONU que a antecedeu. No domínio policial, a estrutura de polícia das Nações Unidas que sucedeu à CIVPOL, a UN International Police Task Force (IPTF), seguia, no entanto, um racional semelhante ao do antecedente, apresentando uma capacidade operacional reduzida. Tornaram-se patentes os obstáculos à sua eficácia quando foi colocada a questão da detenção de pessoas indiciadas por crimes de guerra, a mando do Tribunal Criminal

para a ex-Jugoslávia. Por outro lado, os tumultos que se verificaram em 1997, na região de Brcko, revelaram a incapacidade da IFOR para fazer face a esta tipologia de problemas de segurança e acentuou as dificuldades de coordenação operacional da atuação entre militares e polícias.

Só em 1998, já sob o mandato da Stabilization Force (SFOR), com a criação da Multinational Specialized Unit (MSU), uma força de gendarmerie liderada pela Itália e colocada sob comando da SFOR, aquele hiato de segurança viria a ser eliminado. A MSU mostrou-se relevante na B-H e também a partir daí em todas as operações da NATO, sendo um instrumento essencial à disposição do Comando militar da operação em domínios tão relevantes quantos os do controlo de tumultos, investigação criminal, informações policiais, atuação de equipas SWAT (operações especiais) e no processo de capacitação das forças de polícia locais. Foi a MSU que possibilitou o desenvolvimento de conceitos de atuação conjunta agora amplamente adotados, como o de Blue Box/Green Box, destinado a simplificar procedimentos táticos e clarificar relações de comando, possibilitando uma articulação correta entre forças armadas e policiais. Por outro lado, também inspirou uma evolução no campo da polícia civil com o surgimento das Special Police Units (SPU), unidades de polícia mais robustas e com um quadro de atuação mais abrangente.

O domínio da capacitação das estruturas de segurança locais (Security Sector Reform), seja das forças armadas seja das policiais, é outro dos importantes desafios que se colocam à liderança política das operações multinacionais. Também aqui persistem modelos distintos e perspetivas concorrentes sobre os referenciais a seguir: entre os defensores da edificação de uma polícia de matriz civil, regulada por mecanismos de governação e escrutínio democrático em tudo idênticos aos dos países ocidentais; aos que protagonizam a criação de forças gendármicas, com estruturas mais robustas, mas com capacidade de atuação em todo o espectro das missões policiais, entendidas como o modelo mais ajustado a um ambiente de segurança com a vicissitudes próprias das situações de pós-conflito; e, por fim, aos que defendem a edificação de forças em tudo idênticas às militares, ou de matriz paramilitar, aptas para atuar como as forças armadas, quando necessário, com vista a poderem conduzir ações de contrainsurgência e contraterrorismo, através do recurso a níveis de força máxima. Neste do-

mínio, as quase duas décadas da operação no Afeganistão têm sido um *case study* sobre os reiterados esforços encetados por parte de uma pluralidade de atores, que compreende militares, gendarmes, polícias civis e empresas privadas de segurança.

Nos cerca de trinta anos de operações de apoio à paz e de estabilização, que constituem o esforço que a comunidade internacional tem vindo a realizar em prol da paz e segurança internacional, por via da intervenção em conflitos regionais, dos Balcãs ao Médio Oriente, do Sahel a Timor-Leste, outra das alterações a registar enquadra-se na metodologia do seu planeamento e condução. O Estado Final desejado pressupõe alcançar os objetivos, após atingidas as condições decisivas, permitidas pelos efeitos provocados pelas ações desenvolvidas por uma panóplia de atores, que não se subsumem às forças armadas. Envolvem igualmente forças policiais, organizações internacionais, organizações não governamentais e atores locais, para além de outros agentes, concorrendo todos de modo interdependente para o Estado Final desejado.

Para obviar hiatos de segurança durante o período a seguir às operações de combate, quando as opções de resposta se limitam apenas às militares, potencialmente excessivas por serem desproporcionais face à dimensão dos problemas de segurança, ou conduzindo a situações de paralisia decorrentes da decisão de não empregar a força máxima, é hoje dado assente que na panóplia de opções devem constar capacidades de força intermédia e de força mínima, aquelas garantidas pelas polícias de matriz gendármica e estas por polícias civis. No seu conjunto asseguram um requisito essencial à operação – a emprego versátil da força. Acresce que com frequência o emprego destes níveis de força deve ser simultâneo e de forma conjunta e coordenada, pelo que não basta deter a capacidade, sendo preciso ser capaz de a empregar com a efetividade necessária.

A questão de fundo que então se coloca é como preparar forças armadas para o emprego da força abaixo do nível máximo para que estas estão vocacionadas e como adequar as polícias a utilizar níveis de força mais elevados do que aqueles para que foram dimensionados. Neste último domínio basta olhar para as cidades europeias e norte-americanas para depreender que o terrorismo se encarregou de mudar quer a imagem como a postura e forma

de atuação dos diferentes níveis da intervenção policial.

Nas atuação das forças armadas, mas também no fenómeno de militarização das polícias civis a que se tem assistido ao longo dos últimos cinco anos, importa ter em conta as diferenças nos planos do material, do treino e preparação, da cultura organizacional, do quadro legal, da estruturas organizacionais e no âmbito das formas de atuação operacional, onde persistem substanciais e óbvias diferenças, não obstante no primeiro (material) comece a ser difícil diferenciar polícias e militares, até pelo facto da adoção de uniformes em tudo idênticos.

6. CONCLUSÕES

A fase inicial das operações de combate faz apelo à utilização de capacidades que, por regra, recorrem à "força máxima", enquadradas num quadro jurídico do Direito Internacional Humanitário ou dos Conflitos Armados. Este é um domínio para a qual as forças armadas estão, naturalmente, melhor dotadas, sendo mesmo o seu *core business*. Volvida essa fase os desafios de segurança no Teatro de Operações permanecem, embora com outra matriz, que pode ir do terrorismo à insurgência, dos tumultos à criminalidade organizada, até à criminalidade comum, passando pelas questões do combate às redes de narcotráfico, de tráfico de seres humanos e a outras formas de crime organizado. Frequentemente, acresce ainda a captura de pessoas indiciadas por crimes de guerra. Este conjunto de requisitos de segurança complexificam o cumprimento da missão, confrontando a direção política e o comando da operação com vicissitudes para as quais as forças militares regulares não estão dimensionadas.

A aplicação de níveis de força intermédia e de força mínima não é uma vocação das forças armadas, não se enquadrando na tipologia do seu material, doutrina, quadro legal de atuação e na estrutura cultural que as molda. A utilização exclusiva de forças armadas tem conduzido, por regra a um emprego desproporcionado da força, ou, em contrapartida, à sua paralisia, penalizando a legitimidade da operação e dificultando o objetivo de conquistar as mentes e os corações das populações.

As forças de segurança, quer as de matriz gendármica como as de polícia civil apresentam-se, assim, como os atores que preenchem um espectro de atuação compreendido entre a força máxima (das forças armadas), força intermédia (das gendarmeries) e força mínima (das polícias civis), conferindo assim ao comando da operação a versatilidade que se impõe para o cumprimento cabal e efetivo da sua missão.

Acresce que este desafio não se coloca apenas às operações internacionais durante a chamada fase de transição que se segue à das operações militares de combate, até ao retorno do território à situação de normalidade, de que as operações da B-H e do Kosovo são exemplos. Surge também no quadro das operações em teatros onde, concomitantemente, a força internacional se tem que confrontar com o misto das questões de segurança acima referidas, que vão do crime comum à insurgência, sendo o Afeganistão um caso paradigmático.

Em ambos os cenários a volatilidade do ambiente de segurança requer da parte da força internacional a capacidade para dosear o emprego da força em função do problema de segurança e encetar a capacitação das forças de segurança locais para resolverem de forma efetiva (com eficácia e eficiência) as questões de segurança. Pressupõe a observância de um quadro legal assente no Direito Internacional dos Direitos Humanos, onde o insurgente, o terrorista e o traficante são tratados como delinquentes, a serem presentes a tribunal, negando-lhes o estatuto de combatentes, onde a alternativa é serem abatidos ou tratados à margem dos princípios do Estado de Direito.

Em síntese, quer nas operações internacionais como no quadro da segurança interna, a questão em análise não se subsume a questionar a coexistência de forças armadas e policiais, mas antes a forma de assegurar a sua efetividade, esbatendo mal-entendidos, eliminando entropias e assegurando estruturas de comando e regras de atuação adequadas e consequentes.

A experiência mostra-nos que no seu conjunto, forças armadas, de gendarmerie e de polícia civil, preenchem a totalidade do espectro das capacidades necessárias para emprego da força de uma forma doseada e ajustada às circunstâncias da operação, evitando assim quer o emprego desproporcional da força, quer situações de paralisação motivados pela desadequação do

nível de resposta. Esta realidade mostra-se um imperativo crescente mercê da natureza dos desafios complexos à segurança que presentemente as operações enfrentam, em ambientes de segurança voláteis, com atores que frequentemente recorrem a formas de atuação assimétrica e que requerem respostas de amplo espectro.

Consequentemente, a questão de fundo que se coloca às Forças Policiais, no contexto das operações multinacionais com um forte pendor da componente forças armadas, é por um lado a questão da efetividade do seu emprego, em virtude de eventuais distopias no entendimento das suas capacidades e, também, pelo atrito decorrente de modos de atuação distintos. Por outro lado, as questões de interoperabilidade que não se subsumem ao comando e controlo, mas essencialmente a questões de doutrina, treino conjunto e conhecimento mútuo entre forças armadas e policiais.

O conceito de força versátil, em que as forças armadas são convocadas ao emprego da força mínima e as forças policiais, quando necessário, a empregar a força máxima, contraria o da especialização, que tem sido a matriz da "divisão de trabalho" entre militares e polícias e que continua a moldar o quadro intelectual tanto de uns como de outros. Não obstante as boas-vontades e o entusiasmo no plano das intenções, os ânimos parecem esfriar quando está em causa a alocação de meios, de capacidades ou missões. O recente desconforto causado pelo reequipamento da Unidade de Controlo Costeiro da GNR como meios oceânicos é disso exemplo, atestando que o interesse nacional deverá sempre sobrepor-se às disputas corporativas e, sobretudo, ter consciência de que a diferença está sempre no plano da liderança política.

Não está nos objetivos desta reflexão especificar os detalhes da forma como as forças armadas e policiais deverão atuar conjuntamente no quadro da segurança interna do nosso país, atentos os condicionantes normativos que enquadram o assunto. A consciência de que já o fazem no âmbito das missões internacionais é demonstrativa de que a questão não é intransponível, não obstante a pluralidade de fatores de entropia e disfuncionalidade que persistem na articulação das próprias polícias. Estes estão patentes em premissas anacrónicas como as de "polícia integral", "competência reservada" e no sacrossanto princípio da "territorialidade", para além da

proliferação de uma miríade de atores com competências de investigação criminal que fazem da eficiência do sistema de segurança interna um verdadeiro nó górdio.

Em conclusão, o tema em apreço faz apelo a uma transformação do sistema de segurança nacional, convidando-nos a repensá-lo e a encetar uma *Security Sector Reform* que tenha em conta os imperativos de mudança nos planos material, educacional, cultural, legal, organizacional e operacional. Esse é, decididamente, o grande desafio que se coloca a Portugal no tempo presente, para que tanto as forças armadas como as forças de segurança possam estar em sintonia com os desafios colocados pelo atual ambiente de segurança e o Estado possa eliminar anacronismos que não só penalizam o erário público, como são motivo de justificada perplexidade por parte dos cidadãos.

Lisboa, 27 de novembro de 2020

REFERÊNCIAS BIBLIOGRÁFICAS:

Friesendorf, C. & Krempel J. (2011). Militarized versus Civilian Policing: Problems of Reforming the Afghan National Police: Peace Research Institute Frankfurt (PRIF).

Friesendorf, C. (2012). International Intervention and the Use of Force: Military and Police Roles: The Geneva Centre for the Democratic Control of Armed Forces.

ACO (2013). Allied Command Operations Comprehensive Operations Planning Directive (COPD) Interim Version 2.0. Mons: Allied Command Operations.

Krahmann, E. & Friesendorf, C. (2014). Undermining Human Security - Private Security Companies, the APPF, Militias and Auxiliary Police in Afghanistan: Peace Research Institute Frankfurt (PRIF)

Lourenço, N. & Costa, A. (2018). Estratégia de Segurança Nacional. Portugal Horizonte 2030. Coimbra: Almedina.

UNIÃO EUROPEIA

A NECESSIDADE DE COOPERAÇÃO NA DEFESA

ANTÓNIO BRÁS MONTEIRO

Gestor de Projetos no Grupo Tekever

Membro da Direção da Euro-Defense Portugal

Membro do Conselho Consultivo da IntellCorp

Membro do Conselho Consultivo do AED Cluster Portugal

Editor e Correspondente Especial na European Security & Defence

Enfrentamos há cerca de um ano a pandemia de SARS-CoV-2 e, em algumas zonas de Espanha e Itália durante o primeiro semestre de 2020, bandeiras da União Europeia não foram hasteadas em sinal de protesto ou foram incendiadas. Não querendo ser alarmista, e tendo observado um conjunto de eventos contrários ao espírito da UE, creio que estamos em boa altura de reforçar a cooperação na Defesa da União Europeia.

No quadro supra, a União Europeia adotou, surpreendentemente, um corte de 39% no Fundo Europeu de Defesa (uma redução de seis mil milhões de euros). Boris Johnson anunciou um incremento de mais de 18 mil milhões de euros para a Defesa no Reino Unido. Já os EUA auguram despender este ano mais de 600 mil milhões de euros com a Defesa.

Nos anos noventa já Molas-Gallart e Hawkins tinham escrito um estudo que acabou por se tornar famoso, o "Sussex Study". Neste estudo, onde

relataram várias recomendações, os autores declararam que a UE deveria desenvolver um "*European Defence Standardisation Handbook*". Na altura, a Comissão Europeia seguiu o parecer e a UE iniciou o novo milénio focando os seus esforços no aperfeiçoamento da eficácia militar, na poupança e redução de custos nos investimentos com a Defesa, acautelando uma duplicação de capacidade e equipamento. Lutando ainda por uma economia e união política mais inovadora e interoperável, se considerarmos as cadeias de abastecimento e as alianças além-fronteiras. Assim, um significativo número de políticas e estratégias foram estabelecidas para tornar a segurança da UE mais forte e permitir uma maior cooperação na Defesa entre Estados-Membros.

Decorridas três décadas, não seria tempo de inverter a tendência de investimento na Defesa europeia, face a um crescente número de novas ameaças transnacionais e um contexto securitário e geopolítico totalmente distinto, substancialmente mais complexo e fluído?

Uma síntese dos complexos, mas eficazes acrónimos

A Política Comum de Segurança e Defesa que segue a Estratégia Global da UE para a política externa e de segurança de 2016, define não só a agenda político-militar (enquanto o Tratado de Lisboa dá mais poder às tarefas do Parlamento Europeu e aos seus aspetos institucionais), como é parte integrante da Política Externa e de Segurança Comum que é a política de segurança e defesa estabelecida pela UE para as relações internacionais, sendo vital para a Defesa da UE e para o seu processo de gestão de crises.

Novembro de 2016 foi um mês decisivo, com conclusões críticas do Conselho da UE baseadas no Plano de Implementação da UE na Defesa e Segurança, apresentado na altura, pela Alta Representante e Vice-Presidente Federica Mogherini, colocando assim em prática a supramencionada Estratégia Global da UE de forma a proteger a UE e os seus cidadãos. Medidas adicionais para melhorar a segurança da UE incluíram a Cooperação Estruturada Permanente (*Permanent Structured Cooperation* - PESCO), iniciada com o Tratado de Lisboa, onde a agenda acordada entre os Estados-Membros participantes se comprometem imperiosamente a uma estreita cooperação com o objetivo de uma Defesa mais capaz e eficaz nos investimentos.

A Agência Europeia de Defesa e o Serviço Europeu para a Ação Externa têm um papel crucial na Cooperação Estruturada Permanente, até porque são ambos o seu secretariado. A Cooperação Estruturada Permanente está também diretamente relacionada com a Análise Anual Coordenada em Matéria de Defesa (*Coordinated Annual Review on Defence* - CARD), também gerida pela Agência Europeia de Defesa, e com o recente e importantíssimo Fundo Europeu de Defesa e o seu Programa Europeu de Desenvolvimento Industrial no domínio da Defesa, que complementam a Cooperação Estruturada Permanente.

A Análise Anual Coordenada em Matéria de Defesa monitoriza os planos nacionais de investimento em Defesa, ao passo que o Fundo Europeu de Defesa concede incentivos financeiros para estimular a pesquisa, desenvolvimento e a cooperação em matéria de projetos colaborativos de capacidades militares. Temos como exemplo os perto de 50 projetos empreendidos pela Cooperação Estruturada Permanente, onde Portugal também participa. Também a Análise Anual Coordenada em Matéria de Defesa é fundamental para operacionalizar o Plano de Desenvolvimento de Capacidades, que é por sua vez essencial para o processo de tomada de decisão da UE, relativamente ao desenvolvimento de capacidades militares. Em 2018 o Plano de Desenvolvimento de Capacidades foi revisto e atualizado e a Agência Europeia de Defesa classificou-o como uma ferramenta estratégica geral, no pacote das quatro estratégias de longo prazo, direcionada para as necessidades de capacidades futuras de curto a longo prazo da UE.

Cooperação e estandardização para reduzir a fragmentação e duplicação de capacidades militares

A Agência Europeia de Defesa dispõe de diversas ferramentas para operacionalizar estas políticas e estratégias e também para encorajar a supramencionada estandardização. Podem-se indicar duas, a título de exemplo, nomeadamente: o *European Defence Standardisation Information System* (EDSIS), que é o portal central para todos os serviços Europeus de equipamentos de Defesa, e o *European Defence Standards Reference System* (EDSTAR), uma plataforma Web que abarca as normas de utilização de milhares de *standards*, fundamentais para suportar a Indústria de Defesa para o *procurement*. Entretanto, um novo Comité para a Estandardização da

Defesa Europeia (*European Defence Standardisation Committee* - EDSC) foi lançado na Agência Europeia de Defesa no final do ano passado, e na sua primeira reunião os participantes acordaram em produzir um novo estudo para uma revisão profunda do atual EDSTAR.

O fundamento para tantos instrumentos é que os Estados-Membros da UE estão a investir mais de €200 mil milhões por ano em Defesa (mais do que 1.3% do PIB da UE) e, de acordo com estatísticas oficiais da Comissão Europeia de 2018 ("*the business case for Defence cooperation*") **poder-se-á poupar entre 25 a 100 mil milhões de euros por ano se existir uma maior cooperação.** Necessitamos simplesmente de reduzir a existente duplicação. Atualmente, a UE tem 29 modelos diferentes de *destroyers* e fragatas e os EUA têm quatro. A UE tem 20 diferentes modelos de aviões de combate e os EUA têm seis. A UE tem 17 modelos diferentes de carros de combate e os EUA têm apenas um modelo. Também o atual Alto Representante e Vice-Presidente, Josep Borrell, alertou publicamente para esta fragmentação e duplicação existente na UE. Como Daniel Fiott declarou recentemente, por cima destes custos e duplicações está ainda o panorama geopolítico Europeu Numa altura em que a despesa com a Defesa estava a crescer, a padronização e cooperação deveriam ser a prioridade da Defesa da UE.

Portanto, a Análise Anual Coordenada em Matéria de Defesa, a Cooperação Estruturada Permanente e o Fundo Europeu de Defesa são três ferramentas fundamentais de um pacote de Defesa abrangente e desenvolvido para o futuro da cooperação da UE no domínio da Defesa, a fim de garantir o crescimento de capacidades militares, bem como alcançar um nível de competitividade maior da indústria de Defesa da UE. De referir que com o recente Fundo Europeu de Defesa é, pela primeira vez na história da UE, dedicada uma parte do orçamento da UE à Defesa, de 13 mil milhões de euros de (2021 a 2027) que iriam financiar desde a pesquisa até ao desenvolvimento de capacidades. Também o *Preparatory Action on Defence Research* continuou com os seus 90 milhões de euros, em 2020, e estava previsto um "*European Defence Research Programme*" que iria assegurar com 500 milhões de euros por ano.

É notável que a Comissão Europeia e a Agência Europeia de Defesa tenham

vindo a trabalhar arduamente para atingir uma forte e competitiva Base Tecnológica e Industrial de Defesa Europeia. Como a Alta Representante e Vice-Presidente Federica Mogherini afirmou em dezembro de 2017, "ativei uma Cooperação Estruturada Permanente na Defesa – ambiciosa e inclusiva. Vinte e cinco Estados-Membros comprometeram-se a unir forças regularmente, a fazer coisas juntos, gastar juntos, investir juntos, adquirir juntos e agir em conjunto. As possibilidades da Cooperação Estruturada Permanente são imensas."

SARS-CoV-2 e a primeira CARD

Presentemente, a China consolida o seu papel no novo ambiente de segurança global. A par disso, outros grandes *players* como o Brasil, a Índia e a Rússia desenvolvem tecnologias de ponta. O atual Presidente dos EUA discute a vitória do Presidente-eleito Joe Biden, o mundo luta contra uma Pandemia e o Fundo Europeu de Defesa viu o seu orçamento ser cortado em 39% (de 13 mil milhões de euros para 7 mil milhões).

A Agência Europeia de Defesa e o *Military Staff* da UE prepararam a primeira Análise Anual Coordenada da Defesa, que teve lugar em novembro passado, tendo sido um sucesso. Todavia, ao nos debruçarmos sobre os resultados da primeira Análise Anual Coordenada da Defesa chegamos à mesma conclusão – fragmentação e duplicação – o que diminui drasticamente a eficácia dos investimentos de cada Estado e tem um enorme impacto na interoperabilidade das Forças Armadas dos Estados da UE. Este facto reforça a urgência de cooperação na Defesa. A Análise Anual Coordenada da Defesa solicitou aos Governos da UE que se apressem e se focalizem em "seis capacidades de próxima geração" de armamentos, com o intuito de acabar com a duplicação nacional onerosa. Isto inclui o desenvolvimento de um novo carro de combate, navios de patrulha, defesa no espaço, sistemas de combate individual, tecnologia de supressão de drones, sistemas de anti-acesso e de negação de área e desenvolvimento da mobilidade militar.

Neste quadro, para além da Análise Anual Coordenada da Defesa, também no verão passado vários Ministros da Defesa da UE começaram a desenvolver o "*Strategic Compass*" que será adotado em 2022, para orientar a implementação do nível de ambição da UE em matéria de Segurança e

Defesa.

Jiří Šedivý, *Chief Executive* da Agência Europeia de Defesa, afirmou recentemente numa entrevista ao EURACTIV que, "com a crescente pressão no ambiente estratégico da UE, o bloco não deve perder a oportunidade de começar a empregar todas as ferramentas ao seu alcance para aumentar a cooperação em defesa."

Como mencionado anteriormente, tem sido notável o trabalho que a Comissão Europeia e a Agência Europeia de Defesa têm vindo a desenvolver. Consequentemente, importa não esmorecer este esforço, procurando ir além da Declaração assinada em Varsóvia a 8 de julho de 2016, tendo por horizonte assegurar a autonomia estratégica da UE, rumo a uma Europa da Defesa. É fundamental uma UE mais unida, forte e autónoma. Aliás, afigura-se não existir alternativa.

Neste contexto, torna-se aconselhável colocar em prática todas estas políticas, estratégias, iniciativas e ferramentas, adotando uma verdadeira cooperação na Defesa da União Europeia. Não apenas pela eventual poupança de 100 mil milhões de euros por ano, mas ainda por óbvias mais-valias da efetividade que tal medida comporta para uma União Europeia mais segura e capaz de desempenhar o papel que lhe cabe no contexto da comunidade internacional.

O *NEW SPACE* E A SEGURANÇA E DEFESA

FRANCISCO VILHENA DA CUNHA
Chief Strategy Officer – Omnidea

Este artigo aborda um conjunto de considerações sobre as implicações da emergência do *New Space* para a Segurança e Defesa, e para as bases tecnológicas e industriais a trabalhar nestes setores.

O ESPAÇO E A DEFESA

A exploração do Espaço está desde a sua génese ligada à Defesa, em particular, à Guerra Fria que deu, nos anos 50, palco à corrida espacial que opôs os Estados Unidos à União Soviética na luta pela primazia: no posicionamento de satélites em órbita, para recolha de imagens e informação, e na exploração espacial, da qual foi um marco fundamental a chegada do Homem à Lua em 1969.

Desde então, a atividade espacial foi crescendo até representar, em 2019, um mercado de 366 mil milhões de dólares, dos quais 43% são referentes a Televisão e Comunicações, e 27% a sistemas de Navegação. Atualmente, só 25% deste mercado é da responsabilidade direta dos governos mundiais (cerca de 94 mil milhões de dólares).[1]

1 Bryce, The 2019 Global Space Economy at a Glance.

NEW SPACE

O acesso ao Espaço evoluiu, assim, de um contexto em que estava ao alcance apenas de poucos países e grandes organizações, para um em que está acessível não apenas a pequenos países como a um grupo cada vez maior de empresas.

Este processo está associado a um novo paradigma que emergiu em anos recentes e é comummente chamado *New Space*, embora seja também referido, em especial no contexto da Agência Espacial Europeia, como *Space 4.0*.

Este paradigma, segundo o qual o Espaço surge como um facilitador (*enabler*) de conhecimento, postos de trabalho e conhecimento, está associado à dimensão crescentemente comercial do Espaço e à democratização das atividades espaciais, tendo sido induzido pela coalescência de dinâmicas tecnológicas (technology push) e de mercado (market pull).

De facto, o desenvolvimento tecnológico das últimas décadas permitiu a simplificação e miniaturização de componentes e subsistemas, com a redução de custos no seu desenvolvimento, produção e operação.

Em paralelo, a proliferação de aplicações de base espacial (baseadas em navegação, comunicações e observação da Terra), tanto institucionais como comerciais, tem vindo a atrair cada vez mais investidores privados, como demonstram os 166 mil milhões de dólares investidos em equity no Espaço desde 2009.[2]

Como resultado, há um número cada vez maior de satélites em desenvolvimento para serem operados em constelações, e de microlançadores para colocarem pequenos satélites em órbita.

2 Space Capital, Space Investment Quarterly Q3 2020.

IMPLICAÇÕES PARA A SEGURANÇA

Desde o início, a exploração espacial está associada a questões de soberania e, não obstante os tratados internacionais apontarem para a livre exploração do Espaço para fins pacíficos e estabelecerem que o Espaço e os corpos celestiais não estão sujeitos a soberanias nacionais, são conhecidas as corridas à Lua, a Marte, a asteróides e a outros corpos celestiais.

O Espaço é, de forma incontornável, o palco de decisões geoestratégicas, ou neste caso geo-espacio-estratégicas3, das nações. Exemplos disso são a criação da Space Force pelos Estados Unidos e a sua mais recente edição da National Space Policy que refere o domínio espacial como um cenário de guerra[4]; ou a colocação de uma bandeira chinesa já em dezembro de 2020 na Lua, a partir do veículo lunar Chang'e 5 Lander.

Neste contexto, os desafios da emergência do New Space para a Segurança são vários e devem ser geridos sem que seja limitado o potencial inovador deste novo paradigma e nem os consequentes benefícios socioeconómicos que dele podem advir. Destacamos, de seguida, dois destes desafios.

Os sistemas espaciais, em particular os relacionados com o acesso ao Espaço, Observação da Terra e Comunicações, são eminentemente de duplo-uso e estão hoje ao alcance de um conjunto cada vez mais alargado de organizações, na sua maioria privadas e sem ligação direta a governos.

Também os satélites em particular, independentemente do local onde são lançados, podem monitorizar praticamente todos os locais da Terra. A proliferação de pequenos satélites que podem ser equipados com câmaras de alta-resolução coloca desafios adicionais à proteção de áreas sensíveis e comunicações, entre outros.

No entanto, as oportunidades para o domínio da Segurança são várias e sobrepõem-se aos riscos.

3 O termo geospace designa a combinação das camadas superiores da atmosfera e do Espaço próximo, de acordo com o Dicionário Merriam-Webster.

4 No original: "T*he United States seeks a secure, stable, and accessible space domain, which has become a warfighting domain as a result of competitors seeking to challenge United States and allied interests in space*.", National Space Policy of the United States of America.

O aumento substancial do número de satélites esperado para os próximos anos representa um incremento, em quantidade, qualidade e cobertura geográfica, de fontes de dados e informação que acrescentam eficácia à análise situacional.

Também a transição de missões baseadas num único satélite para missões baseadas em constelações (multi-satélites) traz resiliência aos ativos espaciais. Os satélites deixam de ser potenciais pontos únicos de falha (*single point of failure*) e o desempenho, risco e a obsolescência passam a ser geridos ao nível da constelação, e não do satélite. Também do ponto de vista operacional, se é relativamente fácil detetar, e até neutralizar, satélites geoestacionários, que têm órbitas predeterminadas, é significativamente mais difícil, se não impossível, fazê-lo a redes baseadas em dezenas ou centenas de pequenos satélites distribuídos em órbitas baixas.

Finalmente, a crescente pressão comercial do setor do Espaço leva a que a robustez que caracteriza o setor tenha de ser compatibilizada com taxas de inovação significativamente superiores às atuais, levando ao aparecimento de novos sistemas e capacidades mais rapidamente do que até aqui.

IMPLICAÇÕES PARA AS BASES TECNOLÓGICAS E INDUSTRIAIS

As afinidades entre o Espaço e a Defesa vão bastante para além da sua génese e das aplicações espaciais (comunicações ou imagens de satélite, por exemplo) para fins militares. Têm semelhanças enquanto mercados e setores industriais que importa relevar.

Enquanto mercados, tanto o Espaço como a Defesa requerem sistemas com um elevado nível de robustez e confiabilidade. Falhas no seu funcionamento podem ter consequências graves.

Num sistema espacial, uma falha pode implicar a perda de uma missão de centenas ou milhares de milhões de euros e atrasos substanciais nas operações. Por exemplo, em 2019, a falha num dos giroscópios do satélite de observação ótico WorldView-4 do grupo Maxar, a principal referência

norte-americana em Observação da Terra, levou a uma perda registada próxima dos 200 milhões de dólares. No mesmo ano, a perda do satélite de comunicações Intelsat-29e (que se pode ter devido a um curto circuito), para além de originar uma perda de 50 milhões de dólares nas receitas anuais, levou ao registo de 400 milhões de dólares em perdas nas contas da Intelsat.

Num sistema de Defesa, uma falha pode ter implicações que vão muito para além dos prejuízos económicos ou operacionais, com importantes consequências geoestratégicas, potencialmente associadas à perda de vidas humanas e a ameaças à Segurança.

Enquanto setores industriais, são ambos setores integradores de alta-tecnologia, motores de inovação e pioneiros no desenvolvimento de tecnologia que depois é migrada para outros setores.

Os exemplos são conhecidos mas é interessante lembrar que, da exploração espacial vieram, por exemplo, novos materiais para membros artificiais, proteção contra fogo, absorção de vibrações em edifícios, e lentes resistentes aos riscos; mas também tecnologia para TAC e Ressonâncias magnéticas; Purificadores de água e de ar, ou os auscultadores sem fios. Ou que da Defesa para o quotidiano vieram, por exemplo, o GPS, a supercola e a fita adesiva, ou o forno de micro-ondas.

As afinidades descritas estabelecem pontos comuns entre a cultura industrial do Espaço e da Defesa que constituem uma base para explorar as sinergias entre ambos.

A indústria do Espaço fornece serviços e produtos de elevada complexidade tecnológica, desenvolvidos no contexto de sistemas de qualidade exigentes e cujo desempenho é avaliado de forma exaustiva pelos clientes e entidades financiadoras. As empresas de Espaço fazem, por isso, inerentemente parte da Base tecnológica e industrial para a Defesa. «Para» e não «da» Defesa no sentido em que, não sendo na sua grande maioria credenciadas para fornecer o mercado da Defesa, têm capacidades que podem ser exploradas para benefício das operações de Defesa e Segurança.

Por outro lado, a Defesa é também um importante mercado para as empresas do Espaço. Um sistema espacial é, por regra, significativamente mais caro do que sistemas tecnologicamente semelhantes para outros mercados (como o automóvel por exemplo), por causa dos requisitos de robustez e qualidade que são impostos a estes sistemas para operar no Espaço, e que não são necessários para um carro ou um sistema de geração de energia. A Defesa é dos poucos setores em que este acréscimo de qualidade e robustez é valorizado.

Esta é, atualmente, uma tendência que se verifica em Portugal e fora: encontrar mercados complementares ao do Espaço que permitam continuar o desenvolvimento da indústria Espacial sem onerar mais os orçamentos públicos para o setor, contribuindo para aumentar a resiliência da indústria a evoluções nos ciclos de financiamento.

PORTUGAL NO CONTEXTO DO *NEW SPACE*

Quando se completam 20 anos da adesão de Portugal à Agência Espacial Europeia, continua a ser impressionante a evolução que se operou na indústria e nos centros de investigação nacionais durante este período.

Do fornecimento de pequenos serviços, a indústria foi complexificando e integrando a sua oferta para ser reconhecida internacionalmente em determinados subsistemas e, hoje, ter em curso dinâmicas de consolidação para ganhar escala e criar capacidade de integração de sistemas completos em Portugal, esforço a que não é alheia a Defesa nacional.

Em paralelo, a estratégia nacional para o Espaço, vertida em vários documentos e comunicações, aponta claramente para a aposta em grandes desafios programáticos (Constelação Atlântica, Planeta Digital, 5G, Ecossistema de inovação espacial nos Açores)[5] que beneficiam desta dinâmica de capacitação nacional e permitirão estabelecer em Portugal lideranças globais nestas áreas beneficiando todos os *stakeholders* locais e europeus.

5 Portugal Space, Workshop Space Systems and Innovation: Portugal and Europe 2020-2030.

CIBERDEFESA EM PORTUGAL

HENRIQUE GOUVEIA E MELO
Vice-almirante
Adjunto para o Planeamento e Coordenação do Estado-Maior-General das Forças Armadas

RESUMO HISTÓRICO

Começo este artigo fazendo um breve resumo da evolução da Ciberdefesa em Portugal.

O primeiro grande choque que fez acordar o mundo ocidental para a consciencialização da necessidade de criar mecanismos de defesa no ciberespaço foi o ataque ciber da Rússia à Estónia, em abril de 2007. No conflito da Geórgia, em 2008, a Rússia fez um ataque massivo através do ciberespaço contra as redes e infraestruturas da Geórgia, enquanto conduzia em simultâneo um ataque militar cinético ao território desse país.

Em 2013 a União Europeia (UE) individualiza, pela primeira vez, o conceito de Ciberdefesa, na sua Estratégia de Cibersegurança o mesmo acontecendo na Organização do Tratado do Atlântico Norte (NATO), com o Secretário Geral a lançar o repto de reforçar a capacidade da Aliança no ciberespaço. Nesse mesmo ano, a nível nacional, o Conceito Estratégico de Defesa

Nacional[1] destaca a segurança do ciberespaço como uma prioridade e recomenda a edificação de uma capacidade de Ciberdefesa ao nível das Forças Armadas.

No ano seguinte, em 2014, o Centro de Ciberdefesa é criado, enquanto estrutura conjunta, na dependência do Chefe do Estado-Maior General da Forças Armadas (CEMGFA)[2].

A NATO assumiu, em 2014, na Cimeira de Gales, que a Ciberdefesa faria parte dos objetivos de defesa coletiva da Aliança e que se aplicaria ao ciberespaço o Direito Internacional. Resultou dessa cimeira um compromisso de os Aliados desenvolverem a capacidade de Ciberdefesa no âmbito da defesa coletiva.

Em 2016, na Cimeira de Varsóvia, o ciberespaço foi assumido pela Aliança como o 4.º domínio das operações militares, em acréscimo aos ambientes terrestre, naval e aéreo.

Em 2019, a Lei de Programação Militar (LPM)[3] veio reforçar o investimento na edificação da capacidade de Ciberdefesa, no âmbito da modernização das Forças Armadas.

No mesmo ano, a Estratégia Nacional de Segurança do Ciberespaço[4] estrutura as competências dos organismos com responsabilidades na segurança deste espaço e atribui a exclusividade das ações ofensivas, nesse âmbito, às Forças Armadas.

Em 2020 a UE apresenta a Estratégia de Cibersegurança para o espaço europeu, que compreende três vetores essenciais: resiliência, liderança e soberania tecnológica; capacidade operacional para prevenir, dissuadir e responder; cooperar para promover um ciberespaço aberto e global.

1 Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril.

2 Lei Orgânica do Estado-Maior-General das Forças Armadas, aprovada pelo decreto-lei n.º 184/2014, de 29 de dezembro.

3 Lei Orgânica n.º 2/2019, de 17 de junho.

4 Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho.

Realizada esta breve introdução histórica importa caraterizar o ciberespaço enquanto domínio de condução de operações de forma a apresentar uma visão para o desenvolvimento da Ciberdefesa.

O CIBERESPAÇO ENQUANTO DOMÍNIO DAS OPERAÇÕES

O ciberespaço[5] é uma entidade materializada numa rede global, híper conectada, de computadores, comunicações, roteadores e aplicações, onde são transmitidos e armazenados dados que resultam da interação, a uma escala mundial, de seres humanos e entidades.

Esta rede tem uma natureza supranacional e é verdadeiramente desprovida de um sistema de governação central. No entanto, muitos governos impõem regras e restrições ao uso desregulado/livre da rede, por parte dos seus cidadãos.

Essas restrições podem ter por base, na forma mais benigna, princípios democráticos consagrados no direito internacional, e na mais austera, práticas comuns aos regimes autocráticos, impostas através do controlo das infraestruturas físicas e da interceção, roteamento e análise de tráfego que aí circula.

Apesar das restrições, o ciberespaço constitui-se, na utilização partilhada e interligada à escala global, como um espaço comum da humanidade[6].

Comparativamente a outros espaços comuns da humanidade - mar; ar; e espaço -; o ciberespaço é, numa perspetiva internacional, fortemente desregulado, para além dos padrões tecnológicos que permitem a sua interconexão. É também, um espaço não natural, criado pelo ser humano em resultado do progresso tecnológico.

5 Internet, WWW.

6 Na descrição interessante que o professor Barry R. Posen faz, na sua análise da fundação da hegemonia militar dos Estados Unidos da América, na revista International Security, no verão de 2003.

Apesar das diferenças evidenciadas, não deixa de ser um espaço comum da humanidade, com elevado valor económico, social e político, constituindo-se como um domínio de estratégias de confrontação, competição e cooperação.

Estas estratégias, nomeadamente as de confrontação, quando operadas numa lógica westefaliana, transformam o ciberespaço num domínio de operações militares[7].

O ciberespaço tem, contudo, quando comparado com os espaços naturais, caraterísticas muito diferenciadas que o tornam um domínio de operações muito singular:

- enquanto espaço híper conectado a uma escala global, onde a transmissão de dados se faz praticamente à velocidade da luz, é adimensional, sem fronteiras, distâncias, frente ou retaguarda;

- a sua natureza adimensional, materializada num emaranhado de híper ligações, servidores, aplicações e roteamentos, dificultam, senão quase que impossibilitam, fazer a localização da origem de uma atividade hostil;

- os protocolos de rede, que constituem a espinha dorsal da sua conetividade, estabelecidos na origem da Internet[8], continuam a privilegiar a conetividade/resiliência à segurança, tornando-o intrinsecamente inseguro.

O ciberespaço, enquanto domínio das operações, contem, claramente, três subdomínios de atuação: infraestrutural, informacional e comportamental, relacionados com a tecnologia, os dados e as crenças intrínsecas dos utilizadores, respetivamente.

7 Usarei no texto a designação mais simples de - domínio operacional - , mas no sentido de um domínio onde podem ocorrer operações militares, quer sejam estas de nível estratégico, operacional, ou tático.

8 O Ciberespaço tem origem num conjunto de protocolos de transmissão e roteamento de tráfego, que nasceu numa rede militar dos EUA a ARPANET na década de 1960.

Os fenómenos de confrontação, competição e cooperação podem ter uma evidência num, ou mais, dos subdomínios operacionais da rede. Por exemplo: a atividade *hacker* está centrada nos subdomínios infraestrutural e informacional, enquanto as atividades de desinformação se concentram no domínio informacional e comportamental.

Em 2013, o General Gerasimov[9], então Chefe do Estado-Maior General Russo, publicou o artigo[10] "O valor da ciência na previsão", onde carateriza e sistematiza uma forma de confrontação entre Estados, abaixo do nível de conflito declarado, onde todas as formas de poder (militar, económico, cultural, tecnológico e diplomático) e todos os tipos de atores, internos e externos, são considerados. A esta doutrina deu-se a designação de guerra híbrida. Na história recente, como demonstram a campanha ciber contra a Estónia em 2007, a guerra híbrida contra a Geórgia em 2008, a anexação da Crimeia em 2014 e mais recentemente, os ataques ciber contra as redes departamentais dos EUA, o conceito está vivo, é exercitado e juntou outros atores internacionais provando que o ciberespaço é uma zona de conflito.

A guerra híbrida, como concebida e praticada, recorre em simultâneo: à movimentação de forças militares – com o propósito de intimidar, dissuadir, ou inibir reações; a confrontos limitados – usando forças regulares, irregulares e/ou grupos de criminosos; à disseminação de campanhas de desinformação - dirigidas à parte emocional e cognitiva das populações-alvo; a múltiplas atividades no ciberespaço; ao uso de uma diplomacia agressiva e decetiva; e à pressão económica. Outros conceitos como o da "Guerra Irrestrita", escrito pelos Coronéis Qiao Liang e Wang Xiangsui[11], práticas igualmente preocupantes de Estados do Médio Oriente e até de potências ocidentais, assim como a utilização do ciberespaço por grupos terroristas, anarquistas e de outros grupos extremistas contra o Estado de Direito, não podem deixar tranquilos os decisores políticos e militares.

Estas doutrinas e práticas, de natureza assimétrica, encontram no ciberespaço um domínio natural de operações. Recolher e manipular dados,

9 Chefe do Estado-Maior General das Forças Armadas da Rússia.

10 Valery Gerasimov, "Tsennost nauki v predvidenii", Voenno-promyshlenniy kurer (27 fevereiro 2013).

11 Pertencentes ao Exército Popular da China. Acedido em janeiro de 2021 em: https//www.c4i.org/unrestricted.pdf

penetrar sistemas, colocá-los reféns, ou negar o acesso destes à rede, por via de ações no e através do ciberespaço, mantendo a dúvida razoável da atribuição do ataque, passou a ser um padrão demasiado comum nos tempos modernos.

Deste modo e em resumo, o ciberespaço é um espaço de confronto diário, com Estados, grupos anárquicos e extremistas que o usam de forma agressiva, prejudicando outros, que estarão mais ou menos vulneráveis, na proporção das suas capacidades para se defenderem e reagirem.

O QUE DEVE SER A CIBERDEFESA

A Ciberdefesa é uma capacidade militar, de acordo com a legislação nacional, definida pela Estratégia Nacional para a Segurança do Ciberespaço, em 2019.

Mas porquê uma capacidade militar? Porque neste espaço comum da humanidade, o nível de competição e confrontação entre Estados e entidades supranacionais assume as mesmas caraterísticas que nos outros domínios, o mar, o ar e o espaço, onde foram edificadas capacidades militares para a defesa dos interesses dos Estados e coligações. Poderá parecer que se optou simplesmente por uma solução mimetista, transversal aos outros domínios de operações, ou simétrica relativamente a capacidades criadas por outros Estados, mas há uma razão mais substantiva para esta opção. A existência da Ciberdefesa, enquanto capacidade militar, reside na necessidade de o Estado dispor de uma ferramenta de natureza ofensiva, num espaço partilhado, alvo de estratégias de confrontação e competição, exercendo dessa forma, um efeito dissuasor importante e se necessário uma capacidade de resposta a agressões externas. O *modus operandi* é por isso distinto do policial e excede o puramente defensivo.

A importância do Ciberespaço e do livre acesso a este, num mundo cada vez mais globalizado e digital, nos aspetos económicos, científicos e culturais, tornou-se verdadeiramente crucial.

Decorre dessa constatação que a missão principal da Ciberdefesa deverá

ser assegurar o direito soberano de Portugal de aceder e utilizar de forma livre e segura o ciberespaço, em igualdade de circunstâncias com os outros Estados, promovendo a defesa dos seus legítimos interesses, o desenvolvimento e progresso nacional.

No entanto, a Ciberdefesa não deve resumir-se apenas a uma capacidade ofensiva, deve também providenciar a proteção necessária às redes da Defesa, das Forças Armadas e de outras consideradas críticas para a soberania nacional.

Uma defesa coletiva e coordenada das redes da Defesa, interconectadas entre si, faz todo o sentido. O conjunto passa a ser uma nova rede, cuja vulnerabilidade é o elo mais fraco desta, o que exige padrões de defesa e resiliência comuns, estabelecidos por uma direção centralizada, com a capacidade para realizar a monitorização do perímetro defensivo, enquanto um todo e não uma soma das partes. Concomitantemente, a capacidade ofensiva, face às implicações do seu uso, deve ser exercida sob forte escrutínio político e estar ancorada no nível estratégico da Defesa. Compreende-se assim, mais facilmente, que a decisão do legislador tenha sido a de federar, sob a direção central do Estado-Maior General das Forças Armadas, a Ciberdefesa, garantindo simultaneamente uma defesa conjunta e uma capacidade ofensiva na dependência direta do nível estratégico. Este arranjo organizacional não impede que os ramos sejam responsáveis pelas suas redes e respetiva administração, participando na defesa coletiva das redes da Defesa. As Forças, em ação, devem operar sob uma perspetiva de nível tático no âmbito da guerra eletrónica, lato senso, o que inclui o conceito anglo-saxónico de *Network Warfare*. As limitações deste tipo de ações são a geografia de atuação, os tempos e efeitos imediatos pretendidos, sem a dimensão do envolvimento global de um Estado contra outro Estado, mas sim de uma Força contra outra Força. No caso das Forças atuarem no nível operacional-estratégico, devem-no fazer sob a coordenação centralizada da Ciberdefesa, mais uma vez pelas implicações que esse tipo de ações poderão ter nos equilíbrios do ciberespaço e da relação entre Estados, incluindo terceiros.

Importa também conceptualizar o que se entende por ações ofensivas. No âmbito das ações ofensivas poderemos enquadrar as ações reativas (defesa

ativa), exploratórias, preventivas e deliberadas. Os alvos deverão ser entidades/atores sediados no, ou dirigidos do, exterior do território nacional (TN), que possam colocar em perigo a segurança, a soberania, a ordem constitucional, os valores e os interesses nacionais e ou de coligações a que Portugal pertença. Esta capacidade poderá também ser usada como multiplicador de operações militares no âmbito nacional e ou das coligações e alianças do país. A capacidade ofensiva deverá integrar operações de informação e psicológicas no Ciberespaço (redes sociais), em ambiente de conflito declarado, ou híbrido.

COMO DESENVOLVER A CIBERDEFESA

A edificação de uma capacidade, como a Ciberdefesa requer, necessariamente, a adequada articulação de recursos humanos, materiais e financeiros, materializados numa organização enformada por princípios doutrinários com um propósito bem estabelecido.

Recursos humanos qualificados e em quantidade suficiente para se alcançar a nível de ambição definido são essenciais à edificação de qualquer capacidade, mas na Ciberdefesa, uma área de conhecimento fortemente especializado, eles serão críticos. No entanto, a disponibilidade de recursos humanos qualificados constitui-se como uma séria dificuldade, face à atual escassez desses recursos no mercado de trabalho. Sendo escassos no mercado de trabalho e fortemente especializados, as Forças Armadas têm encontrado sérias dificuldades em recrutá-los e retê-los. A Ciberdefesa, não podendo competir em remuneração com o mercado de trabalho, deverá promover como diferenciadora a formação, fortemente especializada, num modelo prático e pragmático, vocacionado para uma população com o ingresso ao nível do ensino secundário. Deverá também promover a diferenciação pela experiência e contexto de trabalho únicos e aliciantes, assim como pelo prestígio resultante de se ter passado pelas fileiras deste Centro. A Ciberdefesa deve constituir-se para os militares e civis que por aí passarem, como um bilhete de acesso a um leque de oportunidades alargado, associado a uma subida significativa de estatuto remuneratório, no retorno à vida civil. Para que este mecanismo de funcionamento não contribua para a rarefação dos quadros da Ciberdefesa, a formação e a experiência deverão ser ajus-

tadas de forma progressiva, permitindo um equilíbrio entre o investimento e o retorno, incentivando a permanência por períodos superiores a seis anos de atividade. O recrutamento necessita também de uma aproximação disruptiva, privilegiando a seleção psicológica adequada em detrimento de uma excessiva preocupação com qualificações nas áreas tecnológicas de interesse.

A observação atenta do ciberespaço revela que as atividades disruptivas e ilícitas são perpetradas por um "inimigo", maioritariamente constituído por jovens sem formação superior, mas muito capazes tecnologicamente, correspondendo a um perfil psicológico de certa forma delimitado. Sem menosprezar a importância da formação académica, o que a realidade nos parece indicar é que a formação estruturada, exaustiva, mas em contrapartida lenta, pode não ser o caminho ideal na preparação dos futuros ciberguerreiros. Esta deve ser mais interativa, lúdica, focada no essencial, desafiante e vocacionada para objetivos específicos, sequenciais e progressivos. O desenho do modelo de prestação de serviços e carreiras deverá basear-se na premissa da retenção temporária suficiente. Isto é, deixar fluir naturalmente para o mercado de trabalho, após um prazo razoável, uma parte significativa dos seus recursos. Este processo servirá como incentivo ao recrutamento, contribuindo para assegurar uma capacidade nacional mais alargada, estabelecendo uma rede de contactos importante, que poderá reforçar a capacidade militar - num eventual cenário de um ataque em larga escala no Ciberespaço. Ainda neste contexto, as Forças Armadas terão a possibilidade de explorar a reconversão de muitos dos seus quadros, nomeadamente as praças, para o desempenho de funções no âmbito da Ciberdefesa e da administração de redes.

A importância de ter nas fileiras ciberguerreiros tecnologicamente capazes será crítica para o sucesso. Deste modo, analisando outras potências e países da dimensão de Portugal, considero que a componente humana desta capacidade deve ter mais de duas centenas de elementos. Só assim terá uma capacidade H24/7, multidisciplinar, capaz de sustentar durante meses uma campanha defensiva e ofensiva, contra um opositor suficientemente capaz. Estes ciberguerreiros deverão ter acesso à melhor tecnologia disponível sendo suportados por uma estrutura de retaguarda de treino, informações e investigação, também ela robusta.

É assim crucial que a Defesa, ao nível das Forças Armadas, edifique uma Escola de formação, prática, conjunta, para a Ciberdefesa e para a administração de redes, na sua total dependência, em razão da criticidade para o sucesso de um tal instrumento. A importância de uma Escola de Ciberdefesa no âmbito das Forças Armadas, com capacidade para formar recursos humanos em quantidade e qualidade, parece-me ser um dos instrumentos cruciais de uma política que garanta a necessária autonomia e capacitação.

Essa escola não só permitiria criar uma base alargada de ciberguerreiros assim como proporcionaria a todos os outros militares que ingressassem nas fileiras, uma espécie de instrução militar básica digital, uma capacidade diferenciadora e revolucionária da qualidade e adaptabilidade do corpo militar, tornando-o apto a operar num mundo cada vez mais digital e interconectado. As escolas militares foram pioneiras no desenvolvimento de escolas práticas e tecnológicas de sucesso no passado, como a dos eletricistas, mecânicos, rádio operadores, radaristas e muitas outras especialidades técnicas, antes do "tempo". Devemos seguir o mesmo caminho na Ciberdefesa - formando e capacitando os nossos ciberguerreiros numa escola de âmbito prático, tecnológico, com um modelo disruptivo de ensino, captação e desenvolvimento de talentos.

Os recursos materiais, incluindo os tecnológicos (servidores, roteadores, software) podem ser facilmente adquiridos, havendo recursos financeiros disponíveis. Na conjuntura atual, os recursos financeiros e materiais não parecem ser uma limitação tendo em consideração o financiamento disponibilizado em sede de LPM.

No entanto, importa investir de forma equilibrada nos dois pratos da balança - recursos materiais e humanos - pois haverá uma tendência para investir nos recursos materiais mais rapidamente do que organizar e capacitar os recursos humanos.

Nos recursos materiais, a excessiva dependência de soluções prontas, comerciais e retiradas das "prateleiras" é um problema que deve ser tratado devidamente. A Ciberdefesa deve assentar em tecnologia aberta, na máxima extensão possível, porque está livre de código não controlado e propositadamente colocado pelos fornecedores e porque dessa forma

contribui também para a soberania tecnológica e digital. A utilização e a adaptação de plataformas abertas serão uma prova da capacidade e da maturidade dos recursos humanos da Ciberdefesa do futuro. Só esse caminho permitirá a independência e a soberania digital possível.

Por fim, importa referir que a capacitação da Ciberdefesa e a operação desta no ciberespaço será extraordinariamente alavancada pela cooperação nacional com outras entidades com responsabilidades na segurança do ciberespaço, assim como com as parcerias internacionais que possam resultar das alianças militares no seio NATO, UE, PALOPs, ou outros acordos multilaterais e bilaterais. A participação em rede numa coligação alargada permite uma maior superfície de deteção, uma troca de informação mais rica, uma resposta mais robusta e o desenvolvimento do conhecimento de forma partilhada, necessariamente num processo mais eficaz e eficiente.

Neste artigo não se desenvolveu propositadamente os aspetos operativos da Ciberdefesa, porque se considera que essa matéria deve ter a reserva adequada e não deve ser exposta de forma a contribuir para o reconhecimento avançado de um eventual opositor.

5G
UM DESÍGNIO NACIONAL

JOÃO GONÇALVES PEREIRA
Deputado à Assembleia da República
Grupo Parlamentar do CDS - PP

Uma recente sondagem sobre o 5G revelou que 68% dos portugueses não sabem o que é – ou para que serve – a quinta geração de rede móvel de comunicações. Esta realidade é manifestamente preocupante, na medida em que o 5G é seguramente um dos temas mais relevantes para o país na próxima década.

Enquanto deputado à Assembleia da República provoquei a discussão do 5G em duas vertentes: primeiro com uma proposta para a realização de uma conferência sobre o 5G, que será realizada no Parlamento em janeiro de 2021; e depois, com a apresentação de um Projeto de Resolução a recomendar construtivamente ao Governo e à ANACOM um conjunto de benfeitorias ao regulamento de leilão do 5G.

Nesta fase, em que não existe ainda verdadeira consciência do potencial máximo do 5G, podemos afirmar que sabemos uma coisa: a verdadeira revolução digital será nas empresas, na indústria e, necessariamente, nas nossas cidades. De facto, numa primeira fase, o cidadão comum sentirá apenas uma maior velocidade no seu telemóvel ou *tablet* porque serão as transformações na indústria e nos seus produtos que concretizarão verda-

deiramente as alterações nas nossas vidas.

Ora, importa olhar para trás e verificar a evolução das redes móveis: no início dos anos 80, a tecnologia analógica do 1G (comunicação por voz); dez anos depois, em 1992, o 2G e a passagem à tecnologia digital (SMS e MMS); em 2002, a banda larga móvel 3G com a internet e o e-mail disponíveis nos *smartphones*; e, mais recentemente, em 2012, o 4G traz a rede móvel mais rápida, mais fiável e com maior volume de dados, o que permite que hoje possamos fazer videochamadas, organizar videoconferências, ver séries ou ouvir música nos nossos telemóveis.

Espera-se que o 5G dê origem a um novo ecossistema digital que ligará pessoas, cidades e coisas. Na realidade, o 5G trará velocidades de acesso a par com as fibra ótica (10Gbps), com elevadas taxas de resposta (<1ms), elevada fiabilidade (>99,999% disponibilidade) e milhões de objetos ligados (1 milhão de objetos por quilómetro quadrado) permitindo novas tecnologias como os *streamings* de vídeo a 360 graus em direto, a realidade aumentada ou a condução autónoma nos automóveis.

As expetativas em relação 5G são muitas e todos pretendem ter um papel relevante a desempenhar, principalmente todos aqueles que têm um elevado espírito empreendedor e que já perceberam que o 5G vai potenciar a criação de novas empresas, de novos negócios e de novas profissões.

Para as empresas, a redução na latência permitirá o controlo de máquinas de precisão a grandes distâncias ou a digitalização completa das fábricas, e haverá seguramente um desbloquear de inúmeras tecnologias ainda a surgir.

Todos os grandes construtores de automóveis, sem exceção, estão a fazer a transição de um mundo físico para o digital. As fábricas estão a modernizar-se e a construção de um automóvel passará a ser feita num único local, onde de forma eficiente estão todos os componentes da viatura, reduzindo assim os tempos de construção.

A indústria automóvel é aquela onde é mais percetível perceber os impactos do 5G. Conceitos como carros autónomos ou carros conectados vão ser uma realidade nas nossas vidas dentro de muito pouco tempo. Todos

iremos assistir a uma redefinição do modelo de negócio dos automóveis, passando, essencialmente, por deixarmos de encarar o automóvel como um objeto para passar a encará-lo como um serviço. Iremos também assistir – e dentro de muito poucos anos – a veículos que conversarão uns com os outros, em troca de informação, o que permitirá uma melhor gestão do tráfego e das infraestruturas. Atenção, isto não é uma possibilidade, será mesmo em breve a nossa realidade.

Atualmente, já podemos afirmar que o 5G também trará benefícios para áreas como a medicina (permitindo, por exemplo, as cirurgias remotas); na segurança pública; na educação; na ciência; na mobilidade e transportes; nos portos e, claro, também no domínio ambiental.

Por exemplo, no caso da segurança pública um fator chave no sucesso de operações de controlo e resposta a emergências é o uso da informação, segura e fiável, e a facilidade de tomada de decisão. O 5G no caso da Proteção Civil tornará possíveis casos de uso como a monitorização em tempo real de bombeiros na luta contra as chamas, medindo o estado do seu equipamento de proteção e enviando esses dados para um centro de controlo capaz de monitorizar níveis de deterioração, sinais vitais, alocação de recursos, risco e prioridades. Permitirá ainda que drones lhes dêem perspetiva da configuração e evolução de um incêndio para o combater mais eficazmente.

Irá também permitir que profissionais médicos sejam capazes de remotamente diagnosticar e acompanhar pacientes com assistência especializada, ou ainda o fornecimento de materiais, medicamentos e equipamentos através de drones; e os agentes públicos, como polícias, bombeiros, profissionais de saúde e outros, beneficiarão de uma capacidade de comunicação segura e imediata em várias situações de missões críticas, devido à velocidade, baixa latência e alta fiabilidade do 5G.

Um dos temas mais sensíveis – e que seguramente as forças policiais e de investigação estão já a prever – é o impacto que a nova tecnologia 5G vai trazer para a prática de crimes e até mesmo de novos tipos de crime em ambiente *cybercrime*. Será desafiante projetar aqueles que vão ser os novos instrumentos de investigação através da utilização desta nova rede e desta

nova tecnologia, designadamente através de aplicações de segurança sem fios para monitorização e detecção.

Muitos telemóveis, principalmente os topos de gama das diferentes marcas, já suportam as frequências 5G, mas a esmagadora maioria dos portugueses ainda não têm equipamentos que consigam trabalhar nessa frequência. Por isso, iremos assistir a um processo que será idêntico ao que aconteceu com o 4G: a massificação gradual do acesso à tecnologia primeiro e, depois, à rede.

Um dos mitos urbanos que tem sido disseminado nas redes sociais, mas que a ANACOM, e bem, já veio clarificar, é que não existe nenhuma evidência científica de que a exposição às ondas do 5G seja prejudicial para a saúde humana. Isto é, o lançamento do 5G não cria riscos "novos", porque as frequências da quinta geração já são usadas por outros serviços há muitos anos. Um bom exemplo disso é a faixa dos 700 MHz, que era usada até agora pela Televisão Digital Terrestre (TDT).

Nos países que já têm rede 5G disponível, os primeiros utilizadores apontam alguns problemas com os telemóveis 5G no geral: a bateria esgota-se rapidamente, os aparelhos tendem a aquecer e a cobertura de rede é fraca. Ou seja, o 5G tem desafios ao nível da cobertura de rede, mas também tem um caminho a fazer no desenvolvimento de melhores equipamentos móveis.

Nesta primeira fase de implementação da rede 5G, o utilizador comum de telemóvel não sentirá enormes diferenças entre o 4G e o 5G, por isso estou certo que muitos portugueses vão optar por continuar a usar o seu equipamento atual, mesmo depois de lançado o 5G em Portugal.

No mais, ainda não há certezas sobre que regiões do país terão 5G numa primeira fase. Mas Lisboa e Porto vão estar certamente no radar dos investimentos das operadoras. Há operadoras que já fizeram testes 5G na capital e tudo indica que tenham as antenas já montadas, somente à espera da licença para poderem começar a irradiar. Neste âmbito, e para cumprir as obrigações de cobertura que decorrem do leilão, cada um dos operadores existentes terá de fazer um investimento em infraestruturas

superior a 300 milhões de euros.

Em que fase estamos, então, no processo de 5G em Portugal? O calendário antes da pandemia já estava ligeiramente atrasado, face a outros países, mas com a pandemia tudo acabou por ser adiado, tendo há umas semanas sido anunciado pela ANACOM – Autoridade Nacional de Comunicações – o regulamento de leilão do 5G.

O leilão é um processo através do qual as operadoras interessadas em lançar redes 5G em Portugal compram à ANACOM as licenças para usarem as frequências. Estas licenças são válidas por 20 anos, mas podem ser renovadas.

A expectativa era de que a atribuição de licenças 5G decorresse no primeiro trimestre de 2021, mas o desentendimento acentuado entre o regulador e os operadores de telecomunicações – que já levou a processos em tribunal, queixas em Bruxelas e a providências cautelares – podem comprometer seriamente este calendário.

Na Europa, os leilões de 5G já foram concluídos em 17 países, entre os quais na nossa vizinha Espanha, e cada mês que passa sem termos uma definição segura do calendário do 5G em Portugal torna-nos menos competitivos face a outras geografias, mesmo dentro do espaço europeu, e coloca as nossas empresas e indústria fora da disrupção tecnológica que está a acontecer um pouco por todo o mundo civilizado e desenvolvido.

Tenho a esperança de que as autoridades nacionais e os operadores de mercado possam ultrapassar as divergências presentes e que se consiga alcançar uma plataforma de entendimento para que Portugal possa sair a ganhar e não desperdice esta oportunidade.

Segundo um estudo recente da Roland Berger projeta-se que até 2035, em Portugal, o 5G crie um impacto de 17 mil milhões de euros na economia nacional e que potencie a criação de quase 20.000 postos de trabalho em diferentes sectores, o que apresenta o 5G como um desígnio nacional evidente.

Após a leitura de vários *papers* dedicados ao 5G, é possível concluir, à data de hoje, que pouco se pode avançar sobre o que será o verdadeiro potencial desta transição tecnológica. Muitos preveem que só após um período de 6 a 7 anos de maturação do 5G vai poder verificar-se a sua verdadeira dimensão nos diferentes domínios sociais, económico e ambientais.

Em suma, o desenvolvimento do 5G será crítico para a competitividade do país ao longo da próxima década. E é por isso que entendo ser este um desígnio nacional que deve mobilizar todos os portugueses.

COMBATE AO TERRORISMO NO MAR:

ARTICULAÇÃO ENTRE FORÇAS ARMADAS E FORÇAS E SERVIÇOS DE SEGURANÇA

JORGE PEREIRA LOURENÇO

Capitão-de-mar-e-guerra FZ Ref.

SME and Instructor NATO Special Operations School

Leidos: NATO Special Operations Education, Training, Exercises and Evaluations Program Management and Organizational Behaviour, MSc

O ano de 2020 no que à segurança diz respeito fica marcado pela assinatura das Orientações para a articulação operacional entre as Forças Armadas (FFAA) e as Forças e Serviços de Segurança (FSS), assinadas em 28 de fevereiro pelo Chefe do Estado-Maior-General das Forças Armadas (CEMGFA) e pela Secretária-Geral do Sistema de Segurança Interna (SGSSI). Estas orientações constituem uma importante base para que uma cooperação que já existe em vários domínios se institucionalize, consolide e se possa alargar, inclusive, no contexto do combate ao terrorismo.

As orientações estão alicerçadas em vários diplomas legais, a Lei de Segurança[1] Interna refere a colaboração das FFAA em matéria de segurança interna, definindo que compete ao SGSSI e ao CEMGFA assegurarem entre si a articulação operacional.

Na mesma linha quer a Lei de Defesa Nacional[2] quer a Lei Orgânica de Ba-

1 Lei nº 53/2008, de 29 de agosto

2 Lei Orgânica nº 1-B/2009 de 7 de julho, republicada pela Lei Orgânica nº 5/2014 de 29 de agosto

ses da Organização das Forças Armadas[3] confirmam que a responsabilidade da implementação de medidas de coordenação, no quadro da cooperação entre as FFAA e as FSS, tendo em vista a o cumprimento conjugado das respectivas missões no combate a agressões ou ameaças transnacionais, é da responsabilidade do SGSSI e do CEMGFA, sem prejuízo das competências de outras entidades previstas em legislação própria, nomeadamente as da Autoridade Marítima Nacional e as da Autoridade Aeronáutica Nacional.

O Conceito Estratégico de Defesa Nacional de 2013[4] refere a necessidade de aprofundar a cooperação entre as FFAA e as FSS em missões no combate a agressões e às ameaças transnacionais, através de um Plano de Articulação Operacional que contemple não só as medidas de coordenação, mas também a vertente de interoperabilidade dos sistemas e equipamentos, promovendo assim uma abordagem integrada da segurança interna, articulando e coordenando capacidades e meios.

No contexto particular da ameaça terrorista, a Estratégia Nacional de Combate ao Terrorismo[5] reafirma o aprofundamento da cooperação entre as FFAA e as FSS em situações de intervenção perante agressões terroristas e, em permanência, através de mecanismos de cooperação, no âmbito da segurança interna, no quadro das competências do SGSSI e do CEMGFA.

As ameaças transnacionais, em que naturalmente se destaca o terrorismo, têm claramente um caracter multidimensional. O terrorismo entrecruza-se com o crime organizado, sendo que este possibilita o financiamento daquele. A evidência das múltiplas vertentes do crime organizado facilita a criação de um ambiente de impunidade favorável ao crescimento de inúmeras formas de criminalidade. O desenvolvimento associado destes fenómenos poderá, no limite, ser facilitador da disrupção da organização social dos estados.

A ponderação holística destas ameaças e riscos, percecionando-os na sua transversalidade e intersecção é bem patente nos documentos estratégicos nacionais, de países amigos e das organizações internacionais de que Por-

3 Lei Orgânica n.º 1-A/2009, republicada pela Lei Orgânica n.º 6/2014 de 1 de setembro

4 Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril

5 Resolução do Conselho de Ministros n. 7-A/2015, de 20 de fevereiro

tugal faz parte, evidenciando que a resposta integrada à ameaça das redes terroristas, não é compatível com compartimentações redutoras, devendo afirmar-se através da articulação de medidas diplomáticas, de controlo financeiro, judiciais, de informação pública e de informações, policiais e militares, destacando-se mormente a responsabilidade de vigilância e controlo das acessibilidades marítima, aérea, terrestre e do ciberespaço.

A Aliança Atlântica identifica no seu conceito militar para a defesa contra o terrorismo[6] medidas operacionais para lidar com a ameaça, agrupando-se em:

- Contraterrorismo (CT) que engloba medidas ofensivas que implicam estratégias ofensivas / ativas para reduzir a vulnerabilidade das forças, pessoas e bens contra ameaças ou actos terroristas, contemplando ações diretas de captura, ou a eliminação física dos terroristas.
- Antiterrorismo (AT) em que se enquadram medidas de carácter preventivo e defensivo para reduzir as hipóteses de um potencial ataque ou reduzir a vulnerabilidade de alvos potenciais, constituindo um esforço a longo-termo sobre as bases de apoio do terrorismo e suas causas, atuando nos ambientes que possam potenciar a ameaça.
- Gestão de consequências (GC) que abrange medidas pró-ativas e reativas, conduzidas com o objectivo de minimizar e mitigar os efeitos destrutivos de um ataque terrorista.

As FFAA e em particular a Marinha têm atuado externamente em particular no contexto do AT em missões internacionais de vigilância e controlo de espaços marítimos que contribuíram, direta ou indiretamente, para o combate ao terrorismo, quer no quadro da Aliança Atlântica, caso das operações Active Endeavour, IFOR Sharp Guard, IFOR Allied Force, Allied Protector e Ocean Shield, quer no âmbito da União Europeia nas operações Frontex e Atalanta

Residem ainda na Marinha meios e capacidades para o cumprimento operacional de ações de CT e de GC.

Especificamente no âmbito do CT salientam-se as capacidades para con-

6 MC 472, 2002 Military concept for defence against terrorism. – September 26, 2002

duzir operações de interdição marítima envolvendo meios de superfície, submarinos, aéreos e o emprego do Destacamento de Ações Especiais.

A proficiência da Marinha em operações de interdição marítima com emprego daqueles meios, tem tido tradução na experiência consolidada de colaboração designadamente com a Polícia Judiciária no que concerne ao combate ao narcotráfico, que tem tido expressão em inúmeras operações de apreensão de estupefacientes no mar. No contexto desta colaboração, que se iniciou há mais de 25 anos, a Marinha tem empenhado diferentes meios e capacidades orgânicos em articulação operacional com as capacidades próprias da Polícia Judiciária na repressão da criminalidade, legitimada inclusive no quadro do direito internacional.

O empenhamento da Marinha no contexto de ações de GC pode enquadrar-se no vasto leque das missões de interesse público, englobando, entre outras, as de salvamento e salvaguarda da vida humana no mar e combate à poluição no mar, em que que este ramo possui uma vastíssima experiência, podendo para o efeito articular-se, ainda, com FSS e estruturas da proteção civil.

As ações terroristas têm surpreendido o mundo pelo inusitado de que se revestem, em que o que inimaginável ou que considerávamos apenas do domínio da ficção pode acontecer. A este propósito, é interessante conhecer ou revisitar uma interessante obra de ficção "A Laranja Maculada – terrorismo no mar português"[7], da autoria do Contra-Almirante João Nobre de Carvalho. Trata-se de uma estória bem pensada e articulada, em que a realidade e a ficção se interligam, descrevendo o autor uma acção de terrorismo marítimo que se desenvolve na costa portuguesa, envolvendo a tomada de reféns a bordo de um petroleiro, pairando ainda o espectro do derrame intencional de muitas toneladas de crude ao longo da costa. O autor descreve ainda a atuação da estrutura de segurança portuguesa na resolução da situação, na qual destaca o papel da Marinha.

Os acontecimentos narrados nesta obra podem ser um excelente pretexto para se refletir acerca da articulação entre FFAA e FSS no âmbito do combate ao terrorismo, tendo como referencial as orientações para a articulação

7 Carvalho, J.N., 2015. *A Laranja Maculada; Terrorismo no Mar Português*, 2ª Ed., Lisboa: Edições Revista de Marinha.

operacional entre aquelas estruturas.

Cremos não haver dúvidas que uma situação como a descrita na "Laranja Maculada" requere em termos de resposta uma intervenção extraordinária e urgente no âmbito da segurança interna, nos termos das orientações para a articulação operacional entre as FFAA e as FSS.

Assim sendo, somos de opinião que a intervenção no mar, assentaria, entre outras, e numa primeira análise nas capacidades articuladas nacional e internacionalmente de vigilância e controlo do tráfego marítimo; no conjunto de protocolos e mecanismos adstritos às informações sobre tripulações, cargas e produtos transportados pelos navios[8], que permitem estabelecer o quadro situacional do incidente, e que assentam em capacidades residentes na Marinha, e também na Força Aérea.

Atendendo a que o incidente se desenvolve no quadro da segurança interna os meios e capacidades das FFAA serão empregues em apoio às FSS, sem prejuízo da sua dependência hierárquica e da autonomia técnica e tática, atuam sob a direção operacional do responsável da FSS competente (territorial ou funcionalmente) que exerce o comando da operação ou do incidente de segurança.

Este tipo de articulação operacional subjaz em medidas de coordenação há muito assimiladas pelas FFAA, no contexto da sua integração em forças multinacionais conjuntas e combinadas, na relação entre componente apoiada (a que detém o comando ou direção operacional) e a apoiante que dispõe de meios e capacidades (recursos materiais, humanos e informacionais, valências ou aptidões que lhe são próprias), indispensáveis ao cumprimento da missão.

A integridade destes processos é salvaguardada no adequado planeamento do emprego operacional e no estabelecimento de estruturas de ligação, residentes permanentemente nas componentes apoiada e apoiante, ao longo de toda a operação, como garante da eficaz e eficiente interoperabilidade.

8 Lourenço, A. J., 2012. Segurança Marítima Cooperativa: Perspectivas face às Novas Ameaças. Lusíada; Política Internacional e Segurança, 6/7, Lisboa: Universidade Lusíada Editora, pp. 97-122.

Assim, a articulação sob a autoridade da FSS apoiada pelas capacidades das FFAA, assentará na coordenação ou controlo tático, ou porventura, mesmo no comando tático dos militares, que se manterão sob o comando operacional do CEMGFA, sendo a direção dos meios e capacidades das FFAA, limitado no tempo e no espaço, apoiada através do(s) elemento(s) de ligação das FFAA, bem como, no aplicável, aos serviços de proteção civil e de emergência médica.

Por inerência do exposto nas orientações, mas também do explanado na Estratégia Nacional de Combate ao Terrorismo são desenvolvidos Planos de Articulação Operacional, que necessariamente terão que ter subjacentes, entre outros:

- Processos de planeamento que, numa abordagem articulada, garantam a interoperabilidade de sistemas e de equipamentos das FFAA e FSS;
- A sistematização de procedimentos de gestão de incidentes tático-policiais e de regulação das atividades de investigação, recolha de prova e identificação de suspeitos, identificando de forma clara as competências e responsabilidades de cada força ou serviço.
- A realização de treino integrado e exercícios conjuntos;
- A definição de regras de empenhamento claras.

O grau de colaboração das FA tenderá a ser tanto mais activo quanto o grau de especialização insubstituível e indisponível nas FSS.

Partilhamos em absoluto da visão expressa por Lemos Pires[9] que defende que a resposta ao terrorismo transnacional só pode ser uma: holística, abrangente, feita com todos e para todos. No direito, na diplomacia, na segurança interna e externa, na economia e nas políticas de desenvolvimento.

Um modelo de combate ao terrorismo eficaz terá necessariamente que comtemplar uma matriz de abordagens e perspetivas múltiplas, adaptável a diversos estádios evolutivos do fenómeno. A versatilidade, dinamismo e a volubilidade da ameaça terrorista a isso obrigam.

9 Pires N. L., 2015. As Forças Armadas e o Terrorismo Transnacional. Revista Segurança & Defesa, (31), pp.08–14.

A ECONOMIA DA DEFESA

UM DESAFIO ÀS PME NACIONAIS

JOSÉ ALBERTO PEREIRA
Eurodefense Portugal
JESSICA CAETANO
Eurodefense Jovem Portugal

1. INTRODUÇÃO

Num momento em que a pandemia nos empurra para dentro de casa, os carros saem menos à rua, as marcas vendem e produzem menos viaturas, muitas empresas que trabalham para a exigente indústria automóvel são forçadas a repensar a sua atividade e o seu posicionamento. Simultaneamente, do outro lado do Oceano Atlântico, as eleições norte-americanas parecem finalmente indicar um novo rumo para o país e para as relações que mantêm com parceiros de há muitos anos, nomeadamente os parceiros da NATO. Desta forma, se por um lado a quebra no setor automóvel pressiona muitos dos seus tradicionais fornecedores a reposicionar a sua atividade, o reequilíbrio das relações no seio da NATO tenderá a estabilizar a produção industrial no setor da defesa e, desta forma, a sugerir um cenário futuro de desanuviamento e recuperação, ideal para a incorporação destas empresas industriais, maioritariamente PME, para as quais a indústria automóvel já não oferece a mesma segurança. É, assim, altura de repensar uma estratégia

nacional para a economia da defesa, atraindo competências produtivas e inovadoras, reforçando o reconhecimento e o posicionamento do nosso País quer ao nível da captação de investimento externo quer ao nível da internacionalização.

2. PRINCIPAIS CONCEITOS

"*A definição de economia de defesa tem vindo a refletir novas ameaças e novos desenvolvimentos de políticas. Durante a Guerra Fria e suas consequências imediatas, a economia de defesa era definida como o estudo económico da defesa, desarmamento e paz. No pós-Guerra Fria, o foco tem sido a economia da guerra e da paz. As mais recentes definições abrangem o estudo de guerras e conflitos convencionais e não convencionais*" (Hartley, 2006, pp. 1-2).

No entanto, a associação entre economia e defesa reforça-se a partir da Segunda Guerra Mundial, com base nos estudos de diversos economistas norte-americanos e na sequência da enorme e inovadora estrutura logística que as forças armadas deste país montaram nos diversos teatros de operações.

Assim, áreas como os modelos de corrida ao armamento, a teoria económica das alianças, a procura nas despesas militares, o papel da defesa no crescimento e desenvolvimento, a economia dos recursos humanos nas forças armadas ou a logística e contratação passaram desde a década de 60 a ser objeto de estudo científico.

A partir do ano 2000, com o final da Guerra Fria, o arranque da globalização e o aparecimento de novas ameaças à segurança mundial, temas como desarmamento, comércio de armas, terrorismo, gestão de conflitos ou a economia de manutenção da paz passaram também a constar deste objeto de estudo (Hartley, op. cit.).

Estas são abordagens mais ligadas à teoria económica e de mercado, embora os mesmos conceitos possam ser visitados numa perspetiva mais conforme com a ciência militar.

Nesta vertente, poderemos entender por "*defesa económica a atividade desenvolvida pelo Estado no sentido de, face às reais ou potenciais ameaças, perigos e riscos, proteger o desenvolvimento da economia nacional, minimizando as suas vulnerabilidade e maximizando as suas potencialidades*" (Eurodefense Portugal, 2006, pag 16), por "*economia de defesa o ramo da ciência económica que estuda os efeitos da defesa sobre as escolhas económicas (ou que estuda o processo de compatibilização e rentabilidade das atividade e despesas da defesa com a política económica nacional)" (ibidem)* e por "*economia da guerra a economia orientada para a satisfação das necessidades originadas pela realização de um esforço de guerra, centrado nas necessidades militares, mesmo com restrições das necessidades civis; extremamente dirigista a fim de compensar carências na produção, matérias primas e comércio externo*" (ibidem).

Estes são os conceitos básicos associados à economia da defesa, aos quais estão subjacentes outros, provenientes da ciência militar, como segurança nacional[1], defesa nacional[2], estratégia[3] e planeamento[4].

No entanto, em abordagens mais recentes, alguns novos conceitos têm vindo a ser utilizados, provenientes da economia e da gestão, tais como:

1 "Condição da nação que se traduz pela permanente garantia da sua sobrevivência em Paz e Liberdade, assegurando a soberania, independência <e unidade, a integridade do território, a salvaguarda coletiva de pessoas e bens e dos valores espirituais, o desenvolvimento normal das tarefas do Estado, a liberdade de ação política dos órgãos de soberania e o pleno funcionamento das instituições democráticas" (Cardoso, 1981, pag. 23)

2 "Conjunto de medidas, tanto de caráter militar como político, social e cultural que, adequadamente integradas e coordenadas, e desenvolvidas global e sectorialmente, permitem reforçar as potencialidades da Nação e minimizar as suas vulnerabilidades, com vista a torná-la apta para enfrentar todos os tipos de ameaças que, direta ou indiretamente, possam pôr em causa a segurança nacional" (ibidem)

3 "Ciência e arte de edificar, dispor e empregar os meios de coação, num dado meio e tempo, para se materializarem objetivos fixados pela política, superando problemas e explorando eventualidades, em ambiente de desacordo" (Ribeiro, 2009, pag. 27)

4 "Processo pelo qual, em âmbito militar, se estabelecem requisitos de meios, baseados numa avaliação das necessidades de defesa nacional, e se edificam e estruturam forças militares, dentro das limitações orçamentais" (Ribeiro, 2006).

mercado[5], planeamento estratégico[6], posicionamento[7], valor[8] ou marketing[9]. Esta nova perspetiva transporta a economia da defesa para uma realidade onde a competitividade, a diferenciação, a qualidade do serviço ou o acréscimo de valor para o cliente passa a ter um papel cada vez mais relevante no sucesso dos players que intervêm no mercado.

3. A DEFESA COMO ALAVANCA DO CRESCIMENTO ECONÓMICO

"Não há defesa forte baseada numa economia fraca" (Veríssimo, 2005, pag. 170). Esta evidência retrata bem a estreita ligação entre o esforço de guerra e uma estrutura económica que gere os fluxos financeiros necessários à sua subsistência. No entanto, a atual realidade económica, condicionada pela competitividade à escala global e por uma inovação tecnológica exponencial, que alavanca o crescimento das empresas e das economias onde estas se inserem, leva-nos a colocar a questão inversa: não será de igual forma a indústria da defesa responsável por uma parte muito relevante do crescimento económico?

Cabe aqui definir indústria da defesa como " o conjunto de empresas públicas e privadas que constituem a base produtiva industrial dos equipamentos de segurança e defesa" (Heidenkamp, Louth & Taylor, 2011, pag. 6). Por tradição, o ecossistema empresarial ligado à economia da defesa é dominado pelas grandes empresas multinacionais, na sua maioria OEM (Original Equipment Manufacturer), ou seja, empresas que desenvolvem e produzem estes equipamentos ou, em alternativa, adquirem as necessárias licenças para os poderem produzir. A estes respeito, Lambert & Kareta (2020)

5 "Conjunto de pessoas capaz de transformar o livre intercâmbio numa ordem social, onde a mercadoria é aceite como valor e o desejo do ganho comum por toda a sociedade" (Ganem, 2005, pag. 5).

6 "O planeamento estratégico analisa a cadeia de consequências causa - efeito ao longo do tempo, com vista a uma decisão pretendida, atual ou futura" (Steiner, 1979, pag. 14).

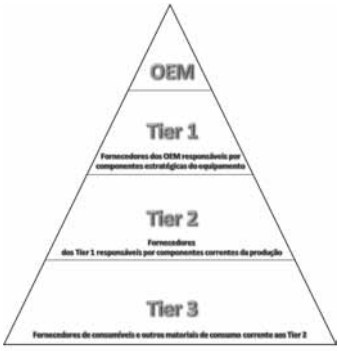
7 "Criação bem-sucedida de uma proposta que agregue valor para o mercado-alvo comprar determinado produto" (Kotler & Keller, 2006).

8 "Fatores qualitativos, quantitativos, subjetivos e objetivos, que compõe a experiência de compra" (Rust, Zeithaml & Lemon, 1988).

9 "Envolve a identificação e satisfação de necessidades humanas e sociais para suprir necessidades de forma rentável" (Kotler & Keller, 2006).

estabelecem uma hierarquia para a cadeia de fornecimentos da indústria automóvel que é perfeitamente aplicável à indústria da defesa, conforme se pode observar na figura seguinte:

Figura 1. Cadeia de abastecimento da indústria da defesa



A aplicação deste modelo de supply chain à indústria da defesa é perfeitamente pacífica. Torna-se, inclusivamente, relevante observar a forma como se distribuem as empresas ao longo da pirâmide, a respetiva dimensão, know-how e níveis de investigação em cada um dos patamares, o seu poder individual para influenciar as condições de mercado e os seus níveis de resiliência em ambientes adversos.

Efetivamente, os OEM são normalmente grandes empresas, nacionais ou transnacionais, com elevada experiência acumulada e uma significativa reputação técnica e operacional. Podem ou não manter ainda a vertente produtiva, que por vezes é subcontratada a empresas de menor dimensão ou deslocalizada para países de mão de obra mais barata. Não prescindem, no entanto, de manter sob controlo direto as áreas de inovação (I&D), críticas para o desenvolvimento de novos produtos ou funcionalidades para os atuais, assegurando desta forma o crescimento sustentado do seu negócio e a liderança do seu segmento.

Os Tier 1 são os fornecedores certificados dos OEM, os responsáveis pelo fornecimento de matérias primas e outros produtos estratégicos no processo produtivo. O seu sucesso é o sucesso do OEM que fornecem e, por isso, tratam-no como um cliente especial. Frequentemente são constituídos

propositadamente para assegurar o fornecimento ao OEM, centrando-se neste objetivo e obstando à existência de atrasos nas entregas e de quebras na produção. Os seus níveis de especialização e de certificação levam a que o seu posicionamento esteja focado num OEM, no máximo dois ou três, desde que as respetivas especificações sejam aproximadas. Uma maior dispersão é prejudicial ao cliente e, consequentemente, aos níveis de serviços que se pretendem alcançar.

Quanto aos Tier 2, estes são fornecedores dos Tier 1 e correspondem a modelos de fornecimento menos especializados, com controlos menos austeros. Apesar disso, os níveis de certificação exigidos são mais elevados que ao comum das empresas, o que implica não só o investimento num processo contínuo de certificação como a gestão permanente deste processo no âmbito do quadro operacional da empresa. Por outro lado, o grau de dependência dos seus clientes Tier 1 é também elevado, embora o nível de especialização seja menor e isso lhes permita alargar a sua carteira de clientes, reduzindo assim o risco de concentração.

Por fim os Tier 3, mais indiferenciados de todos mas mesmo assim longe das empresas cuja oferta não se encontra numa cadeia de valor tão específica e condicionada. São os fornecedores dos Tier 2, com responsabilidades ao nível dos consumíveis de peças ou equipamentos de desgaste mais ou menos rápidos. As suas especificações são mais genéricas mas, cruzando isso com a sua dimensão, a atratividade dos Tier 2 expressa-se pelo potencial de encomendas e pela capacidade de manter um nível sustentado de vendas/rentabilidade, fundamental para assegurar a sobrevivência de um Tier 3.

Destaca-se nesta "hierarquia" de fornecimentos que, à medida que se vai descendo na pirâmide, a dimensão das empresas vai sendo menor, bem como o seu poder negocial, a sua capacidade financeira (fundos próprios para investimento e tesouraria) e, sobretudo, a sua capacidade para influenciar as condições de mercado[10]. Desta forma, na passagem de Tier 1 para Tier 2 e de Tier 2 para Tier 3 a indústria da defesa vai-se tornando um mercado mais atomizado, onde o poder negocial destes operadores é incrementalmente menor, em oposição aos OEM e aos seus clientes,

10 Teoricamente a economia chama a este modelo concorrência perfeita, em que nenhum agente tem capacidade para influenciar os preços, logo, o seu poder de mercado é nulo (Correia, 2018, pag. 3).

maioritariamente governos.

Neste cenário, observamos a capilaridade desta cadeia de fornecimentos, que se radica em dois tipos de atividades geradoras de valor: a indústria e a investigação tecnológica. São estas duas atividades os principais drivers de crescimento económico associados à indústria da defesa. Mas não podemos pensar apenas a nível interno, pois muitos dos concursos para o fornecimento de equipamentos de segurança e defesa são transnacionais, o que promove naturalmente as exportações e a internacionalização das empresas. Esta realidade não é válida apenas para as grandes empresas, pois com frequência as empresas maiores levam para as empreitadas internacionais os seus pequenos fornecedores nacionais, em quem depositam confiança na qualidade dos produtos/serviços e no cumprimento dos prazos (veja-se, por exemplo, o que ocorre há décadas com a EFACEC).

Toda esta teia de ligações, relações, complementaridades e sinergias é, ao fim ao cabo, o grande efeito da economia da defesa no crescimento económico de um país. À medida que a tecnologia se vai tornando mais acessível e barata, que os custos de transporte vão diminuindo, que o acesso à informação e formação se vai disseminando e que os governos continuem a investir nestes equipamentos para missões de paz e apoio às populações, a indústria da defesa terá um papel cada vez mais relevante no crescimento económicos dos países.

4. O PAPEL DAS PME NA ECONOMIA DA DEFESA

Conforme referido no "Relatório Anual das PME Europeias 2018-2019" (European Commission, 2019), 99,8% das empresas europeias (EU-28) são PME (destas 93% são microempresas), que respondem por 55% do volume de negócios transacionado, 56,4% do valor acrescentado gerado e 66,7% do emprego. A nível europeu, a presença das PME na indústria da defesa corresponde a uma quota de 15% sobre o valor acrescentado gerado pelo setor[11] (Europe Economics, 2009, pag.33). Por outro lado, no seu "Relatório de Avaliação da Diretiva das Armas de Fogo" (European Commission, 2014), a Eurostat refere que, quanto ao número de empresas em atividade, o setor

11 Dados estatísticos de 2006, os últimos disponibilizados pela Eurostat.

(EU-28) é dominado pelas microempresas (76,5% do total), enquanto as PME representam 21% quer do emprego quer do volume de negócios. Por fim, a Comissão Europeia afirma no seu site que "… existem mais de 2.500 PME a desempenhar um papel central nas complexas cadeias de abastecimento de defesa na Europa"[12].

Em termos de futuro próximo, o site norte-americano "SME" propõe 6 tendências para observar no aeroespacial e defesa em 2020, que poderão vir a condicionar o mercado nos próximos anos (Kenkel, 2020). São elas:

- abundância de incertezas, com grande dificuldade em planear o futuro;
- grande pressão sobre a liquidez, com as receitas a não acompanharem os custos;
- atratividade do setor face à quebra em setor próximos (indústria automóvel);
- grande atratividade do digital gera interesse em tecnologia incrementais;
- maior atenção à gestão da cadeia de fornecimentos;
- reconversão da oferta das empresas é vantagem comparativa.

E no que respeita a Portugal? A indústria de defesa nacional representa hoje cerca de 3% do PIB, sendo que 80% da sua produção se destina à exportação[13]. No seu programa, o Governo de Portugal aponta a Lei da Programação Militar (LPM) como o principal instrumento financeiro plurianual de defesa nacional, baseado na inovação e na geração de valor acrescentado para a economia nacional, reforço do emprego

12 "There are more than 2,500 SMEs playing a central role in the complex defence supply chains in Europe". (obtido em 28.11.2020 de https://ec.europa.eu/growth/sectors/defence/smes_en).

13 Segundo informação disponibilizada pelo Sr. Ministro da Defesa, João Gomes Cravinho, durante um encontro com empresários da região de Leiria, sob o tema "Economia de Defesa para o Futuro" (obtido em 28.11.2020 de https://www.portugal.gov.pt/pt/gc22/comunicacao/noticia?i=economia-de-defesa-e-uma-oportunidade-para-as-empresas-nacionais).

qualificado e promoção das exportações das empresas neste setor. Para cumprir este objetivo, foi criada em 2014 a Plataforma das Indústrias de Defesa (idD), uma empresa pública que visa a promoção externa da BTID - Base Tecnológica e Industrial de Defesa, uma base de dados com mais de 380 empresas, sobretudo PME duais (que produzem para clientes civis e militares), com o objetivo de desenvolver as capacidades nacionais nesta área, assumindo Portugal como produtor e exportador de tecnologia e serviços de defesa.

Não existindo ainda uma prática específica para contratação de PME, verifica-se no entanto um aumento da participação da indústria no ciclo de programação da defesa militar (CPDM), nomeadamente na deteção de potenciais áreas de negócio, em articulação com a BTID e centros de investigação militares e civis. A este respeito, o recente "Manual para o Planeamento Estratégico Militar do Estado Maior General das Forças Armadas" (EMGFA, 2020) inclui propostas muito interessantes relativamente à articulação entre o Governo, as Forças Armadas, a indústria de defesa e outros stakeholders[14] na revisão/reformulação da LPM e do CPDM.

Efetivamente, conforme refere este documento, "A dimensão industrial é um fator relevante na decisão política, considerando as oportunidades de acesso a parcerias com centros de investigação e empresas de outros países europeus, capazes de fomentar a inovação e a eficiência da BTID nacional. (…) Será essencial uma participação nacional coordenada (política, militar e empresarial) quer na contribuição para a formulação pela UE de projetos no quadro da PESCO, do FED, etc., que interessem a Portugal, quer na participação nacional nos projetos aprovados, nomeadamente nos que se enquadrem nas necessidades militares e do desenvolvimento da BTID nacional, bem como que garantam impactos positivos no âmbito do tecido científico-tecnológico nacional e no quadro empresarial e industrial da BTID do nosso país." (EMGFA, 2020, pp. 72 – 74).

Mas, para além de detetar a necessidade, o documento vai mais longe na medida em que apresenta uma metodologia específica para a articulação entre estas entidades, referindo que "… esta metodologia requer a imple-

14 Um stakeholder é uma parte interessada numa empresa, num projeto ou num negócio a qual pode afetar ou pela qual pode ser afetada. (obtido em 29.11.2020 de https://www.investopedia.com/terms/s/stakeholder.asp).

mentação de estruturas e processos, que possibilitem a interação entre os diferentes stakeholders do processo, nomeadamente a coordenação entre a idD, a DGRDN, as Forças Armadas e as demais entidades representativas da Indústria Nacional, nomeadamente da BTID, bem como do SCTN ."(EMGFA, 2020, pag. 75). O culminar desta definição metodológica é a tipificação da interação entre os diversos stakeholders, criando um modelo de envolvência alargada nos seguintes termos: "Esta interação poderá ocorrer em dois planos: no plano político-estratégico e no estratégico-militar. No plano político-estratégico, assume papel relevante o GAPP-PESCO (Grupo de Acompanhamento da Participação nos Projetos PESCO) com perspetivas de alargamento das respetivas competências à coordenação dos outros mecanismos de financiamento da UE, assegurando a interface entre a DGPDN e a DGRDN, ambas com competências próprias nestes domínios. No plano estratégico-militar, releva o papel central do EMGFA e dos Ramos das Forças Armadas, através da DIPLAEM e das respetivas Divisões de Planeamento. No quadro da ligação às indústrias de Defesa são relevantes as participações da idD, da EURODEFENSE Portugal e da Associação Industrial Portuguesa-Câmara de Comércio e Indústria (AIP-CCI), entre outras, como facilitadores e plataformas de ligação e comunicação." (EMGFA, 2020, pag. 79).

A inclusão do GAPP-PESCO neste modelo endossa o tema para o domínio financeiro, onde a estratégia do Governo assenta na LPM e no Fundo Europeu de Defesa (FED), enraizado nos projetos da PESCO para apoiar o investimento das PME no abastecimento de OEM, Tier 1 e Tier 2. Nesta área, é crucial apoiar financeiramente o investimento das PME na certificação, um esforço contínuo e crescente que é incontornável para qualquer PME que pretenda estar a montante neste setor, mas para o qual até ao momento não existe uma linha de crédito específica com condições atrativas.

A título de exemplo, podemos referir que a articulação institucional promovida pelo Ministério da Defesa Nacional funcionou com sucesso no recente caso do "Sistema de Combate do Soldado", projeto de uniformes, equipamentos e comando e controlo liderado pelo Exército Português em parceria com o idD. Para além dos centros de investigação das Universidades do Minho, Coimbra e Porto, o projeto incluiu também o Citeve - Centro Tecnológico da Indústria Têxtil e do Vestuário de Portugal e as

empresas Lavoro, Damel, Riopele e Monte Campo. A inovação é uma das principais características deste projeto, que inclui equipamentos com capacidade adicional de resistência ao calor e à chama, impermeabilização, proteção balística e regulação da temperatura corporal, camuflados com têxteis inovadores não detetáveis por radar ou sistemas infravermelhos e botas adaptáveis a diferentes tipologias de missão. O objetivo principal é aumentar a capacidade de sobrevivência do soldado e os efeitos são, para já, a redução do peso dos componentes do novo uniforme, com o inerente aumento da velocidade e mobilidade no cenário operacional, maior nível de conforto para o soldado e maior dificuldade de deteção pelo inimigo (visualmente ou infravermelho) devido ao padrão de camuflagem.

A chave para o envolvimento das PME na indústria de defesa é a necessidade de ter uma visão clara do futuro, do tipo de equipamento e dos requisitos exigidos em cada revisão da LPM, mantendo a continuidade e consistência de cada tipologia de equipamento, apesar do efeito de desinvestimento na defesa nacional que tem sido observado nos últimos anos. Quanto à comparação com outros setores, algum benchmarking permite novas propostas alinhadas em três eixos fundamentais: dinâmica da concorrência, articulação do processo produtivo e soluções de apoio financeiro.

No primeiro caso, mantendo uma visão de favorecimento do modelo de consórcio como forma de agilizar o acesso das PME ao setor, é importante considerar um conjunto de majorações no valor técnico e económico dos projetos (PESCO, nacional, outros) que premeiem a inclusão de PME e centros de investigação europeus. Esta majoração pode surgir sob a forma de aumentos diretos do montante a atribuir, subsídios à produção ou outras formas a considerar (eventualmente com aconselhamento do Banco Europeu de Investimento).

No segundo caso, a articulação do processo produtivo pode ocorrer pela inclusão de PME europeias nos processos produtivos dos grandes operadores europeus, pelo apoio direto em ações concretas, pela viabilização de processos de concorrência, ou pelo apoio à participação conjunta em eventos internacionais de grande visibilidade e / ou reputação.

No terceiro caso, as soluções de financiamento assemelham-se a outros

fundos comunitários europeus, nomeadamente através da conceção e disponibilização de linhas de crédito atrativas, focadas no apoio ao investimento, inovação tecnológica e empreendedorismo, formação / tutoria e gestão de tesouraria de empresas do sector (com ciclos de operação mais longos). No entanto, a principal lacuna identificada pelas PME nacionais é a falta de informação sobre oportunidades e procedimentos para responder a pedidos de financiamento comunitário. Neste contexto, é importante destacar o esforço investido pelos vários intervenientes na esfera da defesa nacional (nomeadamente Ministério da Defesa Nacional, Estado-Maior General das Forças Armadas, Grupo de Acompanhamento do Projeto PESCO e idD, entre outros) no sistema de capacitação, visando maior articulação nacional com base na BTID e vinculação do financiamento nacional (LPM) ao financiamento comunitário (EDIDP, FED, outros).

Por fim, destacamos o reconhecimento que as PME e startups nacionais de tecnologia têm no setor. Da Critical Software (que desde 1998 trabalha para a NASA, ESA, Agusta Westland e outras) à Theia, recentemente galardoada com o Copernicus Masters 2019, existe um ecossistema empreendedor de elevada qualidade e potencial em Portugal. O IdD, por meio do BTID e da Startup Defense, tem vindo a promover estas competências. Mas outras entidades já entenderam esta oportunidade, como a AIP, AED - Portugal ou o Instituto Politécnico de Setúbal, que em 2017 abriu um Curso de Aeronáutica, em parceria do Aeródromo de Ponte de Sôr.

5. CONCLUSÕES

A economia da defesa tem vindo a ganhar relevância desde a Segunda Guerra Mundial. Nos últimos anos, com as dinâmicas de globalização e de transformação digital, tem abandonado os modelos económicos/econométricos para focar com atenção crescente nos aspetos ligados à gestão e aos mercados, tais como gestão de processos e produção, fornecimentos e cadeia de valor, inovação e orientação ao cliente, mercados e competitividade. É uma mudança enorme, não apenas do modus operandi dos agentes, mas sobretudo do respetivo mindset e dos seus stakeholders.

A capilaridade da cadeia de fornecimentos, muito semelhante à da indústria

automóvel, junta-se à produção industrial e à inovação tecnologia para constituir o triplo driver do setor na atual conjuntura, cujos principais insights para o futuro próximo passam pela incerteza do ambiente, a pressão sobre a liquidez, a atratividade de nicho, a aposta nas tecnologias incrementais, na gestão da cadeia de fornecimentos e na reconversão da oferta como geradores de vantagens competitivas a curto/médio prazo.

Em Portugal, a LPM e o CPDM mantêm-se como os grandes referenciais para a indústria da defesa, sendo que o modelo sugerido pelo EMGFA/DIPLAEM alarga a participação na respetiva revisão/reformulação a um número alargado de stakeholders. A idD, através da BTID, continua a ser o agente privilegiado do Governo para captar novos operadores para o setor, preferencialmente PME. O Fundo Europeu de Defesa, como modelo supranacional de financiamento dos projetos, será importante a complementar o financiamento público via LPM. No entanto, com a atratividade do setor a aumentar no contexto da pandemia, para as empresas que operam a montante da produção automóvel, trata-se de uma oportunidade de ouro para aproveitar o potencial das nossas PME industriais e reforçar a posição portuguesa na economia da defesa, a nível comunitário e até mundial.

6. BIBLIOGRAFIA

Cardoso, L. (1981). Defesa Nacional - Segurança Nacional. Lisboa: Instituto da Defesa Nacional. Nação e Defesa, nº 17, pp.11-24.

Correia, A. (2019). A Cooperação Estruturada Permanente, o Fundo Europeu de Defesa e a Lei de Programação Militar 2019-2030. (obtido em 28.11.2020 de https://eurodefense.pt/a-cooperacao-estruturada-permanente-o-fundo-europeu-de-defesa-e-a-lei-de-programacao-militar-2019-2030-segunda-atualizacao/).

Correia, J. (2018). Microeconomia II. Porto: Faculdade Economia Universidade Porto.

Costa, A. (2020). Overview of the Portuguese Defense Industry. (obtido em 28.11.2020 de https://eurodefense.pt/overview-of-the-portuguese-

defence-industry/).

Eurodefense Portugal (2006). A Economia de Defesa: Sua Integração no Planeamento Estratégico. Lisboa: Centro de Estudos Eurodefense Portugal.

Europe Economics (2009). Study on the Competitiveness of European SME in the Defense Sector. Brussels: European Commission.

European Commission (2014). Evaluation of the Firearms Directive. Brussels: European Union.

European Commission (2019). Annual Report on European SMEs 2018/2019. Brussels: European Union.

Estado-Maior-General das Forças Armadas (2020). PEMGFA/PLN 001. Manual para o Planeamento Estratégico Militar do Estado Maior General das Forças Armadas. Lisboa: MDN/EMGFA/DIPLAEM.

Ganem, A. (2005). Regras e Ordem do Mercado nas Visões de Adam Smith e F. A. Hayek. Anais do XXXIII Encontro Nacional de Economia. Niterói, RJ: ANPEC - Associação Nacional dos Centros de Pós-Graduação em Economia.

Hartley, K. (2006). Defense Economics: Achievements and Challenges. Proceedings of the 10th Annual International Conference on Economics and Security. York: Centre for Defense Economics, University of York.

Heidenkamp, H., Louth, J. & Taylor, T. (2011). The Defense Industrial Ecosystem: Delivering Security in an Uncertain World. Whitehall, Royal United Services Institute. London: Stephen Austin and Sons, Ltd.

Kenkel, J. (2020). Six Trends to Watch for in Aerospace and Defense This Year. (Obtido em 28.11.2020 de https://www.sme.org/technologies/articles/2020/october/six-trends-to-watch-for-in-aerospace-and-defense-this-year/).

Kotler, P.& Keller, K. (2006). Administração de Marketing. 12ª edição. São

Paulo: Pearson Hall.

Lambert, S. & Kareta, N. (2020). The automotive supply chain: Tier suppliers explained. (obtido em 28.11.2020 de https://www.mes-insights.com/the-automotive-supply-chain-tier-suppliers-explained-a-966964/).

Ramos, A. & Vasconcellos, D. (2020). O Fundo Europeu de Defesa em Movimento. (obtido em 28.11.2020 de https://eurodefense.pt/o-fundo-europeu-de-defesa-em-movimento/).

Ribeiro, A. (2006). Planeamento Estratégico e de Forças. Revista Militar, nº 2457 (obtido em 23.11.2020 de https://www.revistamilitar.pt/artigo/136).

Ribeiro, A. (2009). O Essencial ao Processo Estratégico - Teoria Geral da Estratégia. Coimbra: Livraria Almedina.

Rust, R. & Zeithaml, V. & Lemon, K. (2001). O Valor do Cliente: Customer Equity. Porto Alegre: Bookman.

Steiner, G. (1979). Strategic Planning: What Every Manager Must Know. New York: Free Press.

Veríssimo, H. (2005). A Defesa Económica como Componente da Defesa Nacional. Nação & Defesa, nº 110, 3ª série, pp. 167 – 189.

TRANSIÇÃO DIGITAL: MUDAR A CULTURA ORGANIZACIONAL

LUÍSA PROENÇA
Diretora Nacional Adjunta da Polícia Judiciária

BREVE ENQUADRAMENTO

A Administração Pública é, por regra, lenta a mudar a sua organização e os seus processos de trabalho.

Ao longo das últimas décadas, sobretudo ao longo das últimas duas décadas, foi-se assistindo a inúmeras tentativas de desmaterializar a Administração Pública, em resultado da inovação tecnológica a que fomos assistindo e atendendo à necessidade premente de uma melhor gestão de recursos, quer humanos, quer financeiros.

A adoção, em Portugal, em meados da década de oitenta, de princípios inerentes ao conceito de *New Public Management*, em reação aos críticos dos serviços públicos que, ao longo dos anos, os foram considerando ineficiente a absorvedor de enormes recursos públicos, assenta no pressuposto de que tudo o que é público é ineficiente e sai mais caro ao cidadão do que se fosse prestado pelo setor privado.

Em termos gerais, trata-se de uma corrente de pensamento que considera que a gestão pública deve importar os modelos da gestão privada, de modo a reduzir custos, aumentar a produtividade, o desempenho, a transparência

das decisões e a tornar-se mais eficiente e eficaz. Como tal, promove reformas que reduzam o peso do Estado, aumentem a participação do sector privado na prestação de serviços com maior qualidade e reduzam a despesa pública. A preocupação com uma melhor gestão da coisa pública assume enorme relevo.

As diferenças entre a gestão pública e a gestão privada têm sido objeto de inúmeros estudos científicos, na procura de um equilíbrio entre ambas as dimensões e na forma como estas divergem ou convergem, quando se trata de prestar um melhor serviço público ao cidadão. Mintzberg (2010, pp. 55-130) considera que existe uma diferença fundamental entre gestão pública e gestão privada, na medida em que os cidadãos não podem ser encarados como meros consumidores, ou clientes, e que muitos dos problemas com que a Administração Pública se debate, resultam da tentativa de imitação da gestão empresarial. Mintzberg afirma que não é possível transferir para a complexidade do sector público princípios de gestão empresarial, como a autonomização de atividades, a medição do desempenho através dos objetivos atingidos e assumindo que os gestores profissionalizados podem gerir de forma eficiente as organizações públicas, podendo ser responsabilizados pelo seu desempenho. Também o cidadão não pode ser encarado como um cliente, dada a diferença das relações entre estes e a Administração Pública, em contextos muito diversificados.

O *New Public Management* ganha maior expressão à medida que se desenvolvem as tecnologias da informação e da comunicação, que tornam possível atingir os objetivos de uma melhor gestão e de uma atitude inovadora em matéria de Administração Pública. É essencial reduzir a burocracia, tanto quanto for possível, colocar o cidadão no centro das preocupações e dar competências aos funcionários públicos, para que seja possível focarem-se em tarefas de maior valor e obterem melhores resultados.

Parece não poder afirmar-se que existe um modelo perfeito de gestão pública, na medida em que a Administração Pública lida com as várias dimensões da vida humana, sendo a sua tarefa principal a de gerir conflitos e procurar consensos (Rocha J. A., 2009, pp. 184-186). É isto que a distingue do sector privado. A transposição das boas regras de gestão do sector privado para o sector público, sem se conhecerem as diferenças entre as duas realidades

e, consequentemente, sem serem acauteladas as especificidades do sector público, veio a revelar-se negativo. Essas especificidades, conforme refere Pollitt (1993), citado por Elisabete Carvalho (2001, pp. 56-62), são: responsabilidade perante os representantes eleitos; múltiplos e conflituantes objetivos e prioridades; ausência ou raridade de organizações em competição; relação oferta/rendimento; processos orientados ao cidadão-cliente; gestão de pessoal e enquadramento legal. Nenhuma destas especificidades encontra paralelo no sector privado, pelo que a transposição se tornou nefasta à prossecução de uma boa gestão.

A transposição dos princípios do *New Public Management* para a Administração Pública portuguesa levou a que ganhassem relevo os aspetos relacionados com uma melhor gestão de recursos humanos e financeiros, a transparência dos atos da Administração Pública, a importância do cidadão enquanto cliente e a qualidade do serviço que lhe é prestado. Tratou-se de transpor para a gestão pública conceitos da gestão privada, substituindo a administração da coisa pública pela gestão da coisa pública, assumindo que a gestão privada é mais eficiente que a gestão pública, que uma boa gestão é determinante para fazer face a uma enorme variedade de problemas económicos e sociais e que a gestão é um corpo distinto de conhecimentos universalmente aplicáveis (Carvalho, 2001, pp. 46-61).

A adoção do novo modelo de gestão tornou-se evidente em Portugal, na década de noventa, pela orientação da Administração Pública para o mercado e para o cliente/cidadão. Em virtude desta orientação, a Administração Pública procurou ser mais flexível, quer ao nível organizacional, do pessoal, ou da administração financeira. Contudo, e contrariamente aos princípios da nova gestão pública, a Administração Pública politizou-se fortemente (Rocha, 1998), na medida em que os cargos de topo passaram a ser ocupados, na maior parte dos casos, por políticos ou por pessoas ligadas ao poder político. O poder político passou a ter um domínio muito forte sobre os gestores de topo da Administração Pública, o que deita por terra qualquer tentativa de equiparar a gestão pública à gestão privada. Para além do mais, os funcionários públicos de carreira não foram envolvidos em nenhum processo de mudança. Pelo contrário, mantiveram um papel passivo, quase de meros observadores, ao longo dos anos. A gestão pública passa a estar, em larga medida, ligada aos ciclos eleitorais, enquanto

a gestão privada tem o mercado como único foco.

A transformação da Administração Pública tem ocorrido pela via da adoção de tecnologias inovadoras. Faltam, contudo, instrumentos que meçam o grau de transformação dos seus processos. Apesar da introdução dos conceitos do *New Public Management*, existem poucos dados disponíveis, que permitam analisar até que ponto os organismos estão a alterar os seus processos de trabalho, à medida que vão introduzindo inovações tecnológicas. Acresce o facto de manterem estruturas hierárquicas rígidas, regidas por leis e normas, antagónicas dos princípios da reengenharia e desadequadas à flexibilidade que a inovação e a mudança requerem. As estruturas e relações hierárquicas não se reajustam perante a necessidade de existência de equipas multidisciplinares de projeto, com hierarquias de projeto distintas das hierarquias organizacionais, o que se revela um fator de constrangimento na prossecução dos objetivos de uma Administração Pública digital, centrada nos processos e orientada para o cidadão. O aumento da capacidade de inovação e a flexibilidade no modelo de gestão andam a par e potenciam-se entre si.

A reforma da Administração Pública, mais do que uma questão de mentalidades, é uma questão de processos e as mentalidades são também consequência dos processos (Mozzicafreddo & Gomes, 2011, pp. 2-4). É da alteração dos processos e, consequentemente dos procedimentos e dos comportamentos que pode resultar um novo modelo de gestão, que cumpra os objetivos de uma gestão mais racional, nomeadamente de recursos humanos, de competências, de sistemas e tecnologias de informação e de infraestruturas. Também Pollitt e Bouckaert (2004) consideram que a reforma da gestão pública é um meio para atingir vários fins, nomeadamente uma maior poupança nos gastos públicos, a melhoria da qualidade dos serviços públicos, ações governativas mais eficientes e uma maior eficácia das políticas públicas implementadas.

A reengenharia e/ou o redesenho de processos apresenta-se como um meio indispensável para a transformação das organizações em contextos de mudança e um contributo decisivo para a obtenção de melhores resultados a todos os níveis. Sem repensar os processos, redefinindo-os e orientando-os para a obtenção de maior valor acrescentado, a tecnologia de pouco

serve. As novas tecnologias a suportar processos antigos tornar-se-iam um perigo, pois permitiriam tomar más decisões de forma mais rápida (Hammer & Champy, 2003).

Na Administração Pública portuguesa, este conceito tem estado presente ao longo das últimas duas décadas, como resultado da introdução massiva das tecnologias de informação e comunicação. Contudo, a prática parece revelar que o perigo a que Hammer e Champy se referiam não era infundado, pois muitos são os exemplos de projetos em que a inovação parece ter ficado pela introdução da tecnologia, sem alterações significativas ao nível dos processos. Implementar tecnologia inovadora a suportar processos tradicionais, sem se ter aproveitado as potencialidades da tecnologia para repensar os processos de trabalho, revelou-se negativo para o processo de transformação dos serviços públicos, nos quais se incluem as funções exercidas pelas forças e serviços de segurança. Repensando os processos de trabalho e fazendo a sua reengenharia, teria tido um melhor resultado no desejado aumento da eficiência e eficácia dos serviços públicos prestados ao cidadão, ao mesmo tempo que teria contribuido para a redução do peso dos serviços públicos no orçamento do Estado. Durante anos, assistimos a inúmeras tentativas de reengenharia, sem que se tivessem operado verdadeiras alterações aos modelos de funcionamento e aos processos de trabalho da Administraçao Pública.

CULTURA, PODER E MUDANÇA ORGANIZACIONAL

A reforma da cultura organizacional assume premência quando se pretende adotar modelos de funcionamento disruptivos e mais em linha com as tendências de uma moderna Administração Pública, que cada vez mais se assume como *digital-by-default*. Impõe-se uma mudança da cultura organizacional, que permita aliar os valores do serviço público às preocupações com a eficiência e a eficácia. As organizações da Administração Pública foram, ao longo destas últimas duas décadas, interiorizando a ideia de que, para cumprir os objetivos de uma melhor gestão, será necessário redesenhar os seus processos de negócio. Foi-se assistindo a uma maior preocupação com a otimização de processos, com a tentativa de eliminar burocracias desnecessárias e rumar no sentido da "digitalização" de serviços. Ainda

estamos, contudo, longe da transição digital, que assenta no desenho de serviços nado digitais e não na digitalização de serviços a partir de modelos pré-existentes.

Mas importa, antes de mais, refletir um pouco sobre a organização e a cultura organizacional. Afinal o que é uma organização? O que é a cultura organizacional? Como referem Laudon e Laudon (2005), uma organização é uma entidade formal, criada de acordo com a lei, regulada por regras e procedimentos sujeitos à lei. Embora muito poderosa, esta definição é simplista, na medida em que deixa de parte os aspetos comportamentais que caracterizam e influenciam a organização. Procurando chegar a uma definição mais realista, estes autores afirmam que uma organização é um conjunto de direitos, privilégios, obrigações e responsabilidades, delicadamente balanceados entre o conflito e a resolução do conflito, durante um determinado período de tempo.

A cultura organizacional é uma força unificadora poderosa, que restringe o conflito e promove a compreensão mútua, a aceitação de procedimentos e a interiorização de práticas comuns (Laudon & Laudon, Jane, 2005). Quando todos partilham a mesma visão e os mesmos valores é mais fácil atingir consensos noutras matérias. Em contrapartida, a cultura organizacional revela-se um forte obstáculo à mudança, nomeadamente quando se está perante projetos que transformam a organização, nomeadamente pela adoção de tecnologias inovadoras da informação e da comunicação. Qualquer mudança tecnológica que constitua uma ameaça aos valores culturais comummente aceites torna-se muito difícil de concretizar. No entanto, algumas organizações acabam por perceber que, para sobreviver, têm que inovar, têm que mudar, nem que seja pela introdução de uma nova tecnologia, mesmo que esta ponha em causa a cultura da organização. Nestes casos, são as tecnologias e os sistemas de informação que mudam a organização. A primeira grande mudança dá-se ao nível da própria estrutura hierárquica, na medida em que a introdução de sistemas de informação conduz ao achatamento da pirâmide hierárquica. Na Administração Pública, nem sempre este achatamento é visível. Algumas organizações mantêm-se fortemente hierarquizadas, como é o caso das forças e serviços de segurança, o que não favorece o processo de inovação e mudança. O achatamento da pirâmide hierárquica torna as organizações mais ágeis e mais rápidas na

resposta à evolução dos contextos em que atuam.

A cultura da organização pode promover ou, pelo contrário, dificultar a mudança. Se, por um lado, pode constituir uma força de unificação, que restringe o conflito político e promove o consenso acerca dos processos e dos procedimentos, pode, por outro, revelar-se um poderoso bloqueio à mudança, sobretudo quando se trata de mudanças tecnológicas. Qualquer mudança tecnológica, que ponha em causa os aspetos culturais, aceites pela organização, pode enfrentar alguma resistência. A mudança tecnológica pode, contudo, assumir-se como a única forma de as organizações evoluírem, sendo ela própria indutora da mudança da cultura organizacional.

Analisando as organizações, estas apresentam seis elementos de base, a que Mintzberg (2010) chama "forças", as quais estão em comunicação constante: Vértice estratégico – gestores e líderes de topo, a quem cabe proporcionar as condições para que a organização possa atingir os seus objetivos; Linha hierárquica média – gestores intermédios, diretores e chefias, a quem cabe a ligação entre o vértice estratégico e o centro operacional; Centro operacional – todos os operacionais que executam trabalhos de suporte na organização; Tecnoestrutura – analistas, engenheiros, contabilistas, funcionários responsáveis pelo planeamento e pela organização e métodos, responsáveis por introduzir sistemas de trabalho uniformes para toda a organização; Logística – pessoas a quem cabe assegurar serviços de apoio, assessoria jurídica, relações públicas, investigação; Ideologia – engloba os valores e as tradições, que distinguem as organizações e dão vida à estrutura organizacional. Todos os indivíduos têm expectativas e ambições diferentes, que podem ser conflituantes entre si. Tendo presente as várias dimensões acima, é muito importante prestar alguma atenção às relações de poder e aos conflitos de interesses dentro das organizações, para se perceber até que ponto estes condicionam o sucesso dos projetos de inovação e mudança e definir as estratégias de mitigação dos riscos de insucesso.

M. Crozier e E. Friedberg (1977), pela sua observação das organizações enquanto sistemas políticos, introduziram os conceitos de "ator social", de "zonas de incerteza", de "margem de liberdade" e de "jogos de poder", para caracterizar a problemática dos comportamentos dos indivíduos. Consideram que as organizações são palcos de interações entre atores sociais, em

que a estrutura fica condicionada pelas disputas de poder. Os atores são desiguais perante as incertezas pertinentes do problema. Segundo estes teóricos, aqueles que, pela sua situação, recursos ou capacidades (que são sempre pessoais e sociais, pois não se podem conceber num campo não estruturado) são capazes de as controlar, utilizarão o poder para se imporem em relação aos outros e dominarão as incertezas dos atores que forem capazes de afirmar e impor o seu domínio das incertezas mais cruciais. As relações entre os atores e a relação destes com os problemas, logo com as zonas de incerteza, inserem-se sempre num campo de desigualdade, estruturado por relações de poder, que, no caso das organizações públicas, decorre, normalmente, da posição hierárquica.

Nos processos de mudança, assumem particular importância os jogos de poder. Os atores sociais só aceitam a mudança se os jogos em que participam lhes permitirem atingir os objetivos individuais, que, normalmente, estão relacionados com o aumento de poder. Tudo o que possa atentar contra estes objetivos constituirá um fator de resistência à mudança. Tentarão orientar a mudança de forma a manter e, eventualmente, reforçar as zonas de incerteza que controlam. Toda a mudança representa um perigo, na medida em que põe em causa as regras do jogo em que o ator participa, as fontes de poder e a margem de liberdade, alterando ou fazendo desaparecer as zonas de incerteza que controlam. Crozier e Friedberg (1977) contrapõem as teorias de que a mudança falha devido à falta de comunicação, informação e envolvimento, na medida em que consideram que as forças em jogo são outras e que não se dominam pela comunicação.

A implementação de um novo sistema tecnológico, assente na desmaterialização/digitalização de documentos, conteúdos e processos, altera a forma como todos os colaboradores desempenham as suas funções. Trata-se de uma mudança planeada, profunda, do tipo transformacional.

Kurt Lewin (2010) analisa a mudança como um processo com três fases: a fase do descongelamento das normas do grupo – quando se abandonam comportamentos e atitudes habituais e se admite que a situação não está bem e é preciso mudar; a fase de deslocação – que dá lugar à mudança, reduzindo as forças de resistência que representam a ligação às normas. Esta é uma fase de transição, em que se experimentam as novas práticas;

e a fase do congelamento – em que se criam novamente as normas que permitem atingir um novo ponto de equilíbrio e evitar o retorno ao estado inicial, capaz de desestabilizar o novo campo de forças. Esta fase consiste na introdução e interiorização de novos hábitos de trabalho, de modo a que a mudança se torne permanente. Na mudança organizacional é preciso que todos os *stakeholders* compreendam os desafios que obrigam à mudança, que entendam porque é que a situação atual está desajustada e quais as consequências da não mudança.

Beckard e Harris (1987) defendem que a mudança ocorre quando o nível de insatisfação com o *status quo*, somado ao desejo de mudança e à exequibilidade da mesma é superior ao custo da mudança. Isto significa que, para que a mudança seja viável, é necessário que os intervenientes estejam suficientemente insatisfeitos, ansiosos por alcançar o resultado final que a mudança propõe e convencidos de que a mudança é viável.

A mudança transformacional requer uma nova forma de pensar, estar e sentir; a mudança transformacional exige uma nova cultura. Ora, quando se trata de organizações da Administração Pública, fortemente hierarquizadas e legalistas, a cultura não muda de um momento para o outro, muito menos pela adoção de um novo sistema tecnológico, apesar das alterações profundas no quotidiano dos colaboradores. A consciência de que as pessoas são o elemento chave em qualquer processo de mudança tem levado muitos estudiosos a analisar comportamentos e a definir linhas de orientação para líderes e equipas de projeto, com vista a perceber a génese das resistências e a forma de as ultrapassar, com a consciência de que, à partida, ninguém gosta de mudar.

Peter Drucker (1997) afirmava que não se pode gerir a mudança, só se pode antecipá-la ou liderá-la.

John Kotter (1996) representa um importante contributo para a definição de uma estratégia possível para gerir a mudança, ao preconizar as oito etapas de um processo de mudança:

- Criar um sentimento de urgência;

- Criar uma poderosa coligação de liderança;
- Criar uma visão;
- Comunicar essa visão;
- Dar poder para implementar a visão;
- Planear e implementar mudanças de curto prazo;
- Consolidar melhorias e produzir mais mudanças; institucionalizar as novas abordagens.

Finalmente, Kotter e Rathgeber (2011) defendem que a comunicação é o segredo para se gerir a mudança com eficácia.

TRANSIÇÃO DIGITAL

A Administração Pública enfrenta o enorme desafio da transição digital. Não lhe basta otimizar os seus processos de trabalho ou proceder à sua reengenharia; é preciso redesenhar os serviços que presta, para que estes nasçam logo digitais, tirando proveito da evolução tecnológica.

O desafio é tanto maior quanto a lentidão com que as organizações foram mudando e se foram transformando. Ou seja, a premência é maior para as entidades que foram tardando em adotar ferramentas tecnológicas modernas, resistindo à mudança que há muito se afigura como inevitável. A mudança é agora maior, mais disruptiva, não havendo lugar a hesitações. A Administração Pública tem que prosseguir o caminho da gestão mais eficiente e mais eficaz, de modo a responder às obrigações que a lei lhe impõe, sob pena de ver os seus orçamentos penalizados. Esta é também a condição para que os organismos sejam apoiados com fundos europeus ou com o Plano de Recuperação e Resiliência. Por outro lado, as tecnologias emergentes, como a Inteligência Artificial, o blockchain e outras, são essenciais para que os organismos sejam mais rápidos e melhor capacitados para lidar com os enormes volumes de informação. Só uma organização "digital

por defeito" reúne as condições de base para tirar pleno proveito destas tecnologias.

O contexto de pandemia pelo Covid-19 veio reforçar a necessidade de os organismos operarem a mudança ainda em falta e prosseguir no caminho da transição digital. A rápida adoção do teletrabalho, quando as funções o permitem, veio demonstrar que a transição para o mundo digital é possível, mas, ao mesmo tempo, veio evidenciar as fragilidades das infraestruturas das redes de comunicação das entidades de serviço público. As questões da (ciber)segurança e da (ciber)resiliência das redes de comunicação colocam-se agora com maior acuidade e assumiram primazia na estratégia dos organismos para as Tecnologias da Informação e da Comunicação.

Operacionalizando a transição digital dos serviços, estaremos perante uma grande mudança na Administração Pública portuguesa, que poderá resultar numa Administração Pública mais eficiente, mais eficaz, menos onerosa para o cidadão e, ao mesmo tempo, um motor do desenvolvimento económico, da competitividade e do emprego em Portugal.

REFERÊNCIAS BIBLIOGRÁFICAS:

Beckhard, R., & Harris, R. (1987). *Organisational Transitions: Managing Complex Change*. Boston: Addison-Wesley.

Carvalho, E. R. (2001). *Reengenharia na Administração Pública: A Procura de Novos Modelos de Gestão*. Lisboa: ISCP..

Crozier, M., & Friedberg, E. (1977). *L'Acteur et le Systême*. Paris: Éditions du Seuil.

Drucker, P. F. (1997). *Inovação e Gestão*. Lisboa: Presença.

Hammer, M., & Champy, J. (2003). *Reengineering the Corporation: a Manifesto for Business Revolution*. EUA: Harper Business Essentials.

Kotter, J. P. (1996). *Leading Change*. Boston: Harvard Business School Press.s.

Kotter, J., & Rathgeber, H. (2011). *O nosso iceberg está a derreter.* Lisboa: Ideias de ler.

Kurt, L. (1951). *Field Theory in Social Science: Selected Theoretical Papers*. Michigan: Harper.

Laudon, K. C., & Laudon, Jane. (2005, Fevereiro 02). *Management of Information Systems: Managing the Digital Firm.* New Jersey: Prentice Hall.

Lewin, K. (1951). *Field Theory in Social Science: Selected Theoretical Papers*. Michigan: Harper.

Mintzberg, H. (2010, 4ª ed.). *Estrutura e Dinâmica das Organizações*. Alfragide: Dom Quixote.

Mozzicafreddo, J., & Gomes, S. (2011). *Projectos de Inovação na Gestão Pública.* Lisboa: Mundos Sociais.

Pollitt, C. (Jan-Mar de 2010). *Rumo a uma nova estrutura de Gestão Pública no século 21*. (ENAP, Entrevistador)

Pollitt, C., & Bouckaert, G. (2004). *Public Management Reform: a Comparative Analysis.* Oxford: Oxford University Press.

Rocha, J. A. (2009). *Gestão Pública e Modernização Administrativa.* Oeiras: INA.

TRATAMENTO DE DADOS PESSOAIS
POR FORÇAS E SERVIÇOS DE SEGURANÇA, OPC E AUTORIDADES JUDICIÁRIAS
(LEI 59/2019)

MANUEL GOMES FERREIRA
Consultor em Segurança da Informação
Mestre em Direito e Segurança
Presidente do Observatório de Segurança Interna

A protecção de dados pessoais tem vindo a estar cada vez mais na ordem do dia, tornando-se, ao longo dos últimos quatro anos, um dos mais frequentes e relevantes temas de discussão no domínio do Direito — não só no plano teórico, mas também no que respeita à aplicação prática nas empresas e em todas as organizações que, de alguma forma, procedam ao tratamento de dados pessoais.

Quanto à actuação das autoridades que se encarregam da salvaguarda da segurança pública e da prevenção de ameaças que a perturbem, temos, no ordenamento jurídico nacional, a Lei 59/2019 (que resulta da transposição da Directiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016[1]) que regula a protecção das pessoas singulares no âmbito do tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, detecção, investigação ou repressão de infracções

1 DIRECTIVA (UE) 2016/680 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de Abril de 2016, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infracções penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

penais ou de execução de sanções penais.

Neste momento civilizacional em que os dados (também os pessoais) assumem tão grande e crescente relevância, parece-nos pertinente e atempado reflectir sobre o papel dos actores visados nesta Lei 59/2019 no que concerne ao tratamento de informações pessoais dos cidadãos, que estão cada vez mais conscientes dos seus direitos e de como os exercer.

Com este breve estudo, propomo-nos analisar a forma como a Lei 59/2019 pode produzir alterações nos meios de investigação, detecção e repressão de infracções penais, e se estas mudanças trazem, ou não, mais protecção aos cidadãos no que respeita à privacidade e aos direitos à protecção de dados.

São ainda objecto deste estudo as capacidades e as valências técnicas e organizacionais das autoridades, tais como as forças e os serviços de segurança, os órgãos de polícia criminal, as autoridades judiciárias e os serviços prisionais, e a adequação das suas respostas aos requisitos legais enunciados na referida lei.

Por último, faremos aqui uma análise transversal à Lei 59/2019 considerando a sua origem na Directiva (EU) 2016/680.

LIMITAÇÕES E EXCLUSÕES

Após análise do objecto e do âmbito da aplicação da presente lei, poderá parecer que a sua aplicação resulta num regime demasiado restritivo para que as autoridades possam agir na persecução das respectivas atribuições.

No que respeita à matéria da protecção de dados, esta tem sido uma resposta recorrente a desfavor da aplicação do Regulamento (UE) 2016/679[2], também conhecido como RGPD[3]. É muitas vezes repetida a noção de que

2 REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de Abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Directiva 95/46/CE (Regulamento Geral sobre a Protecção de Dados)

3 Regulamento Geral sobre a Protecção de Dados

o RGPD veio proibir ou limitar o tratamento dos dados pessoais, prejudicando o normal funcionamento das organizações.

Ora, este argumento deve ser contrariado por não ser nem preciso nem correcto. A Directiva 2016/680 e o Regulamento 679/2016, pertencentes ao mesmo pacote legislativo, têm o objectivo principal de garantir a segurança e a licitude no tratamento dos dados de pessoas singulares, independentemente da entidade que trata os dados, devendo esta fazê-lo atendendo a que está a lidar com um direito fundamental.

Uma das razões pelas quais os dados pessoais são muitas vezes encarados como produtos que se podem comercializar sem o controlo dos titulares é, precisamente, o facto de não se cumprir o princípio básico de os tratar como se esse tratamento fosse, porque assim é, uma resposta a um direito fundamental consagrado em vários documentos legais, tais como:

- a Carta dos Direitos Fundamentais da União Europeia (Artigo 8.º, n.º 1)

- o Tratado sobre o Funcionamento da União Europeia — TFUE (Artigo 16.º, n.º 1) estabelece que todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito;

- a Constituição da República Portuguesa (Artigo 34.º — Inviolabilidade do domicílio e da correspondência, e Artigo 35.º — Utilização da informática), que asseguram as bases legais da privacidade e do direito à informação pessoal na nossa Constituição.

Sendo um facto que a protecção dos dados pessoais é um direito fundamental, põe-se, no entanto, que as autoridades a quem compete assegurar a segurança interna não podem estar limitadas no desempenho das suas atribuições, surgindo a dificuldade de equilibrar o objectivo da segurança com o cumprimento das leis impostas por um Estado de direito.

Como não poderia deixar de acontecer, a Lei 59/2019 estabelece esse equilíbrio recorrendo a um conjunto de exclusões que possibilita, conjugando, o exercício das normais responsabilidades das autoridades competentes com

o cumprimento das leis: como podemos observar no n.º 2 do Artigo 2.º, esta lei não se aplica ao tratamento de dados pessoais relacionados com a Segurança Nacional.

Neste ponto, importa atentar ao conceito de segurança nacional tal como referido na Lei 59/2019: se considerarmos que a segurança nacional, de uma forma simplificada, é uma cúpula amparada por quatro pilares que a sustentam, a saber, a segurança do Estado (SIRP[4] – SIS[5] + SIED[6]), a defesa nacional (Exército + Marinha + Força Aérea), a segurança interna (PSP[7] + GNR[8] + SEF[9] + PJ[10]), e a segurança humana (ANEPC[11]), podemos facilmente perceber que existe, no termo «segurança nacional» tal como usado na lei em questão, um potencial motivo de equívoco, uma incompatibilidade aparente, que reside no facto de a lei em análise visar precisamente regular o tratamento de dados pessoais para efeitos de prevenção, detecção, investigação ou repressão de infracções penais ou de execução de sanções penais.

Se consideramos o pilar da segurança interna como uma das componentes da segurança nacional, sendo que são justamente as entidades envolvidas na salvaguarda da segurança nacional as mais visadas na presente lei, ficariam excluídas do âmbito de aplicação as forças de segurança tais como a PSP ou a GNR, o que obviamente não faz sentido.

Dada a normal interpretação do termo em questão, talvez o mais acertado fosse definir «segurança nacional» considerando que se exclui a defesa nacional, a cargo do EMGFA[12].

4 Sistema de Informações da República Portuguesa

5 Serviço de Informações de Segurança

6 Serviço de Informações Estratégicas de Defesa

7 Polícia de Segurança Pública

8 Guarda Nacional Republicana

9 Serviço de Estrangeiros e Fronteiras

10 Polícia Judiciária

11 Autoridade Nacional de Emergência e Protecção Civil

12 Estado-Maior-General das Forças Armadas

TRANSFERÊNCIA DE DADOS

Como refere a Lei 59/2019: o intercambio de dados pessoais entre autoridades competentes na União Europeia, quando legalmente exigido, não é limitado nem proibido por razões relacionadas com a protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

Significa isto que os compromissos internacionais de cooperação assumidos entre países e com entidades congéneres na persecução dos interesses de prevenção de ameaças à segurança pública continuam assegurados.

É disso exemplo o Sistema de Informação Schengen[13], que, enquanto sistema de informação, permite às autoridades nacionais responsáveis controlar um espaço sem fronteiras e emitir alertas sobre pessoas procuradas, ou fornecer informações sobre pessoas que não têm direito de acesso ou permanência no espaço Schengen, ou sobre pessoas desaparecidas procuradas no âmbito de ilícitos criminais ou ainda sobre objectos, tais como veículos e documentos roubados.

É importante salientar que este tipo de cooperação entre Estados não é prejudicado pela aplicação da Lei 59/2019, ainda que esteja previsto e assegurado um conjunto de direitos que os titulares de dados têm e podem exercer.

Num panorama de ameaças transnacionais que inquietam os Estados em diversas plataformas, considerando o aumento de casos de cibercrime de ano para ano, a cooperação policial, bem como a partilha de informações, assume uma importância vital. Um dos desafios perante a enorme proliferação e partilha de informação pelas várias redes sociais e similares, é poder, em consonância com as leis e com os direitos fundamentais, munir as forças e os serviços de segurança com ferramentas e possibilidades de actuação neste campo sem fronteiras físicas chamado ciberespaço[14].

13 SIS II (2.ª geração)

14 Segundo Pierre Lévy, *Cibercultura, Epistemologia* e *sociedade,* Instituto Piaget, Lisboa, 2000. p. 16, o ciberespaço é um novo espaço de comunicação proporcionado pela interconexão mundial de computadores e das memórias dos computadores. Incluindo aí todos os sistemas de comunicação electrónica que transmitem informações oriundas de fontes digitais ou que sejam destinadas à digitalização.

As leis da protecção de dados têm de ser um complemento à garantia de controlo dos dados dos titulares e à sua privacidade, não uma limitação ao exercício das funções e atribuições das forças e dos serviços de segurança, como está, de resto, patente na Lei 59/2019.

As autoridades públicas e os poderes públicos que tenham como atribuições e competências a prevenção, a detecção, a investigação e a repressão de ameaças à segurança pública, não estão limitadas pela presente lei no que respeita à persecução da sua actividade.

Contrariamente ao que sucede com o conceito de segurança nacional, anteriormente mencionado, outro muito importante é o que entendemos por «autoridades competentes». Neste caso, o legislador foi claro e esclarece que

> *« […] são autoridades competentes as forças e os serviços de segurança, os órgãos de polícia criminal, as autoridades judiciárias e os serviços prisionais e de reinserção social, no âmbito das suas atribuições de prevenção, detecção, investigação ou repressão de infracções penais ou de execução de sanções penais, nos termos previstos nos respectivos estatutos e nas leis de segurança interna, de organização da investigação criminal e do processo penal.»*[15]

PRINCÍPIOS DA PROTECÇÃO DE DADOS

Para que o tratamento de dados pessoais possa ser efectuado no estrito respeito pelos direitos, pelas liberdades e pelas garantias das pessoas singulares, há que ter em conta um conjunto de princípios que devem ser cumpridos e praticados. O tratamento de dados deve ocorrer:

- de forma licita e leal;
- para finalidades determinadas e explicitas;

15 Forças e serviços de segurança, os órgãos de polícia criminal, as autoridades judiciárias e os serviços prisionais e de reinserção social.

- na medida do estritamente necessário para as finalidades definidas;

- conservando a informação pelo tempo necessário às finalidades determinadas aquando da recolha dos dados;

- adoptando todas as medidas de segurança associadas que garantam a exactidão e integridade da informação.

As autoridades competentes que sejam tidas como responsáveis pelo tratamento, e sê-lo-ão quando sejam estas a definir os meios e as finalidades do tratamento de dados, ou que sejam identificadas pela Lei como tal, devem cumprir os princípios enunciados, bem como ser capazes de enunciar as medidas adoptadas que demonstrem que cumprem os requisitos legais em matéria de protecção de dados.

No concernente aos princípios gerais da protecção de dados elencados atrás, além da necessidade de se garantir a licitude e lealdade no tratamento, refere-se que os dados devem ser recolhidos para finalidades determinadas, não podendo ser utilizados para finalidades diferentes daquela determinada inicialmente.

Ora, no âmbito da investigação criminal e da cooperação entre entidades que prosseguem fins de segurança (forças e serviços de segurança), é muitas vezes fundamental o seguimento de pistas e dados que podem não ser relevantes numa determinada fase da investigação, mas que podem ser fundamentais numa fase posterior.

Também no que toca ao prazo de conservação da informação contendo dados pessoais, o que está estipulado é que deve respeitar-se e garantir-se que estes são guardados apenas durante o período estritamente necessário à conclusão das finalidades pré-definidas, o que pode levantar obstáculos, designadamente quando se tenha de eliminar dados que poderão ser importantes no futuro. O responsável pelo tratamento deverá avaliar o impacto que poderá ter a conservação de dados cuja finalidade foi concluída, para efeitos de prova, investigações, inquéritos, ou de processos judiciais, em relação aos riscos para os direitos, as liberdades e as garantias das pessoas singulares.

LICITUDE DO TRATAMENTO

As autoridades competentes[16] encarregues de assegurar a licitude do tratamento de dados pessoais têm de garantir a aplicabilidade de pelo menos uma das premissas abaixo.

- O tratamento de dados pessoais está previsto na Lei, ou esta estipula as medidas em que o tratamento de dados é necessário para o exercício de uma atribuição da autoridade competente.

- A Lei indica, pelo menos, os objectivos do tratamento, os dados pessoais a tratar e as finalidades do tratamento.

- Caso não esteja autorizado pela Lei, o tratamento dos dados pessoais apenas pode ser realizado se for necessário para a protecção dos interesses vitais do titular dos dados ou de outra pessoa singular.

TRATAMENTO DE CATEGORIAS ESPECIAIS DE DADOS

O Artigo 6.º refere-se, com especial enfoque, aos dados sensíveis, cujo tratamento em circunstâncias menos prudentes pode acarretar um elevado risco para as liberdades e garantias dos titulares.

O tratamento de dados pessoais que revelem origem racial ou étnica, opiniões politicas, convicções religiosas ou filosóficas ou filiação sindical, dados genéticos, dados biométricos que identificam uma pessoa singular de forma inequívoca, dados relativos à saúde, ou de dados relativos à vida sexual ou à orientação sexual, só pode ser efectuado se for estritamente necessário, se estiver sujeito a garantias adequadas de protecção dos direitos e liberdades do titular dos dados, e se:

- for autorizado por lei;

- se se destinar a proteger os interesses vitais do titular dos dados ou

16 Artigo 29º, n.º 1, da Lei 59/2019 — No caso de um certo tipo de tratamento ser susceptível de representar um elevado risco para os direitos, as liberdades e as garantias das pessoas, o responsável pelo mesmo deve efectuar uma avaliação do impacto das operações que o compõem antes de lhe dar início.

de outra pessoa singular;

- estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados.

São ainda proibidas as definições de perfis que conduzam à discriminação de pessoas singulares com base nas categorias especiais de dados pessoais previstos no número anterior.

No Artigo 9.º é mencionado que deve ser feita uma distinção entre categorias de titulares de dados sempre que possível (e se aplicável) entre as pessoas sobre as quais se conhecem motivos fundamentados para crer que cometeram ou que estão prestes a cometer um crime das pessoas condenadas pela prática de infracção penal, vítimas, potenciais vítimas ou terceiros envolvidos como testemunhas.

Ora, esta situação pode propiciar a definição de perfis que, como referido anteriormente, é proibida. É nestas situações que terão de ser feitas avaliações de impacto às operações que se pretende levar a cabo. Para fazer uma distinção entre categorias, por exemplo, entre dados de identificação e dados onde se revelem informações de saúde ou relativas a convicções políticas ou religiosas, podem estar, concomitantemente, a gerar-se perfis de pessoas singulares com informação pertencente às categorias especiais de dados.

No Artigo 7º. refere-se a possibilidade de utilização dos dados para finalidades diferentes das definidas inicialmente, nas situações em que seja necessário e proporcional. A questão que se levanta é: quem avalia essa pertinência e essa necessidade?

Os mecanismos estão previstos principalmente recorrendo às já referidas avaliações de impacto. No entanto, as estruturas de funcionamento das forças de segurança não evidenciam, actualmente, uma aptidão para este tipo de avaliação estruturada e documentada. Outra das dificuldades será o logro de o fazer antes de tratar a informação tal como a Lei prevê[17].

17 Comissão Nacional de Protecção de Dados — É a autoridade incumbida de assegurar a garantia e a fiscalização do cumprimento da presente lei.

Esta subjectividade pode causar impasse na adopção de medidas de acordo com a Lei 59/2019. Alguns termos utilizados, tais como «sempre que possível» podem ser alvo de interpretações variadas e até díspares.

Nesta lei encontramos indicações claras como «Não podem ser transmitidos nem disponibilizados dados pessoais inexactos, incompletos, desactualizados ou não confiáveis». Mas encontramos também outras ambíguas como «Para os efeitos previstos no número anterior, as autoridades competentes verificam, sempre que possível, a qualidade dos dados pessoais antes de estes serem transmitidos ou disponibilizados». Uma vez mais a questão é: quem avalia, quem documenta e quem decide? A lei é clara: será o responsável pelo tratamento. No entanto, a experiência diz-nos que na prática será muito difícil verificar o cumprimento destes procedimentos.

MEDIDAS DE SEGURANÇA DA INFORMAÇÃO

As autoridades competentes devem utilizar sistemas informáticos que facilitem a avaliação periódica da necessidade de conservar os dados e o seu apagamento ou pseudonimização. Devem também manter registos das actividades de tratamento de dados, tais como de recolha, alteração, consulta, divulgação, ou apagamento, que podem ser solicitados pela CNPD[18].

Quer o tratamento de dados seja efectuado em formato físico quer o seja em formato digital, o responsável pelo tratamento deve garantir a adopção de medidas técnicas e organizativas que impeçam:

- o acesso de pessoas não autorizadas;
- que os suportes de dados sejam lidos, copiados, alterados ou retirados sem autorização;
- a introdução não autorizada de dados pessoais.

E que assegurem:

18 Comissão Nacional de Protecção de Dados — É a autoridade incumbida de assegurar a garantia e a fiscalização do cumprimento da presente lei.

- que as pessoas autorizadas a utilizar um sistema de tratamento automatizado só tenham acesso aos dados pessoais abrangidos pela sua autorização de acesso;

- que possa ser verificado e determinado a que organismos os dados pessoais foram ou podem ser transmitidos ou facultados utilizando equipamento de comunicação de dados;

- que possa ser verificado e determinado a posteriori quais os dados pessoais introduzidos nos sistemas de tratamento automatizado, e quando e por quem foram introduzidos;

- que os sistemas utilizados possam ser restaurados em caso de interrupção.

No que respeita às forças de segurança, a utilização do Sistema Estratégico de Informações (SEI) actualmente em uso, corresponde à maioria das exigências antes referidas, ainda que não na totalidade. É recomendável a execução de uma análise cuidada de forma a fazer corresponder os requisitos descritos na Lei e os sistemas utilizados pelas autoridades. O relacionamento e a cooperação próxima com a Comissão Nacional de Protecção de Dados na avaliação das plataformas utilizadas no tratamento de dados pessoais pelas autoridades competentes pode ser fundamental.

ENCARREGADO DA PROTECÇÃO DE DADOS

Exceptuando os tribunais e o Ministério Público, todas as autoridades envolvidas na prevenção, detecção, investigação ou repressão de infracções penais ou de execução de sanções penais têm de designar um Encarregado da Protecção de Dados (EPD).

Este será porventura um dos assuntos menos desenvolvidos, já que nos referimos a uma figura / função que não existia no anterior quadro jurídico, e que tem como missão auxiliar o responsável pelo tratamento a controlar o cumprimento das obrigações decorrentes da presente lei.

A lei prevê um conjunto de condições / garantias na designação do EPD.

- O EPD não recebe instruções relativamente ao exercício das suas funções e não pode ser destituído nem penalizado pelo facto de as exercer, isto para que possa manter a sua independência e autonomia na emissão de pareceres.

- O EPD não está impedido de exercer outras funções, desde que o responsável pelo tratamento ou o subcontratante assegurem que do tal exercício de outras funções não resulta um conflito de interesses.

Torna-se, assim, evidente que ninguém pertencente à cadeia de comando ou de chefia das autoridades competentes pode exercer esta função, uma vez que estaríamos perante um manifesto conflito de interesses.

CONCLUSÕES

Podemos considerar que as forças e os serviços de segurança saberão, como de resto souberam noutras ocasiões, acomodar as suas actividades às exigências legais, e que o farão com maior ou menor dificuldade — este será também um desígnio a médio-longo prazo que terá os seus próprios resultados.

Conclui-se ainda que as plataformas informáticas utilizadas devem ser desenvolvidas e / ou adaptadas aos novos requisitos que vão aparecendo com os novos desafios tecnológicos.

De resto, caberá à autoridade de controlo, a CNPD, a fiscalização e o apoio no desenvolvimento dos conceitos e das práticas em matéria de protecção de dados, que sofreu, nos últimos anos, mudanças significativas.

ENTREVISTA

MANUEL PEDROSA DE BARROS

2021.01.25

1. Num mundo em que as telecomunicações se aproximam das tecnologias de informação e comunicação, como se gerem os novos desafios de segurança das comunicações?

A propósito do novo Código Europeu para as Comunicações Eletrónicas (CECE) destacam-se dois aspetos, a saber: a atualização do conceito de comunicações eletrónicas, passando a abranger, entre outros, os serviços de transmissão utilizados para a prestação de serviços máquina a máquina, bem como o facto de terminar com um vazio existente no anterior quadro regulatório ao estabelecer explicitamente uma definição para «Segurança das redes e dos serviços», designadamente, *a capacidade das redes e serviços de comunicações eletrónicas para resistir, com um dado nível de confiança, a ações que comprometam a disponibilidade, a autenticidade, a integridade ou a confidencialidade dessas redes e serviços, dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou serviços de comunicações eletrónicas, ou acessíveis através deles.*

As disposições do CECE em matéria de segurança das redes e dos serviços são, na sua maioria, muito semelhantes às anteriores, havendo a assinalar algumas diferenças: a inclusão, nas medidas técnicas e organizacionais a

adotar, da encriptação; o estabelecimento de novos parâmetros para a determinação da importância do impacto de um incidente de segurança e a obrigação de informação pelos fornecedores de redes ou serviços aos seus utilizadores, potencialmente afetados por uma ameaça específica e grave, das eventuais medidas de proteção ou das soluções que os utilizadores podem adotar.

Posteriormente à adoção a nível europeu do CECE, regista-se novo desenvolvimento, com impacto significativo em matéria de segurança das redes e serviços com a preocupação em redor das redes 5G. Assim, no contexto da execução de procedimentos para a concessão de direitos de utilização nas faixas do espetro de radiofrequências designadas para as redes 5G, os Estados Membros manifestam ter preocupações quanto aos potenciais riscos de segurança relacionados com estas redes, designadamente com respeito à cadeia de fornecimento dos operadores de redes móveis; em razão de que acordam, com a colaboração da Comissão Europeia, em apoiar o desenvolvimento de uma abordagem da União Europeia destinada a garantir a cibersegurança daquelas redes, ver Recomendação (UE) 2019/534 da Comissão, de 26 de março, relativa à Cibersegurança das redes 5G[1].

Importa realçar que, na mencionada abordagem aos riscos, são tomados em consideração um conjunto de fatores técnicos e de outra ordem.

No respeitante a fatores técnicos incluem-se vulnerabilidades de cibersegurança que possam ser exploradas por ações de ciberespionagem (económica ou política) ou por ciberataques.

Quanto aos outros fatores incluem-se requisitos regulamentares ou outros, impostos aos fornecedores de equipamentos, cuja avaliação deve ter em conta, entre outros, o risco global de influência de um país terceiro, a luta contra a cibercriminalidade e a proteção de dados.

Em paralelo com os aspetos acima mencionados há, obviamente intrinsecamente associados aos mesmos, outros: a evolução das tecnologias ao nível das redes, de que são exemplo o incremento de soluções baseadas

1 Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019H0534&from=EN

em programas e a virtualização de funções de rede e a necessidade de criar condições que sejam atrativas para que se proceda a novos investimentos que reforcem a resiliência das redes e serviços e que, em simultâneo, potenciem a inovação e o desenvolvimento económico.

Neste enquadramento, a gestão dos desafios de segurança das comunicações tem, necessariamente, de ser feita de uma forma integrada e cooperativa e proativa, envolvendo os agentes, empresas e entidades públicas que intervêm em todo o ecossistema. Integrada, pois é necessário desenvolver soluções que incorporem os diversos tipos de perspetivas presentes. Cooperativa, pois que carecem da construção de processos e de mecanismos eficazes de partilha de informação para que as ações a desenvolver atinjam os objetivos, específicos e transversais, de redução dos riscos e dos seus impactos. E proativa pois há sempre que avaliar transversalmente, corrigir prontamente e inovar permanentemente.

A evolução das redes de comunicações eletrónicas, de que a quinta geração é um exemplo, vem enriquecer este ecossistema e, também, alargar o âmbito de prestação de serviços a novos utilizadores. Em termos do novo ecossistema surgem, por exemplo, os prestadores de serviços em nuvem, desenvolvendo a sua atividade a partir de centros de dados localizados na periferia das redes e criando uma oferta de novos serviços, tornados possíveis devido às caraterísticas das futuras redes, nomeadamente pela redução do tempo de latência. Em termos de novos utilizadores temos, por exemplo, as empresas e os organismos públicos que irão recorrer às redes de comunicações eletrónicas para suportar os seus processos de automação industrial e de transformação digital. Observe-se os casos de utilização ao nível do setor dos transportes ou da saúde bem como de outros setores económicos ou o desenvolvimento das cidades inteligentes.

Nesta medida, as aproximações regulatórias à segurança das comunicações têm que ter uma abrangência europeia e nacional que passam pela criação de fóruns de partilha de informação, nos quais participem representantes de entidades, públicas e privadas, nacionais e europeias, bem como, pelo estabelecimento e reforço da articulação destes com outras partes interessadas, nomeadamente de empresas de outros setores e das respetivas autoridades competentes, incluindo outros reguladores. Estes fóruns de-

vem permitir a construção e atualização de cenários de ameaça, realistas, e o desenvolvimento de novas competências e de novos processos.

Finalmente, julgo ser de assinalar, uma última nota: em consequência do modo como se estão a colocar as recentes medidas de cibersegurança, a gestão destes novos desafios assenta, por um lado, numa base de avaliação e de teste técnico e experimental, incluindo a realização de ensaios, e, por outro, em componentes ligadas à normalização técnica, à inovação e ao desenvolvimento da capacidade industrial. Sendo que em todo este processo haverá que assegurar o respeito pelo cumprimento dos requisitos de privacidade e de proteção de dados pessoais a par da capacidade de realização de funções essenciais, incluindo a interceção legal pelas autoridades competentes e o suporte a situações de emergência.

2. Qual o papel do regulador das comunicações no desenho futuro de supervisão e gestão dos riscos de segurança associados às redes de quinta geração?

Neste processo o papel do regulador é determinante: para a melhoria da informação de segurança das redes e serviços que é disponibilizada aos cidadãos, às empresas e às outras autoridades competentes, para a criação de condições que permitam reforçar as características de resiliência das redes e serviços (em termos de cada rede ou serviço e, também, no seu conjunto) e, simultaneamente, para a promoção do desenvolvimento e da adoção de soluções inovadoras em matéria de segurança das redes e serviços.

Para que tal seja possível de concretizar haverá que produzir um conjunto de transformações em termos da atividade de supervisão e de gestão dos riscos as quais se podem equacionar ao nível da automação e da transformação digital destas atividades, nomeadamente por desenvolvimento de novos sistemas de informação, incluindo de informação geográfica, e dos interfaces eletrónicos adequados com as entidades que integram o ecossistema.

Adicionalmente, haverá que criar capacidades de simulação para suporte à realização de simulacros e à avaliação de cenários, bem como, promover

o estabelecimento de, ou em alternativa facilitar o acesso das empresas a infraestrutura laboratorial para a realização de ensaios a equipamentos.

A promoção do envolvimento das empresas na normalização técnica e do desenvolvimento de soluções de inovação tecnológica em matéria de segurança das redes e serviços, bem como o estudo das condições do mercado a montante das comunicações eletrónicas para perceber as condições de funcionamento da cadeia de fornecimento serão outros aspetos a considerar.

3. Declarações de um membro do Governo a propósito da implementação da *toolbox* europeia para as redes de quinta geração apontam no sentido da implementação de "mecanismos de avaliação contínua de risco e de certificação dos equipamentos que a compõem". Que mecanismos podem ser esses e quais os modelos de certificação?

Mecanismos de Avaliação Contínua de Risco

A avaliação de risco que se realizou pela primeira vez em 2019 é válida desde que se mantenham as condições de base subjacentes designadamente: que não haja alteração em termos dos ativos abrangidos, que estes ativos tenham as mesmas vulnerabilidades e, finalmente, que o cenário de ameaça considerado se mantenha o mesmo.

Para além de que se está numa perspetiva em grande parte prospetiva, cada uma das dimensões a considerar, para efeitos de avaliação de risco, é sujeita a uma evolução permanente, pelo que o seu conjunto será ainda mais dinâmico.

A avaliação é resultado de um processo de cooperação para o qual contribuem diversas entidades, o qual importa solidificar e enriquecer com as experiências realizadas a nível nacional e europeu.

A eficácia das medidas de segurança depende do âmbito, da profundidade e da atualização da avaliação de risco pelo que é fundamental que seja assegurada a revisão e atualização da avaliação de risco o que lhe confere um requisito de continuidade.

Mecanismos de Certificação dos Equipamentos

Algumas das medidas europeias para o 5G baseiam-se no desenvolvimento e no estabelecimento de um sistema europeu de certificação em matéria de cibersegurança a equipamentos de tecnologias de informação e de comunicação (TIC), conforme disposto no Regulamento Cibersegurança[2], o qual estabelece, entre outros, *um enquadramento para a criação de sistemas europeus de certificação da cibersegurança com o objetivo de assegurar um nível adequado de cibersegurança para os produtos, os serviços e os processos de TIC na União e de evitar a fragmentação do mercado interno no que toca aos sistemas de certificação da cibersegurança na União*[3].

Atendendo à recente publicação deste Regulamento, as ações em curso a nível europeu, nomeadamente pela ENISA, têm por foco a preparação para a posterior operacionalização daqueles sistemas. Estas ações passam, entre outras, pela identificação e, nalguns casos, pelo desenvolvimento das normas técnicas e procedimentos a adotar para efeitos de avaliação de conformidade dos equipamentos e das linhas de produção, bem como pelo envolvimento e caraterização dos requisitos de acreditação das entidades participantes, nomeadamente para realização de testes. A nível nacional estas ações são coordenadas pelo Centro Nacional de Cibersegurança.

No respeitante às medidas europeias para o 5G[4], importa conhecer como o mecanismo de certificação, específico para 5G, irá ser concretizado tendo em vista a melhoria da segurança destas redes. Neste sentido, as medidas apontam para que aos operadores de redes 5G seja fixada uma obrigação de que a aquisição e posterior colocação em serviço de equipamentos, nas respetivas redes, fique condicionada a que estes detenham a certificação adequada, em conformidade com o que vier a ser definido no âmbito do mencionado mecanismo de certificação europeu. Por outro lado, assegurar

2 Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.o 526/2013 (Regulamento Cibersegurança)

3 Neste contexto, os certificados emitidos no âmbito destes sistemas/mecanismos de certificação serão válidos em todos os Estados Membros da União Europeia.

4 Ver caixa de ferramentas disponível em https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

a obtenção e a manutenção da certificação dos equipamentos será da responsabilidade dos seus fabricantes.

Importa, neste ponto, clarificar os motivos e os objetivos que determinam a criação e a adoção de mecanismos de certificação.

Em termos gerais, o estabelecimento de mecanismo de certificação, designadamente naqueles em que a certificação é voluntária, tem por objetivo a criação de condições de confiança tipicamente associadas a uma marca de reconhecida qualidade na base da qual se podem estabelecer estratégias de diferenciação.

No caso do modelo de certificação ter um cariz obrigatório (objetivo pretendido pelas medidas europeias para a cibersegurança do 5G), resultante da fixação de uma imposição legal, pretende-se fundamentalmente a verificação de requisitos que se consideram por algum motivo ser essenciais.

A título de exemplo, no quadro regulatório atualmente aplicável à disponibilização no mercado e à colocação em serviço de equipamentos de rádio[5], os requisitos essenciais, previstos, dizem respeito à sua construção e dividem-se em dois tipos, a saber: aplicáveis a todos os equipamentos ou somente aplicáveis a certas categorias ou classes. Quanto ao segundo caso a sua fixação depende de decisão específica, feita já durante a vigência do regime, quanto à classe em concreto, nos termos da qual se determina quais os requisitos que se consideram ser de adotar, de entre uma lista pré-estabelecida. No primeiro caso, os requisitos aplicáveis a todos os equipamentos são relativos à proteção da saúde e da segurança das pessoas e dos animais domésticos, à compatibilidade eletromagnética e à utilização eficiente do espetro de radiofrequências, a fim de evitar interferências nocivas.

O estabelecimento de um mecanismo de certificação obrigatória tem sempre impactos diversos na estrutura e funcionamento do mercado ou

5 Decreto-Lei n.º 57/2017, de 9 de junho, estabelece o regime da disponibilização no mercado, da colocação em serviço e da utilização de equipamentos de rádio, transpondo para a ordem jurídica interna a Diretiva n.º 2014/53/UE do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos de rádio no mercado.

mercados afetados. A decisão que determina a sua criação e adoção tem de pesar por um lado os benefícios e, por outro, os custos daí resultantes, baseando-se em que as regras de funcionamento do mercado não asseguram que determinadas condições se verifiquem.

No caso concreto, das alterações no respeitante à estrutura e funcionamento do mercado podemos realçar dois aspetos.

Por parte dos operadores haverá que garantir que, nos processos de aquisição, os equipamentos são certificados, o que garante que o equipamento adquirido esteja em conformidade com as especificações/normas/regras técnicas específicas adotadas.

Por parte das empresas que se posicionem enquanto possíveis fornecedores de equipamento (inclui hardware, programas e aplicações) ou prestadores de serviço aos operadores de redes 5G, o acesso ao mercado fica condicionado à obtenção da certificação, o que constitui, na prática, uma barreira à entrada com todas as consequências daí decorrentes, nomeadamente em termos das caraterísticas dinâmicas de funcionamento do mercado, caso da inovação, e de dificuldades acrescidas para as empresas de menor dimensão.

Em compensação, é típico que, associada à decisão de estabelecer um regime de certificação obrigatória, seja promovida a criação de condições que facilitem o acesso das empresas, fabricantes e operadores, em especial empresas de menor dimensão, a uma infraestrutura laboratorial de base, devidamente acreditada, para a realização dos testes e ensaios aplicáveis.

A explicação que antecede é válida para os cenários em que o produto ou serviço certificado não sofre alterações significativas nas suas características após a sua colocação no mercado ou colocação em serviço, na sequência da respetiva instalação.

Todavia, o mesmo já não se verifica, para a maioria dos atuais equipamentos de tecnologias de informação e comunicação, nestes se incluindo o equipamento de comunicações eletrónicas, cujas caraterísticas e funcionalidades são determinadas pelo software instalado, o qual se mantem em evolução permanente ao longo de todo o ciclo de vida do equipamento, designada-

mente após a instalação e colocação em serviço.

Em consequência, neste caso em concreto, existirão alterações adicionais, nomeadamente, ao nível da relação entre o operador de rede 5G, por um lado, e os fabricantes e os prestadores de serviço, presentes na cadeia de fornecimento daquele, por outro, do envolvimento das entidades em que se baseia a avaliação de conformidade, e, em especial, em que medida esta relação é objeto da supervisão das autoridades competentes.

4. Essa certificação seria válida apenas em Portugal, ou será criado um mecanismo de certificação europeia?

O objetivo é que o mecanismo de certificação a criar produza certificados válidos em todos os Estados Membros.

5. O país de origem de um fornecedor de equipamento pode ser um critério a ter em conta na definição dos requisitos de segurança das redes de comunicações? Se sim, esse critério abrangeria o país de origem do fabricante ou o país onde o equipamento é fabricado?

Se não me parece que faça sentido o critério do país de origem no respeitante a certificação de produto, medidas TM09 e TM11, já o mesmo poderá não ser o caso em termos da implementação da medida SM03 da caixa de ferramentas europeia para a cibersegurança das redes 5G[6], para a determinação do que é um fornecedor de alto-risco na qual se faz ligação ao que no relatório europeu de avaliação de risco[7], se considera no parágrafo 2.37, que se transcreve:

- The risk profiles of individual suppliers can be assessed on the basis of several factors, notably:

- *The likelihood of the supplier being subject to interference from a non-EU country. This is one of the key aspects in the assessment of non-technical vulnerabilities related to 5G networks. Such interference may be facilitated by, but not limited to, the presence of the following factors:*

6 Disponível em https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

7 Disponível em https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

- *a strong link between the supplier and a government of a given third country;*

- *the third country's legislation, especially where there are no legislative or democratic checks and balances in place, or in the absence of security or data protection agreements between the EU and the given third country;*

- *the characteristics of the supplier's corporate ownership;*

- *the ability for the third country to exercise any form of pressure, including in relation to the place of manufacturing of the equipment.*

- *The supplier's ability to assure supply.*

- *The overall quality of products and cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to security practices.*

A resposta concreta à questão colocada quanto à definição de requisitos de segurança das redes de comunicações vai depender, nomeadamente, do que ficar disposto na legislação de comunicações eletrônicas que irá proceder à transposição do Código Europeu das Comunicações Eletrónicas.

6. Em declarações à imprensa, em Fevereiro de 2020, salientou o tema da diversificação de fornecedores. Em que poderá consistir essa diversificação?

A caixa de ferramentas europeia de mitigação de risco de cibersegurança das redes 5G, apresenta um conjunto de medidas, divididas em oito medidas estratégicas (SM01 a SM08) e onze medidas técnicas (TM01 a TM11).

No respeitante à cadeia de fornecimento destacam-se três medidas estratégicas, designadamente:

> – (SM03) – *Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risk - including necessary exclusions to effectively mitigate risks- for key assets;*

– (SM05) – *Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies;*

– (SM06) – *Strengthening the resilience at national level;*

Estamos, portanto, perante dois tipos de medidas.

O primeiro tipo de medida (SM03) assenta na possibilidade de identificação de um fornecedor de alto risco. Neste caso a aplicação de regra daí decorrente pode implicar: o afastamento desse fornecedor (fabricante ou prestador de serviço) da cadeia de fornecimento dos operadores de redes 5G, a limitação da autorização de instalação de equipamento desse fornecedor em determinadas partes das redes de 5G e a proibição de fornecimento de equipamento a outros elementos das redes que sejam considerados mais críticos bem como o estabelecimento de quotas máximas de fornecimento de equipamento desse fornecedor para uma determinada rede.

O segundo tipo de medida (SM05 e SM06) tem por objetivo promover a diversificação de fornecedores e, com isso, conseguir reduzir a dependência do funcionamento de uma rede 5G (SM05) de um fornecedor específico. No caso de SM06, a perspetiva é nacional. Tanto SM05 como SM06 são aproximadas sem que haja, necessariamente, determinação de fornecedor de alto risco.

Em fevereiro de 2020 indiquei que, em Portugal, não está identificado nenhum fornecedor de alto risco, situação que se mantém, pelo que, no respeitante à cadeia de fornecimento, as medidas de mitigação de risco que na altura destaquei são as relativas à diversificação de fornecedores, outras há.

No relatório de implementação da caixa de ferramentas, publicado em julho de 2020, é indicado que o estado de maturidade de implementação das medidas SM05 e SM06 é baixo (ver Tabela 1), pese embora ambas serem identificadas entre as medidas de maior eficácia.

A propósito da implementação das medidas SM05 e SM06 o relatório indica:

> – SM05 – *most Member States seems to be in the early stages of implementation of SM05 with about half of the respondents indicating that they have, or are in the progress of implementing measures but a majority have not indicated a time-plan of the implementation;*
>
> – SM06 – *It is the least implemented strategic measure in the Toolbox according to the answers received.*

E conclui que:

> *Many Member States are currently experiencing challenges in designing and imposing appropriate multi-vendor strategies for individual MNOs or at national level, which can be a complex process because of technical or operational difficulties (e.g. lack of interoperability, size of the country).*
>
> *Further work should therefore be done to clarify the parameters of 'appropriate multi-vendor strategies' under SM05, in particular through further exchanges of experiences and best practices within the NIS Work Stream and within BEREC. On this basis, Member States should also assess the need for additional measures to ensure national resilience.*

Em suma a questão é relevante, mas a resposta não é simples e carece de mais estudo. Trata-se da fixação de uma regra que procura defender relevantes interesses públicos mas cuja implementação se torna complexa e tem fortes impactos em termos de mercado. À complexidade técnica da sua implementação, ligada a questões de interoperabilidade entre soluções de diferentes fornecedores e de normalização técnica, aparecem associados outros aspetos a ter em conta tais como a dimensão da rede ou do país e o reduzido número de fornecedores.

A implementação destas medidas, SM05 e SM06, vai obrigar ao aprofundamento da articulação entre os interesses públicos ligados à segurança e à defesa e aos interesses públicos e privados ligados ao desenvolvimento do mercado, sendo esse o motivo porque se dá o envolvimento do BEREC.

Em resultado da ação desenvolvida em 2020, o BEREC publicou um relatório[8] relativo às medidas de diversificação de fornecedores (SM05) e de reforço de resiliência nacional (SM06), cujo sumário executivo é público e no qual se identificam um conjunto de pontos em aberto para os quais haverá que realizar trabalho de aprofundamento, a saber:

- *As a result of producing this report, BEREC has identified a requirement to establish a deeper understanding of specific risk scenarios related to the MNOs full supply chain. The risk scenarios would also take into account supply availability, as well as obstacles and the actions needed to adapt to the global situation in the case that there are disruptions in the supply market.*

- *Additionally, BEREC identifies a requirement to establish a greater understanding of the potential gains and limitations of Open RAN including the likely timeline before it can become a viable approach, as well as the current status of other pilot projects.*

- *Finally, BEREC generally speaking identifies a need for possible further information gathering as well as for a more holistic understanding of the costs and impacts related to implementing various approaches of multi-vendor strategies by MNOs as a measure to mitigate the risk of single-supplier dependency and improve the resilience of network supply chains at the European as well as at the national level.*

7. O contacto com personalidades de governos estrangeiros tem contribuído para moldar a sua perceção relativamente aos temas de segurança ?

No caso do tratamento de uma matéria como é o caso da segurança das redes e serviços de comunicações eletrónicas este contacto internacional é imprescindível, sendo que, com a evolução das redes e dos enquadramentos regulatórios, ainda será mais necessário no futuro.

8 Report of BEREC recent activities concerning the EU 5G Cybersecurity Toolbox Strategic Measures 5 and 6 (Diversification of suppliers and strengthening national resilience), ref. BoR (20) 228, disponível em https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/9726-report-of-berec-recent-activities-concerning-the-eu-5g-cybersecurity-toolbox-strategic-measures-5-and-6-diversification-of-suppliers-and-strengthening-national-resilience

8. A discussão em torno das redes de quinta geração está centrada nas de utilização comercial. Acha que deve ser desenvolvida uma rede de quinta geração específica para os sectores da segurança e defesa? Pode essa rede ser uma evolução do SIRESP?

Julgo que este foco é posto somente porque a evolução para a quinta geração se dará em primeiro lugar nas redes públicas de comunicações eletrónicas. De qualquer modo a evolução das redes de emergência e de segurança está na ordem do dia sendo que a razão de base, típica para tal, se prende com as possibilidades que esta tecnologia oferece de satisfazer os requisitos operacionais de comunicações, que as entidades com atribuições relativas à proteção civil, à segurança e à defesa têm para o desempenho das suas missões.

A avaliação e teste da introdução de soluções 5G no contexto operacional deste tipo de entidades é já uma realidade, pelo que mais cedo ou mais tarde o 5G irá influenciar a evolução do SIRESP. Tal não obsta, porém que, até lá, estas entidades não recorram a serviços específicos possíveis através das redes de quinta geração.

Para além da introdução do 5G no contexto operacional das entidades ligadas à emergência e à segurança há também a questão do modo como esta se irá concretizar.

No caso nacional o modelo que se adotou, até ao momento, baseia-se na existência de uma rede privativa própria, distinta das redes públicas de comunicações eletrónicas.

As razões para este modelo são conhecidas, entre elas está o facto de que o gabarito de resiliência e robustez aplicável a uma rede de emergência e segurança, que deve sobreviver e manter as suas funcionalidades em situações extremas, ser muito superior ao que é tipicamente associado a uma rede pública de comunicações eletrónicas.

Tal não impede, a meu ver, que não se considerem outros cenários e que não sejam exploradas novas formas de articulação entre os dois tipos de redes e novos enquadramentos na procura de soluções que, assegurando

os requisitos de resiliência e robustez, possam trazer outras vantagens, nomeadamente, em termos de evolução tecnológica e de redução de custos. Destaco, a este respeito, um estudo feito em 2014 para a União Europeia intitulado *Is Commercial Cellular Suitable for Mission Critical Broadband?*[9].

9. Quando pensamos em ameaças à integridade das redes de comunicações devemos focar-nos mais na infraestrutura ou nas aplicações?

A resposta à questão é óbvia, temos de nos focar em tudo dando, todavia, prioridade ao que possa implicar um maior impacto. Em tudo, refiro-me a ativos, a vulnerabilidades e a ameaças.

A avaliação de risco feita em 2019 no âmbito da recomendação europeia para a cibersegurança das redes 5G[10], indica quais são os aspetos em que, em termos de ativos, vulnerabilidades e ameaças, os Estados Membros devem focar a sua atenção.

Na evolução para o 5G, o papel do software aumenta. A dependência do bom funcionamento da rede nas aplicações e nos programas é maior. Citando o relatório mencionado:

> *The technological changes introduced by 5G will* ***increase the overall attack surface and the number of potential entry points for attackers:***
>
> > *– **Enhanced functionality at the edge of the network and a less centralised architecture** than in previous generations of mobile networks means that some functions of the core networks may be integrated in other parts of the networks making the corresponding equipment more sensitive (e.g. base stations or MANO functions);*
> >
> > *– **the increased part of software** in 5G equipment leads to increased risks linked to software development and update processes, creates new risks of configuration errors, and gives a more important role in the security analysis to the choices made by each mobile network operator*

9 Disponível em http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=8211

10 Disponível em https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

in the deployment phase of the network.

Julgo, todavia, ser de realçar que alguns dos incidentes de segurança de comunicações de maior impacto foram causados por fenómenos naturais, nomeadamente por tempestades a que estão associados ventos fortes e altos níveis de pluviosidade, provocando fortes danos, inclusive a destruição, nas infraestruturas das redes elétrica e de comunicações eletrónicas. Fenómenos estes cuja tendência sabemos ser de agravamento em resultado das alterações climáticas e que, adicionalmente, muito contribuem para os incêndios florestais, com especial destaque para os ocorridos em 2017.

Em síntese, a perspectiva das aplicações traz-nos as preocupações associadas à evolução tecnológica dos sistemas de informação e à gestão da informação, mas a realidade vai para além disso pois as infraestruturas de rede, que constituem a componente física das redes de comunicações são vulneráveis a fenómenos naturais e a outros de origem humana. Na realidade este é outro dos eixos associados à segurança das redes 5G de que não se vê o reflexo, que julgamos ser devido, na *toolbox* de medidas europeias.

10. Acha proveitosa uma articulação entre Portugal e Espanha na definição dos pressupostos para as redes de quinta geração?

Parece-me que o desenvolvimento de uma boa articulação entre Portugal e Espanha é positivo, mas peca por ser insuficiente. O âmbito da articulação tem necessariamente de ser mais alargado independentemente da perspetiva sob a qual estejamos a analisar o assunto.

Numa perspetiva técnica, a tecnologia é definida e caraterizada a nível global. As normas adotadas pelo 3GPP[11] ou as recomendações da UIT[12] são globais. Adicionalmente as redes de comunicações eletrónicas constituem uma infraestrutura global de informação que se estende muito para além das fronteiras nacionais e, mesmo, europeias – veja-se o caso dos cabos submarinos.

11 3GPP – Third Generation Partnership Project

12 UIT – União Internacional das Telecomunicações

Numa perspetiva de mercado, pese embora sermos membros da União Europeia, as relações comerciais, nas quais se suporta, nomeadamente, o desenvolvimento, a produção, a instalação, a gestão, a manutenção e a exploração das redes de comunicações atuais e, mais ainda das redes de futura geração, envolvem empresas das mais diversas origens. Esta situação é clara assim que começamos a proceder à identificação das entidades que intervêm nas cadeias de fornecimento. Acresce que o ritmo de inovação e, portanto, de desenvolvimento dependem da dinâmica deste sistema global.

Finalmente, numa perspetiva de segurança e defesa o quadro é, necessariamente, estabelecido pelas relações no seio da Organização do Tratado do Atlântico Norte.

Neste contexto a noção de interligação ou de interdependência, numa linguagem mais de segurança, é uma caraterística intrínseca das redes de comunicações eletrónicas pelo que o estabelecimento de uma visão clara do quadro de articulações, necessário, é fulcral.

DESAFIOS DO 5G NA GESTÃO DO RISCO CIBERNÉTICO DAS INFRAESTRUTURAS CRÍTICAS E SERVIÇOS ESSENCIAIS NO CONTEXTO DAS AMEAÇAS HÍBRIDAS

PAULO MIGUEL SANTOS MONIZ
Diretor Segurança da Informação e Risco TI do Grupo EDP
AFCEA Portugal Cyber Committee Member
IntellCorp Advisory Board Member
CIIWA (Competitive Intel and Information Warfare Association) Board Member
EuroDefense – Portugal Board Member

1. INTRODUÇÃO

É hoje em dia consensual considerar que tecnologias disruptivas, como o 5G, a par de outras que marcam a atualidade, como a computação quântica ou os desenvolvimentos da inteligência artificial, prometem um salto transformacional que revolucionará a forma como vivem as sociedades atuais. Como a história da humanidade nos tem mostrado consistentemente, todos os avanços tecnológicos desta natureza revelam, quase sempre, uma dualidade, por um lado de uma clara criação de valor, com progressos notáveis em diversos campos, quer sejam na saúde, mobilidade ou na energia, ao mesmo tempo que, por outro, expõem a sociedade a novos riscos e desafios, em concreto os que resultam da exploração nociva da tecnologia, de forma intencional ou negligente, com impactos negativos na segurança e resiliência coletiva.

A utilização prevista para a tecnologia 5G implica que a mesma passe a constituir um elemento estruturante onde irão assentar serviços essenciais à sociedade, sendo que, muitos destes serviços, serão utilizados no campo da gestão de infraestruturas críticas. A capacidade de fazer com que esse pilar seja confiável é um aspeto crítico que pode ditar um avanço sustentado da humanidade ou, então, um falhanço de dimensões consideráveis. Num mundo globalizado, caracterizado por novos tipos de riscos, onde existe uma forte e crescente dependência tecnológica, estamos a assistir a novas configurações de ameaças, nomeadamente ameaças híbridas, recentemente reconhecidas por países e organizações mundiais, que jogam com operações em vários domínios da sociedade. O controlo, por agentes mal-intencionados, de uma infraestrutura como o 5G, permitirá que os perpetradores disponham dos meios para poder materializar cenários de ameaças híbridas, perturbando a operação de infraestruturas críticas e elevando o nível de desconfiança e desordem das sociedades, levando assim a uma diminuição da perceção de segurança, o que poderá colocar em causa o progresso e bem-estar dos respetivos cidadãos.

Este artigo propõe-se analisar os impactos dessas ameaças neste novo contexto tecnológico que caracteriza o 5G, identificando as principais características da arquitetura desta recente tecnologia, os seus casos de uso, assim como os novos riscos que coloca e, consequente, a forma como poderá ser utilizada por agentes mal-intencionados. Termina com um conjunto de propostas globais, em que algumas delas são orientadas a operadores de infraestruturas críticas e serviços essenciais, de modo a mitigar os riscos de utilização do 5G.

Importa também salientar que esta reflexão tem como objetivo apresentar uma modesta contribuição para uma utilização mais segura desta tecnologia, sempre assente na filosofia de que o progresso é desejável e um fim, não havendo qualquer intenção de descredibilização, mas antes alertar para possíveis riscos, propondo um conjunto de linhas orientadoras para os mitigar.

2. CARACTERÍSTICAS DA ARQUITETURA DO 5G

O estudo completo e detalhado da arquitetura 5G é complexo e muito técnico, não sendo objeto desta reflexão. Contudo é necessário entender algumas das suas características para percebermos os respetivos cenários de utilização, assim como o panorama dos riscos associados.

Cada nova geração de redes de comunicação móvel tem sempre associadas maiores velocidades de transferência de dados e maiores capacidades de comunicação. A primeira geração (1G) apresentou os primeiros telefones móveis que conhecemos; o 2G trouxe melhor cobertura e mensagens de texto; o 3G introduziu voz com dados / internet e o 4G proporcionou velocidades maiores para acompanhar a procura crescente de dados móveis. A quinta geração (5G) tecnológica representa uma transformação completa das redes de telecomunicações, apresentando uma grande diversidade de benefícios, como taxas de transferência de dados mais altas (velocidades de *download* extremamente rápidas), latência ultrabaixa (interatividade quase em tempo real) e um aumento da capacidade da rede (permitindo a conectividade de muitos mais dispositivos ao mesmo tempo). Estes benefícios abrem caminho para novos recursos e um novo paradigma de conectividade, de forma a suportar a materialização de conceitos há muito idealizados, como cidades inteligentes, veículos autônomos, assistência médica remota e muitos mais avanços que povoam os sonhos da humanidade.

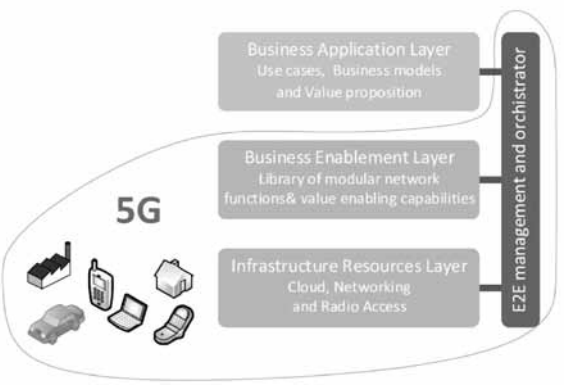


Figura 1 – Arquitetura alto nível 5G (fonte: Threat Landscape and Good Practice Guide for Software Defined Networks/5G: ENISA)

A figura 1 representa uma ilustração de alto nível da arquitetura 5G. Nela se destacam os seguintes componentes:

- **A camada de recursos de infraestrutura,** contém qualquer dispositivo físico, incluindo dispositivos móveis ou dispositivos de Internet das Coisas (IoT[1]), designados 5G, bem como elementos de rede fixa (nós de rede, nós de nuvem[2], nós de acesso, antenas, entre outros). Esta camada utiliza a programação em software SDN / NFV (*Software Defined Network / Network Functions Virtualization*), bem como a configuração de dispositivos 5G, a fim de responder às especificações de desenho das aplicações (por exemplo, largura de banda ou latência).

- A **camada de facilitação de negócio (*business enablement*),** contém todas as funções necessárias para a rede 5G convergir na forma de blocos de arquitetura modular. Esses blocos, e os respetivos parâmetros de configuração, podem ser evocados num repositório comum, mediante solicitação das aplicações e dependendo dos casos de uso.

- **Módulo de gestão e orquestração E2E (End to End),** garante a gestão e organização dos blocos de arquitetura mencionados anteriormente. Além disso define segmentos de rede (*network slicing* - multiplexagem de redes lógicas virtualizadas e independentes, na mesma infraestrutura de rede física) para cada caso de uso, interconecta as funções relevantes da rede e atribui a configuração adequada para atender às especificações E2E. É nesta camada que se realiza o mapeamento com os elementos da rede pertencentes à camada de recursos de infraestrutura.

- A **camada de aplicações de negócios,** contém aplicações e serviços das operadoras de rede 5G ou de outras empresas que usam a infraestrutura de rede. Tem interface para a camada que gere

1 IoT – *Internet of Things, tecnologia que possibilita objetos cotidianos e de diversos tipos, armazenarem, processarem e transferirem informação com ligação à internet.*

2 Nuvem – Nome genérico dado à computação em servidores disponibilizados na Internet por diferentes fornecedores. Também usualmente conhecido como *cloud computing*.

e orquestra E2E, que pode ser usada para mapear uma aplicação a segmentos de rede existentes ou para criar novos segmentos para as aplicações, oferecendo, por essa razão, uma flexibilidade adicional.

Do exposto facilmente se conclui que uma das principais características diferenciadoras do 5G é a implementação de uma abstração de serviços móveis, que podem ser materializados na infraestrutura de vários operadores, dando corpo ao conceito, *as a service*, ao qual já estamos familiarizados pela utilização de *cloud computing* no domínio da computação em TI (tecnologias de informação). Este objetivo, só pode ser materializado através da centralização da gestão da rede, gerida com recurso a *software*, mais concretamente através das tecnologias de SDN e NFV, mudando assim o paradigma das redes de comunicação anteriores, muito baseado em equipamentos distribuídos que incorporam inteligência no encaminhamento de tráfego.

Para se perceber melhor o futuro impacto do 5G, será conveniente descrever os diferentes casos de uso desta tecnologia. Na perspetiva do 5GPPP (5G *Infrastructure Public Private Partnership*), podemos destacar 3 cenários tipo de utilização do 5G:

- **eMBB – *Enhanced Mobile Broadband*:** Banda larga móvel reforçada, que usa o espectro de banda alta, com a capacidade de suportar taxas elevadas de transferência de dados, proporcionando aos consumidores um serviço de conexão mais rápido e confiável, quer em áreas congestionadas ou em movimento. Contudo, devido ao sinal com menor capacidade de penetração e de curto alcance, será necessária mais infraestrutura para concretizar este caso de uso.

- **URLLC – *Ultra Reliable Low Latency Communication*:** A comunicação de baixa latência, com capacidade para cobrir grandes áreas (vários quilómetros), satisfazendo o uso de aplicações que exigem alta confiabilidade e que são extremamente sensíveis à latência, frequentemente para aplicações de missão crítica.

- **mMTC – *Massive Machine Type Communication*:** fornece conectividade a biliões de dispositivos que transmitem pequenas

quantidades de tráfego, de forma intermitente, através da banda de baixa frequência, mas que pode cobrir áreas muito abrangentes (centenas de quilómetros). Estas aplicações não são muito dependentes da latência.

Procura-se agora caracterizar em maior detalhe os cenários que envolvem infraestruturas críticas e serviços essenciais para as próximas sociedades, de forma a melhor caracterizar os riscos de segurança que se encontram associados.

3. CASOS DE USO QUE ENVOLVEM INFRAESTRUTURAS CRÍTICAS E SERVIÇOS ESSENCIAIS

Nesta secção, ilustram-se casos de uso da tecnologia 5G com especial foco nas infraestruturas críticas e serviços essenciais. As descrições aqui presentes são apenas uma pequena amostra do potencial de aplicação do 5G[3], porque os cenários são inúmeros e, obviamente, em contínua identificação e definição, existindo já muito casos de estudo em sectores tão diversos como a indústria, meios de comunicação social ou mesmo turismo e agricultura.

a. Energia

As redes de transporte e distribuição de energia elétrica providenciam a sua condução desde os diversos pontos de geração até aos locais de consumo, atravessando uma extensa malha de cabos elétricos e equipamentos de seccionamento e transformação de potência, como subestações e postos de transformação. As redes de transporte e distribuição de energia são, pois, fulcrais para o funcionamento e segurança da sociedade e, como tal, estão claramente identificadas como serviços essenciais, sendo muitos dos ativos físicos subjacentes, considerados infraestruturas críticas.

3 Como exemplo do reconhecimento dos riscos decorrentes do aumento da utilização de produtos de consumo e dispositivos industriais ligados à Internet, e a consequente necessidade de aumentar o nível de segurança no mercado único digital, a Agência da UE para a Cibersegurança (ENISA) está já a trabalhar em sistemas de certificação da cibersegurança no mercado, a fim de abordar todos os aspetos relevantes da cibersegurança IoT (https://www.consilium.europa.eu/pt/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/)

A correta operação destas infraestruturas baseia-se cada vez mais em soluções automatizadas com suporte a dados de tempo real, de forma a assegurar as atividades dos operadores de despacho (comando da rede) e guiar as intervenções das equipas de campo, quer para trabalhos de manutenção, quer para a reparação de avarias. Adicionalmente, a necessária otimização de serviço, leva a que cada vez mais as redes assentem em protocolos de *selfhealing* (reconfiguração automática da rede para redirecionar a energia para outras rotas não afetadas por avarias ou acidentes), caminhando assim para o conceito de *smartgrids*, que constituem a pedra basilar das ambicionadas *smartcities*.

Estes protocolos de *selfhealing* em redes de missão crítica, necessitam de uma infraestrutura de comunicações de alta qualidade, para funcionar de maneira confiável e em tempo real. Para atender a esses requisitos exigentes, a tecnologia de segmentação de rede 5G, com as suas elevadas taxas de transferência e baixa latência, promete oferecer a solução desejada para alcançar esse objetivo, permitindo, deste modo, a concretização plena do conceito de *smartgrids* (cenário URLLC).

Ainda no domínio das redes de energia, atividades como a manutenção de ativos, em concreto a previsão de avarias e a antecipação eficaz de intervenções nos equipamentos de rede, beneficiam da tecnologia 5G, mormente através da aquisição massiva de dados em tempo real e com grandes taxas de transmissão, o que permitirá escalar a sensorização das redes, com a consequente otimização em termos da respetiva gestão (cenários mMTC e eMBB).

b. Saúde

O setor de saúde encontra-se numa rápida expansão, principalmente devido à aplicação, no domínio médico, da inteligência artificial e analítica sobre os dados de saúde existentes. Com a adoção do 5G novos casos de uso de saúde estão a ganhar forma, potenciando a telemedicina e telecirurgia, assim como a utilização de dispositivos médicos inteligentes.

A telemedicina é, efetivamente, um dos cenários mais premente de utilização do 5G, principalmente nos países onde as infraestruturas de rede

com fio não estão bem desenvolvidas. Os serviços móveis 5G permitirão uma entrega mais eficaz do diagnóstico remoto, assim como o suporte para intervenções das equipas de paramédicos, estendendo o habitual conceito das tradicionais consultas presenciais em unidades de saúde. As características da arquitetura do 5G permitem a concretização do atendimento remoto e da telemedicina ao garantir *streaming* de vídeo de baixa latência e alta qualidade (cenário URLLC).

Para além da telemedicina, também a telecirurgia pode beneficiar da baixa latência e alta largura de banda da tecnologia 5G, possibilitando, aos cirurgiões, a execução de cirurgias em tempo real, mesmo quando não estiverem fisicamente no local, usando um controlo remoto ou simplesmente guiando outros cirurgiões menos experientes. Embora o 4G seja suficiente para os cenários descritos, em concreto assegurando a transmissão de vídeo em tempo real, tem, no entanto, o problema da alta latência, o que o torna inutilizável para telecirurgia (cenário URLLC).

Ainda no campo da saúde, uma das principais razões pelas quais os pacientes com doenças crónicas visitam o hospital é a falta de equipamentos médicos em casa para medir e monitorar os respetivos sinais vitais. Com o 5G vai ser possível ter dispositivos de monitorização de saúde de baixa potência que permitem o rastreamento constante do estado do paciente, permitindo prever o progresso de doenças, alertar para idas urgentes aos hospitais, ajustar doses de medicação ou alterar terapias em tempo quase real e de forma completamente remota (cenário mMTC).

c. Transportes e veículos autónomos

No caso dos transportes resultam benefícios óbvios na otimização da logística de empresas de transporte, quer de mercadorias, quer de passageiros, sendo este outro dos domínios onde o 5G potencia enormes avanços. Poder conectar semáforos e estradas, ou ainda as ferrovias, com os veículos e outras infraestruturas, e poder analisar toda essa informação por meio de inteligência artificial, permitirá desenvolver sistemas inteligentes para que o transporte seja o mais eficiente possível, poupando recursos às organizações e reduzindo o seu impacto no meio ambiente (cenário mMTC).

Os veículos autónomos também beneficiarão desta nova realidade, na medida em que a informação que recebem de outros veículos e de infraestruturas rodoviárias, quer imagens, quer outro tipo de dados, irá permitir a aquisição da quantidade de informação necessária e com baixa latência, que permitirá uma otimização da condução, com vantagens, uma vez mais, na poupança de recursos naturais, ao mesmo tempo que proporciona melhor comodidade para os indivíduos, em especial a redução do flagelo dos incidentes rodoviários (cenário URLLC).

d. Segurança pública

Para o objetivo desta reflexão este será o último cenário de utilização a destacar. A utilização de redes 5G vai permitir criar redes de emergência interligadas que permitirão instalar capacidades de antecipação e reação a cenários de catástrofe. Os recursos de localização oferecidos pelo 5G auxiliarão, por exemplo, na obtenção de dados em tempo real de um ambiente de emergência a ser evacuado, como o número de ocupantes dentro de determinada área, pessoas presas em áreas isoladas do edifício ou a gestão do fluxo em tempo real de evacuados. Os cenários de utilização do 5G na área da segurança pública são inúmeros e, obviamente, ainda em definição, geram, contudo, uma forte dependência desta tecnologia, com potenciais implicações no bem-estar e segurança das sociedades (todos os cenários possíveis, eMBB, URLLC e mMTC).

4. RISCOS DE SEGURANÇA ASSOCIADOS À TECNOLOGIA 5G

Uma análise técnica detalhada das vulnerabilidades de cibersegurança do 5G pode ser realizada utilizando taxonomias reconhecidas e disponíveis[4], incluindo a forma como as mesmas podem ser exploradas e mitigadas. Para o objetivo desta reflexão, interessa destacar as alterações em termos de perfil de risco introduzidas pela tecnologia e a arquitetura subjacente. Nesse sentido, destacam-se o controlo central baseado em software, a expansão da largura de banda e o elevado número de dispositivos na rede:

4 "Threat Landscape and Good Practice Guide for Software Defined Networks/5G": ENISA

a. Controlo central baseado em software

Com o 5G, a rede muda de uma de comutação baseada em hardware, disperso pelos diversos equipamentos ao longo da rede, para um encaminhamento digital distribuído, ainda que definido e controlado centralmente por software (SDN). As redes anteriores são do tipo *hub-and-spoke,* ou seja, compostas por elementos de *hardware* que concentram e distribuem tráfego. Estes equipamentos são alvo de controlo da cibersegurança e a falha de um deles não compromete, com grande probabilidade, toda a rede. Na rede 5G, esta atividade de controlo é retirada da malha de *routers* digitais existentes ao longo das redes, deixando assim de haver a inspeção e controlo de segurança efetuado a esse nível. A centralização pode trazer notórias vantagens em termos de segurança e operação, mas também introduz um enorme risco, caso esse controlo seja usurpado por um agente mal-intencionado, que passe, por exemplo, a ter acesso a segmentos de redes que podem estar atribuídos a serviços críticos como os descritos acima. Este facto exige uma especial proteção nestes pontos de controlo da rede.

O 5G introduz ainda um risco adicional, em relação às tecnologias anteriores, nomeadamente ao virtualizar em *software* um nível superior de funções de rede, anteriormente executadas por elementos de rede baseados em *hardware*. Estas funções são implementadas com base em linguagens comuns e protocolos da Internet bem conhecidos por toda a comunidade que trabalha em engenharia de sistemas. Quer sejam usados por Estados-nação ou atores criminosos, a exploração das fragilidades destes protocolos e linguagens, constituem uma ferramenta valiosa para aqueles que procuram fazer o mal.

b. Expansão da largura de banda.

As redes 5G permitem alavancar o espectro de banda baixa, média e alta, exigindo a implantação de pequenas células (áreas geográficas servidas por um transmissor/recetor), além das torres de comunicação macro. Essas pequenas células, servem como repetidores de sinal, proporcionando maior velocidade, maior capacidade de rede e maior confiabilidade de serviço em áreas de alta densidade. Contudo, estes equipamentos servem também

para aumentar a superfície de ataque pois, fisicamente, são antenas de células pequenas, de baixo custo, curto alcance, implantadas em todas as áreas urbanas, constituindo-se como novos alvos fáceis de atacar fisicamente. É importante ainda realçar que essas estações de equipamentos móveis recorrem à partilha do espectro dinâmico de 5G, no qual vários fluxos de informação partilham a largura de banda, atribuída a segmentos de rede que podem estar a suportar serviços essenciais, como os já aqui mencionados.

c. Biliões de dispositivos na rede

Finalmente, a maior e mais evidente vulnerabilidade criada pelo 5G, é permitir adicionar à rede dezenas de biliões de dispositivos inteligentes (na verdade, pequenos computadores), que, dando corpo ao que é comumente conhecido como IoT *(Internet of Things),* podem ser comprometidos. A utilização destes dispositivos, nos mais diversos cenários, já foi apresentada neste trabalho, mas recorda-se aqui que serão utilizados em atividades que vão desde a segurança pública, até à medicina, passando pela energia e transportes, entre inúmeras outras aplicações.

Não obstante todos os esforços em curso[5], esperar que a segurança seja garantida por estes dispositivos será um erro com fortes impactos na nossa sociedade. Num artigo recente, por exemplo, a Microsoft relatou que *hackers* russos haviam penetrado na corrida de dispositivos IoT para obter acesso às redes[6]. A partir daí, os *hackers* descobrirão outros dispositivos IoT inseguros nos quais eles podem instalar *software* de exploração. Esta superfície de ataque é de bastante difícil controlo, porque está dependente dos fabricantes dos dispositivos, da sua configuração e contexto de uso, assim como da possibilidade de monitorização de padrões de utilização.

5 Como exemplo do reconhecimento dos riscos decorrentes do aumento da utilização de produtos de consumo e dispositivos industriais ligados à Internet, e a consequente necessidade de aumentar o nível de segurança no mercado único digital, a Agência da UE para a Cibersegurança (ENISA) está já a trabalhar em sistemas de certificação da cibersegurança no mercado, a fim de abordar todos os aspetos relevantes da cibersegurança IoT (https://www.consilium.europa.eu/pt/press/press-releases/2020/12/02/cybersecurity-of-connected-devices-council-adopts-conclusions/)

6 https://msrc-blog.microsoft.com/2019/08/05/corporate-iot-a-path-to-intrusion/

5. CENÁRIOS DE AMEAÇAS HÍBRIDAS COM BASE NO USO DO 5G

Os cenários de conflitualidade do mundo atual estão a mover-se cada vez mais para o palco do ciberespaço, sendo que as ações conduzidas neste domínio permitem criar vantagem ou eventos de influência em outros ambientes operacionais, quer no plano informacional quer no plano do mundo físico. Por exemplo, ataques a sistemas que controlam infraestruturas críticas podem conduzir à destruição das mesmas, com impactos na segurança e no bem-estar das sociedades. Desta forma, tem-se assistido cada vez mais à utilização do ciberespaço para a produção de um conjunto diversificado de efeitos, ora isolados, ora coordenados com outras ações, dando origem ao que se chamam de ameaças híbridas.

O conceito de ameaça ou guerra híbrida vai ganhando cada vez mais realidade e é uma preocupação cada vez mais presente na agenda de entidades governamentais e militares, tais como a NATO e a UE[7]. As ameaças híbridas podem ser descritas como o uso sincronizado de múltiplos instrumentos de poder, adaptados para explorar vulnerabilidades específicas em todo o espectro de funções sociais, de modo a convocar efeitos sinérgicos com o intuito de surpreender o individuo e a sociedade; destruir a confiança e causar frustração nas instituições sociais e governos, conduzindo a situações de caos social.

A relativa novidade da guerra híbrida reside na capacidade de um ator sincronizar vários instrumentos de poder simultaneamente e, intencionalmente, explorar a criatividade, ambiguidade, não linearidade e os elementos cognitivos da guerra. A guerra híbrida - conduzida por atores estatais ou não estatais - é normalmente adaptada para permanecer abaixo dos limites óbvios de deteção e resposta, e muitas vezes depende da velocidade, volume e onipresença da tecnologia digital que caracteriza a atual era da informação. Estas características conjugadas levam a uma muito difícil atribuição da causa, tornando a respetiva ação mitigadora complexa e muitas vezes de difícil coordenação.

7 Joint communication to the European parliament, the European council and the council, to Increasing resilience and bolstering capabilities to address hybrid threats: European Commision, Bruxelas, 2018.

Não obstante a compreensão do conceito de guerra híbrida assentar no uso de instrumentos de poder nos domínios informacional, político, militar, económico, social e controlo de infraestruturas, o facto é que qualquer um destes instrumentos está inexoravelmente assente nas tecnologias digitais e na capacidade de exercer o seu controlo. O controlo tecnológico pode potenciar uma atuação sincronizada em vários campos, em concreto aproveitando as características do ciberespaço, que potenciam a ubiquidade dos atores, a dissimulação das ações e controlo da intensidade das mesmas.

Com base no atrás descrito, percebe-se a relação que o 5G tem com as ameaças híbridas aqui referidas. O 5G tem exatamente o conjunto de atributos adequados para ser efetivo neste contexto, designadamente a abrangência de aplicação que cobre todo o leque de instrumentos de poder aqui descritos e, como tal, se de alguma forma for controlado por agentes mal-intencionados, aumenta o potencial para poder gerar cenários de caos, que permitam aos atacantes alcançar os seus objetivos.

Não é difícil imaginar cenários com base no controlo, por atacantes, de segmentos de rede 5G, e que esse controlo tenha sido atingido por via da exploração de vulnerabilidades do *software* utilizado para a gestão das redes de comunicação. Um exemplo seria o espoletar um apagão através da intrusão de uma rede inteligente de energia, associado a outras ações que afetem outros serviços essenciais, como a distribuição de água, o que iria gerar uma sensação de grande insegurança na sociedade. Podemos ir mais além, ao imaginar uma ação de terrorismo perpetrada através de meios convencionais, gerando a necessidade da intervenção de equipas de emergência e socorro, que seriam afetadas por um controlo prévio malicioso dos segmentos de rede em que operam os seus sistemas de apoio, gerando, mais uma vez, um caos e pânico na sociedade.

Os cenários imaginados podem ser inúmeros, contudo, talvez o que pode causar maior preocupação, é a captação massiva de informação do funcionamento da sociedade através do comprometimento da rede 5G e dos diversos sensores que existem nas denominadas *smart cities*, obtendo informação que poderá ser utilizada para enriquecer algoritmos poderosos de Inteligência artificial, que, depois, poderão alimentar campanhas de desinformação muito bem orquestradas e deturpar a perceção das realidades

que, cidadãos incautos, construirão nas suas próprias mentes. Se nada fosse feito, este cenário poderia ser perpetrado por um Estado poderosíssimo ou por grupos terroristas muito motivados e bem financiados que dominem a tecnologia, que ficariam a saber mais sobre os comportamentos das sociedades democráticas que os próprios governos, legitimante eleitos pelos respetivos cidadãos, comprometendo assim os valores essenciais das sociedades de Estado de Direito Democrático[8].

Considerando o que aqui foi exposto, facilmente se conclui da necessidade de continuar a desenhar estratégias e políticas a nível governamental, ao mesmo tempo que as organizações deverão adotar as proteções para assegurar um desenvolvimento sólido e seguro do 5G, de acordo com essas políticas. A próxima secção descreve em mais detalhe algumas das propostas para a mitigação dos riscos identificados.

6. PROPOSTAS PARA MITIGAÇÃO DOS RISCOS DO 5G

Nesta secção propõem-se um conjunto de iniciativas, algumas de âmbito geral, que endereçam o tema de forma global, e outras mais dirigidas às empresas responsáveis pela gestão de serviços essenciais e infraestruturas críticas.

a. Desenvolvimento de políticas e padrões de segurança para o 5G

O desenvolvimento de políticas e padrões de segurança para o 5G serve como base para proteger a infraestrutura de comunicações[9]. As entidades

8 Na sequência da Recomendação (UE) n.º 534/2019, da Comissão, de 26 de março de 2019, relativa à cibersegurança das redes 5G, foi criado um grupo de trabalho que promoveu a realização de uma avaliação de risco nacional e participou na avaliação de risco a nível europeu. Esse mesmo grupo, ao abrigo da Resolução do Conselho de Ministros n.º 7-A/2020 de 7 de fevereiro, elaborou um relatório que, entre outras coisas, identificou as ações a desenvolver a nível nacional para a implementação das medidas de segurança adequadas à atenuação dos riscos em matéria de cibersegurança, que assegurem, nomeadamente, a conformidade com as medidas europeias.

9 A União Europeia (EU) criou uma *toolbox* com objetivo de identificar um possível conjunto comum de medidas capazes de mitigar os principais riscos de cibersegurança das redes 5G e fornecer orientações para a seleção das medidas que devem ser priorizadas nos planos de mitigação a nível nacional e da UE https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

que moldam o futuro destas políticas e padrões devem posicionar-se como líderes globais e ajudarem a facilitar a implantação e comercialização seguras de tecnologias 5G. Para evitar tentativas de agentes mal-intencionados de influenciar o desenho e a arquitetura de redes 5G, é fundamental que que os produtos e as soluções que compõem a cadeia de valor desta tecnologia sejam projetados e implementados com segurança e resiliência desde o início (*Security by Design*) e com base em padrões de segurança bem definidos e aceites pela comunidade.

b. Regulação para refletir as evoluções tecnológicas

É um facto reconhecido que as leis e a regulação andam sempre atrás da evolução tecnológica, evidência que se tem acentuado nas últimas décadas com o crescimento exponencial das tecnologias e na sua aplicação na sociedade. Não obstante esta clivagem, é incontornável que a regulação continua a desempenhar um papel determinante para o equilíbrio entre o desenvolvimento tecnológico e a preservação dos direitos e liberdades fundamentais das sociedades.

A regulação sobre a expansão e implementação do 5G é, desta forma, um edifício que deve ser construído e mantido de forma equilibrada e eficiente, evitando a adoção de regulação com demasiadas especificidades, que se tornam rapidamente obsoletas sem, contudo, serem demasiado generalistas ao ponto de serem suscetíveis de interpretações mais ligeiras que conduzam a uma inação por parte das organizações. Uma legislação com este equilíbrio exige, claramente, a participação e cooperação do mundo empresarial e académico, juntamente com o legislador, colaborando todas as partes com base num alinhamento de incentivos e numa otimização nos processos de atualização dessas leis e regulações.

A questão dos incentivos torna-se também num aspeto crucial na dimensão das leis e regulações. Efetivamente, por vezes, é necessário manter o lado penalizador, baseado em incentivos negativos, para quem não cumpre e, aqui, a fiscalização deverá ser reforçada para verificar os controlos de segurança implementados pelas empresas. No entanto, também é crucial regular em torno de incentivos positivos, que estimulem a que as empresas, quer fornecedores de *supply chain* 5G, quer operadores de serviços, pro-

curem integrar a segurança na sua atividade, com o objetivo de retirarem vantagens comercias para as suas organizações.

Certamente que os mercados, por si só, não resolverão o tema da segurança, quer do 5G, quer de outra tecnologia existente ou que venha a surgir. Contudo estes são uma ferramenta poderosa para esse objetivo, pois se as organizações virem divulgados e reconhecidos os seus esforços em prol da segurança, e a tomada de decisão do comprador trazer esse facto em consideração, muito à semelhança do que já acontece em torno do tema da sustentabilidade ambiental, naturalmente conduzirá a uma mais fácil integração dos aspetos de segurança no desenho e exploração de produtos e serviços.

Finalmente, ainda no que concerne ao tema das leis e regulações, é natural a tendência para que nações, ou grupos de nações, tendam a criar as suas regulações especificas e locais. Contudo, é necessário um esforço coordenado para uma abordagem mais abrangente, dado que os problemas atuais, e em especial o 5G, são globais, que afetam organizações que operam nas mais diversas geografias, e, como tal, a necessidade de adaptação a especificidades locais pode resultar em grandes ineficiências e vulnerabilidades, sem qualquer ganho para o objetivo da segurança.

c. Garantir a segurança na cadeia de fornecimento (supply chain) do 5G

Considerando a abrangência da cadeia de fornecimento do 5G, que integra desde componentes de *software*, fornecedores, equipamentos e redes, a segurança da cadeia de fornecimento desta tecnologia está sob constante ameaça. Como exemplo, ainda que certos equipamentos 5G possam ser de um fornecedor confiável, os componentes de suporte fabricados ou manipulados por parceiros não confiáveis, ou agentes mal-intencionados, podem anular quaisquer medidas de segurança em vigor. Esses componentes, ao serem comprometidos, têm o potencial para afetar a conectividade e a segurança dos dados, assim como das informações transmitidas.

A consciencialização das empresas que adquirem equipamentos e soluções no âmbito do 5G, com especial foco nos prestadores de serviços essenciais

ou operadores de infraestruturas críticas, é um aspeto fundamental para a mitigação dos riscos associados.

d. Analisar e compartilhar casos de utilização 5G

Como já foi possível constatar, as possibilidades da tecnologia 5G dão suporte a uma série de novas funções e dispositivos capazes de materializar uma infinidade de potenciais casos de uso nos mais diversos setores da sociedade. Com a possibilidade de conexão de bilhões de dispositivos à rede, será necessário exigir uma maior segurança para proteger os dispositivos conectados das ameaças e vulnerabilidades potenciais. Para garantir a segurança e integridade desses dispositivos e dos cenários que possibilitam, é fundamental a constante partilha, entre quem gere, opera e utiliza os serviços 5G, das vulnerabilidades conhecidas e estratégias de gestão de risco para casos de uso associados à proteção, em especial no domínio dos serviços essenciais das nações.

e. Proteção baseada em técnicas avançadas de inteligência artificial

Os ataques ao 5G serão, maioritariamente, no plano do *software*. Para poder fazer face às ameaças, cada vez mais automatizadas, sofisticadas e coordenadas, que poderão surgir dos milhões de dispositivos ligados à rede, é necessário recolher toda esta informação e analisá-la com técnicas de inteligência artificial, nomeadamente *deep learning* e *machine learning,* de forma a poder detetar atempadamente as ameaças. Estes tipos de ações de prevenção e deteção deverão ser concretizadas, quer ao nível dos operadores e fornecedores de serviço 5G, como das empresas que os consomem, com especial foco, uma vez mais, para aquelas que gerem infraestruturas criticas e serviços essenciais.

f. *Situation awareness*

A constante monitorização da cibersegurança do estado da infraestrutura e serviços é crucial, quer na perspetiva das organizações, que utilizam esta tecnologia para suportar os serviços que prestam aos clientes e à sociedade, quer na visão dos operadores e fornecedores de serviços 5G como,

igualmente fundamental, no plano das nações, ou grupos de nações, como medida de prevenção contra ameaças híbridas.

Os diferentes níveis de monitorização deverão ser implementados com a clara identificação da informação que deverá ser passada ao nível superior de monitorização, o que deverá exigir uma constante articulação entre os diversos intervenientes na cadeia de valor do 5G. Como exemplo, eventos de anomalias de dispositivos IoT de um segmento de rede dedicado a redes de emergência de um país, podem fazer sentido no plano de *situation awareness* da nação, uma vez que poderão estar relacionados com outros acontecimentos em outros palcos da sociedade, como, por exemplo, informações de segurança interna.

g. Resiliência

Esta é uma capacidade que a maioria das organizações sempre demonstraram ao longo da história e que nunca poderá ser abandonada. As organizações devem ser desenhadas para ser resilientes, em especial as organizações que gerem infraestruturas críticas e providenciam serviços essenciais à sociedade. Sempre que se adotam novas tecnologias para otimizar, ou alterar de forma disruptiva, os processos de negócio e os serviços providenciados, devem ser considerados planos de continuidade e recuperação de desastre, de forma a garantir que, na eventualidade de um cenário de imprevisibilidade e perturbação, os serviços essenciais serão garantidos. A utilização do 5G vai exatamente criar efeitos disruptivos nas organizações e na sociedade, pelo que é fulcral que essas mesmas organizações não se esqueçam de adaptar os seus planos de resiliência, sem ser necessário esperar que os mesmos venham a ser exigidos pelas autoridades responsáveis pela regulação.

7. CONCLUSÃO

Deveremos, sempre que possível, considerar os avanços alavancados pelas tecnologias como acontecimentos moralmente bons, que conduzem a um grau mais elevado de bem-estar e evolução da sociedade, quer no plano do ser humano, quer na sua relação com a envolvente. Existe a consciência

que os saltos evolutivos acarretam sempre uma alteração no panorama do risco, que colocam novos desafios que as sociedades sempre procuraram equilibrar e mitigar. O desafio da adoção do 5G não será, certamente, diferente de outros processos idênticos que tivemos no passado, pelo que, desde que uma parte da sociedade se preocupe com a identificação e controlo desses riscos, equilibrando os mesmos com o progresso, o 5G irá, com toda a certeza, corresponder a todas as expetativas que a sociedade coloca nesta recente e algo diruptiva tecnologia.

Os desafios da introdução do 5G na nossa sociedade estão bem identificados e existe uma oportunidade única, ao contrário do que aconteceu com outras tecnologias que foram surgindo, como a própria internet, onde questões de segurança não foram tidas em consideração no seu desenho, de introduzir os requisitos de proteção de uma infraestrutura tão crítica desde o seu desenho e implementação, pelo que estou certo que essa oportunidade não nos escapará, de modo a podermos usufruir de um mundo melhor e mais seguro.

O IberSafe é uma portaria de segurança automática que impede a entrada num espaço ou instalação a pessoa e pertences que não cumpram a totalidade de um conjunto de requisitos sanitários: a permissão de acesso, a temperatura corporal ser normal, averificação de que a máscara está colocada e ter desinfetado as mãos, após o que a porta da cabina abre automaticamente para o espaço interior onde um atomizador ultra-sónico procede à desinfeção da pessoa e dos seus objetos.

O IberSafe tem as seguintes funções;

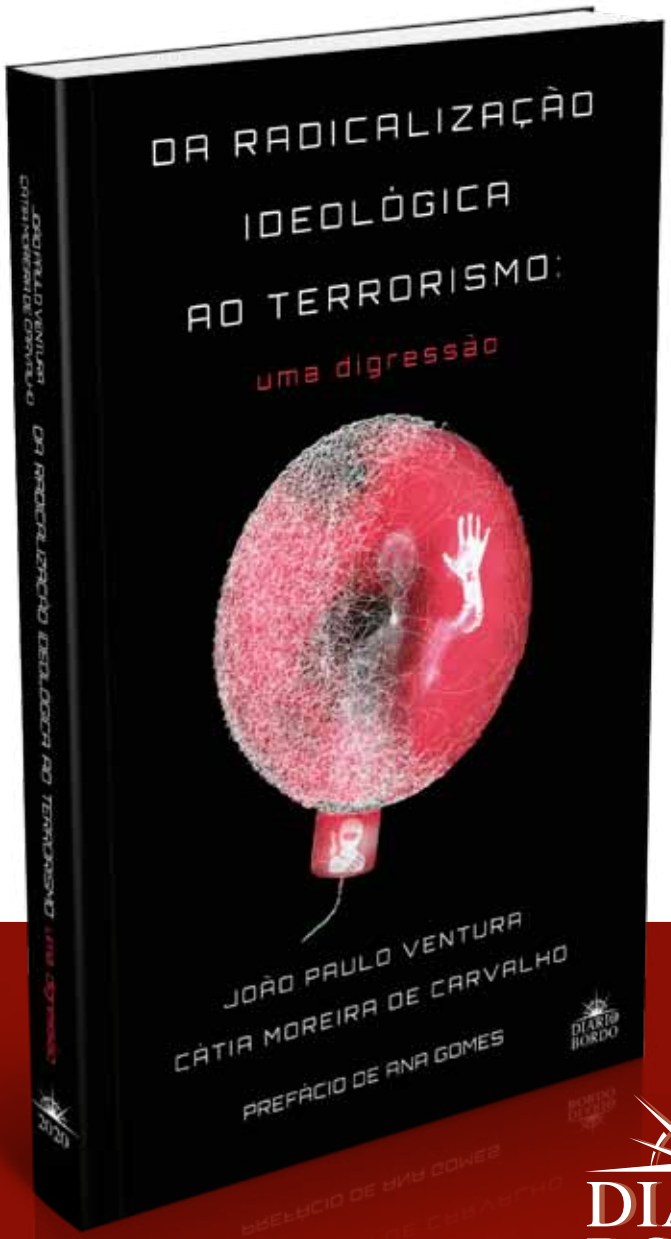
À porta da cabina:
- A identificação da pessoa através de reconhecimento facial ou cartão de identificação;
- A medida de temperatura, feita sem contacto físico, garantindo a segurança da pessoa evitando o risco de contágio;
- A verificação de que a máscara está colocada;
- A desinfeção automática das mãos;

No interior da cabina:
- A desinfeção da pessoa e dos seus objetos.

O IberSafe, projeto apoiado pelo Compete2020, é uma cabina de segurança com certificação eurpeia, concebida e fabricada em Portugal pela IberGlobal, empresa de engenharia mecânica e eletrotécnica com grande experiência no mercado nacional, exportadora da maior parte dos seus produtos. A aplicação informática, desenvolvida à medida, monitoriza o funcionamento automático de todo o processo de um produto 100% português.

Estamos à Vossa disposição para prestar os esclareciemntos complementares sobre o IberSafe e para a marcação de uma reunião, presencial ou virtual, através dos seguintes contactos:

e-mail: ibersafe@iberglobal.pt contacto: 937 167 044



DIÁRIO DE BORDO

Cidadania e Conhecimento

DIÁRIO DE BORDO