Protecção das Infra-estruturas Críticas: Portugal e a União Europeia

Jorge Batalha*

Resumo

Face aos diversos atos terroristas ocorridos desde o 11 de setembro de 2001, a segurança revela-se como uma das maiores preocupações sempre que se registam eventos suscetíveis de ameaçar o bem-estar económico e social dos cidadãos. As diretivas produzidas no âmbito da União Europeia têm levado os Estados-membros a legislar de forma a reforçar as medidas de segurança em infraestruturas críticas, as quais, em caso de destruição ou disrupção, resultariam em consequências catastróficas, não só para o próprio Estado, como noutro Estado transfronteiriço ou ainda outros mais.
Este documento visa mostrar parte do que em Portugal tem sido feito no âmbito da proteção de infraestruturas críticas nacionais, colocar algumas questões quanto à responsabilidade dos donos/operadores, tentando, no final, apontar alguns caminhos em defesa do interesse nacional.

Palavras-chave: políticas de segurança, infraestruturas críticas nacionais, proteção, agente de ligação de segurança, responsabilidade

* Licenciado em Estudos de Segurança. Mestrando em Segurança de Informação e Direito no Ciberespaço

Abstract

Given the many terrorist acts that have occurred since the September 11, 2001, the security turns out to be a major concern when events are reported susceptible to threaten the economic and social well-being of citizens. Directives issued in the European Union context have led the member states to legislate in order to strengthen security measures for critical infrastructures, which, in the event of their destruction or disruption, would have catastrophic consequences not only for the state itself, but also for neighbours and other states.
This essay aims to show part of what has been done in Portugal in the field of national critical infrastructures protection, as well as to ask some questions concerning the responsibility of the owners/operators, in order to point out some guidelines for the defence of the national interest.

Keywords: security policies, national critical infrastructures, protection, security liaison officer, liability

Após os atentados terroristas do início deste século, a União Europeia (UE) aumentou a sua preocupação com a protecção das infra-estruturas críticas no âmbito da luta contra o terrorismo. Cada Estado-membro tem um papel importante a desempenhar, não só quanto às suas próprias infra-estruturas, mas também em relação aos restantes Estados-membros. A política europeia estabelecida revela-se atenta a vários tipos de ameaças, desde as intencionais às de origem natural. Cabe, no entanto, a cada Estado reflectir, no seu território, essa política europeia.

O objectivo principal deste artigo é a sensibilização dos especialistas em segurança e, quiçá, da sociedade em geral para temática da protecção de infra-estruturas críticas.

Tendo em conta a manifesta preocupação da União Europeia com a protecção das respectivas infra-estruturas críticas, a actual legislação portuguesa, seguindo a Directiva Europeia, impõe a existência de um agente de ligação de segurança para cada infra-estrutura crítica, o qual deverá cumprir todos os requisitos da categoria de director de segurança, previstos no regime jurídico da actividade de segurança privada. Neste contexto, o interesse do autor em elaborar um estudo académico da matéria em questão é imediatamente justificado, pois a referida função poderá ser exercida a um nível tão elevado quanto maior for o conhecimento adquirido.

Por fim, ir-se-ão apontar alguns aspectos a melhorar no contexto nacional português no que à protecção de infra-estruturas críticas diz respeito.

1. Protecção das Infra-estruturas Críticas: Programa Europeu

«As infra-estruturas críticas da UE estão cada vez mais interligadas e interdependentes, tornando-se mais vulneráveis às rupturas ou à sua destruição» (União Europeia, 2005).

O terrorismo é a principal preocupação. Os atentados de 11 de Setembro de 2001 deram uma nova dimensão a um problema que não era novo. Os ataques de Madrid e Londres, em 2004 e 2005, respectivamente, confirmaram a necessidade de agir em defesa de infra-estruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade. Embora recentemente tenham aumentado as preocupações com catástrofes naturais, como fenómenos sísmicos,

iremos, no entanto, concentrar a atenção, no presente estudo, na ameaça terrorista e nos ciberataques, ou seja, acções intencionais, não deixando, todavia, de abordar a protecção de infra-estruturas críticas de forma holística.

A interdependência registada entre as múltiplas infra-estruturas críticas obriga a cuidados redobrados e contínuos, pois «a sua inoperacionalidade prolongada causa prejuízos tremendos à economia devido à paralisação das actividades estratégicas, podendo por em causa a capacidade de resposta dos Estados» (ANPC, 2013).

No âmbito da luta contra o terrorismo, a União Europeia manifestou, em 2004, a intenção de estabelecer um Programa Europeu para a Protecção das Infra-estruturas Críticas (PEPIC). Foi aqui que começou a ser definida, a nível europeu, uma política de segurança em relação à protecção de infra-estruturas críticas ou pontos sensíveis, como anteriormente eram mais conhecidos. Este programa visava a elaboração de uma estratégia global, em termos europeus, para proteger as infra-estruturas críticas.

Em Junho de 2004, o Conselho Europeu solicitou à Comissão (apesar de a Organização do Tratado do Atlântico Norte já anteriormente dedicar atenção a esta matéria) o estabelecimento de uma estratégia global para a Protecção de Infra-estruturas Críticas (PIC) (CCU, 2004). No fim desse mesmo ano, em Outubro, a Comissão propôs ao Conselho a elaboração do Programa Europeu para a Protecção das Infra-estruturas Críticas. Mais tarde, em Novembro de 2005, a Comissão apresenta o denominado Livro Verde relativo ao PEPIC (CCU, 2005). Passado um ano, em Dezembro de 2006, foi emanada uma Comunicação da Comissão relativa a um Programa Europeu para a Protecção das Infra-estruturas Críticas (CCU, 2006), «abrangendo especialmente a protecção das Infra-estruturas Críticas Nacionais, cuja responsabilidade recai sobre os países a que pertencem, recomendando a elaboração de Programas Nacionais de PIC» (Pais, Sá & Gomes, 2007: 68), isto é, programas nacionais de protecção de infra-estruturas críticas.

1.1. Definição de Infra-estrutura Crítica

Em 2008, no Jornal Oficial da União Europeia, é publicada a Directiva 2008/114/CE, do Conselho, implicando uma série de medidas a ser tomadas pelos Estados-membros. No texto desta directiva define-se

infra-estrutura crítica (IC) como «o elemento, sistema ou parte deste situado nos Estados-membros que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo num Estado-membro, dada a impossibilidade de continuar a assegurar essas funções» (União Europeia, 2008).

1.2. Definição de Infra-estrutura Crítica Europeia

No mesmo documento é também definido o que se entende por infra-estrutura crítica europeia (ICE), sendo esta «a infra-estrutura crítica situada nos Estados-membros cuja perturbação ou destruição teria um impacto significativo em pelo menos dois Estados-membros. O significado do impacto deve ser avaliado em função de critérios transversais, incluindo os efeitos resultantes de dependências intersectoriais em relação a outros tipos de infra-estruturas» (União Europeia, 2008).

De salientar que esta directiva atribui a responsabilidade pela protecção das infra-estruturas críticas europeias aos Estados-membros e aos proprietários/operadores dessas infra-estruturas.

1.3. Identificação de Sectores

Como vimos, a diretiva europeia destaca a importância da proteção das infraestruturas críticas pelo facto de serem essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade. Posto isto, torna-se necessário definir os setores estratégicos nacionais que lhes estão associados.

São vários os setores que envolvem um programa nacional de proteção de infraestruturas críticas. No entanto, inicialmente, em termos de política europeia, a Diretiva 2008/114/CE, já referida, concentra-se nos setores da energia e dos transportes, prevendo, aquando da sua revisão, caso se entenda necessário, a eventual inclusão de outros setores, designadamente o das Tecnologias da Informação e Comunicação (TIC).

Como adiante veremos, a diretiva europeia deu origem, em Portugal, a legislação nacional. Muitos dos termos utilizados na diretiva, quanto à matéria em análise, são transcritos para o Diário da República. Na descrição dos setores da energia e dos transportes, é notória a semelhança:

«Sector da energia:

a) Infra-estruturas e instalações de produção e de transporte de electricidade;

b) Infra-estruturas de produção, refinação, tratamento, armazenagem e transporte de petróleo por oleodutos;

c) Infra-estruturas de produção, refinação, tratamento, armazenagem e transporte de gás por gasodutos e terminais para gás natural em estado líquido (GNL).

(…)

Sector dos transportes:

a) Transportes rodoviários;

b) Transportes ferroviários;

c) Transportes aéreos;

d) Transportes por vias navegáveis interiores;

e) Transportes marítimos, incluindo de curta distância, e portos» (Portugal, 2011: 2624-2625).

Efectivamente, o anexo I da directiva europeia descreve os sectores, em termos gerais, da mesma forma que a legislação portuguesa.

Poder-se-á questionar a razão da escolha destes sectores numa primeira fase. Mas, de acordo com Isabel Pais e Francisco Sá (2009: 40), apesar da necessidade de preocupação com todos os sectores estratégicos nacionais, justifica-se a prioridade nestes sectores anteriormente referidos pelo facto de ser «o conjunto de sectores de que todos os restantes mais dependem para o seu normal funcionamento».

1.4. Riscos

Partindo do princípio de que a criticidade de uma infra-estrutura não depende necessariamente do seu valor económico, podendo ser a função que desempenha o que maior valor pode ter para um Estado, os riscos são de vária ordem. «Hoje é possível paralisar um Estado à custa, por exemplo, de um apagão informático, e a Internet constitui – situação pouco confortável – um veículo de recrutamento de terroristas e uma fonte de informação para escolha de alvos e de infra-estruturas vulneráveis a esse tipo de ameaças» (Almeida, 2013: 17).

Sendo o risco considerado como o resultado do produto da ameaça, vulnerabilidade e consequência (risco = ameaça x vulnerabilidade x consequência), competirá a quem protege a responsabilidade de mitigar esse mesmo risco, reduzindo as vulnerabilidades e minimizando as consequências, em função da ameaça envolvida. É certo que a total eliminação do risco levaria provavelmente à inviabilização de determinada infra-estrutura; no entanto, é sempre possível fazer uma gestão do risco.

2. Protecção das Infra-Estruturas Críticas: Portugal

Sabendo que existem em Portugal, de acordo com o site da Autoridade Nacional de Protecção Civil, 11.600 infra-estruturas inventariadas até ao momento (ANPC, 2013), apenas uma pequena parcela, cerca de 2,5%, foi classificada como pertencente ao grupo das que são críticas. No entanto, «destas, cerca de metade pertencem aos sectores da energia e transportes. O sector das comunicações/tecnologias da informação e comunicação representa também uma fatia importante das Infra-estruturas críticas nacionais» (ANPC, 2013). Deste grupo, tendo em conta o compreensível elevado grau de classificação de confidencialidade da informação, poder-se-á estimar uma dúzia de infra-estruturas críticas europeias em território nacional português.

2.1. Legislação Nacional

Em Portugal, só em Maio de 2011, através do Ministério da Defesa Nacional, foi emanado o Decreto-Lei nº 62/2011 de 9 de Maio (Portugal, 2011), transpondo a já referida Directiva nº 2008/114/CE, do Conselho, de 8 de Dezembro. Este decreto-lei «estabelece os procedimentos de identificação e de protecção das infra-estruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes» (Portugal, 2011: 2624).

Ficou igualmente estabelecido no referido decreto-lei que compete ao Conselho Nacional de Planeamento Civil de Emergência conduzir de forma permanente o processo de identificação das potenciais infra-estruturas críticas europeias. Ora, em função da recente reestruturação de organismos públicos, a Autoridade Nacional de Protecção Civil (ANPC) passou a ser a detentora das atribuições do mencionado Conselho Nacional de Planeamento Civil de Emergência.

Apesar da directiva europeia estar vocacionada exclusivamente para a protecção de infra-estruturas críticas europeias, o âmbito da legislação foi alargado, atendendo ao artigo 17º do supracitado decreto-lei, o qual «prevê igualmente a aplicação dos mesmos procedimentos às infra-estruturas críticas nacionais» (ANPC, 2013), ou seja, todas as infra-estruturas críticas estão abrangidas.

A título de exemplo, atendendo à proximidade, interessa referir que a legislação espanhola, em matérias de protecção de infra-estruturas críticas, estabeleceu igualmente o âmbito da sua aplicação a todo o território nacional (Espanha, 2011a; Espanha, 2011b).

O mais recente Conceito Estratégico de Defesa Nacional, publicado em Diário da República em Abril de 2013 (Portugal, 2013), onde são definidos «os aspectos fundamentais da estratégia global a adoptar pelo Estado para a consecução dos objectivos da política de segurança e defesa nacional» (Portugal, 2013: 1981), demonstra preocupação com a protecção das infra-estruturas críticas. Quando elencadas as principais ameaças de natureza global, as quais podem pôr em causa a segurança de Portugal, o terrorismo é assinalado em primeiro lugar. De igual forma, no contexto de ameaças, é ainda referida a «cibercriminalidade, porquanto os ciberataques são uma ameaça crescente a infra-estruturas críticas, em que potenciais agressores (terroristas, criminalidade organizada, Estados ou indivíduos isolados) podem fazer colapsar a estrutura tecnológica de uma organização social moderna» (Portugal, 2013: 1985).

Efectivamente, o Conceito Estratégico de Defesa Nacional define a estratégia a implementar para atingir os objectivos de segurança e defesa nacional. Em nosso entender, hodiernamente, a designação mais acertada seria conceito de segurança nacional, tal como advoga José Nunes da Fonseca (2011). Isto se se atender à realidade actual, mas também à percentagem de vezes que, no texto, a palavra segurança supera em quantidade a palavra defesa; são mais de 50%. Pondo de parte, por agora, estes pormenores, note-se que, de forma a responder às ameaças e riscos assinalados, são estabelecidas algumas prioridades. Assim, o referido conceito estratégico, uma vez mais no campo do combate ao terrorismo, estabelece que «para responder eficazmente à ameaça das redes terroristas, Portugal deve desenvolver uma estratégia nacional e integrada que articule medidas diplomáticas, de controlo financeiro, judiciais, de informação pública e de informações, policiais

e militares. Deve ainda atribuir especial atenção à vigilância e controlo das acessibilidades marítima, aérea e terrestre ao território nacional. Neste domínio, adquire grande acuidade a implementação de um Programa Nacional de Proteção das Infraestruturas Críticas» (Portugal, 2013: 1990).

Do anteriormente exposto, imediatamente se chega a uma conclusão: ainda não foi implementado, em Portugal, um programa nacional de proteção de infraestruturas críticas. Caso contrário, não seria sugerida a sua implementação. Sabendo que os esforços desenvolvidos pela ANPC para a elaboração do mesmo têm sido frutuosos, a conclusão do programa nacional ainda não tem fim à vista.

É certo que essa implementação pressupõe a conclusão de um processo que passa pela identificação e classificação das infra-estruturas críticas, estudo e difusão de medidas a tomar para reforçar a sua proteção e, por fim, implementação das medidas necessárias, associadas à monitorização do risco (Pais & Sá, 2009: 39). Embora grande parte deste processo já tenha sido desenvolvido, falta completá-lo.

Por outro lado, ainda no conceito estratégico de defesa nacional, é referido que, «no domínio da cibercriminalidade, impõe-se uma avaliação das vulnerabilidades dos sistemas de informação e das múltiplas infraestruturas e serviços vitais neles apoiados. Neste domínio, definem-se como linhas de ação prioritárias: garantir a proteção das infraestruturas de informação críticas, através da criação de um Sistema de Proteção da Infraestrutura de Informação Nacional (SPIIN)» (Portugal, 2013: 1990). Mais à frente, ainda no mesmo texto, é também referida a prioridade em «sensibilizar os operadores públicos e privados para a natureza crítica da segurança informática e levantar a capacidade de ciberdefesa nacional» (Portugal, 2013: 1990).

Posto isto, uma vez mais se conclui pela falta de implementação de medidas que garantam a proteção de infraestruturas críticas, neste caso, em especial, no domínio da cibercriminalidade.

2.2. Agentes de Ligação de Segurança

O Decreto-Lei nº 62/2011 de 9 de maio (Portugal, 2011), já anteriormente mencionado, estabeleceu, a nível nacional, a necessidade de cada infra-estrutura crítica europeia dispor de um agente de ligação de segurança, designado pelo operador, transpondo uma vez mais a diretiva europeia para o quadro nacional. Este elemento fundamental

na proteção de uma infra-estrutura crítica europeia é identificado como aquele que tem a responsabilidade de representar o operador de uma determinada infraestrutura crítica europeia em matérias de segurança, sendo o ponto de contacto com o Secretário-Geral do Sistema de Segurança Interna (SGSSI). Este último é representado pela força de segurança territorialmente competente.

Um aspecto a que interessa dar relevo é o facto de cada um destes agentes de ligação de segurança dever, por lei, «cumprir todos os requisitos da categoria de director de segurança previstos no regime jurídico da actividade de segurança privada» (Portugal, 2011: 2626). Ora, atendendo ao Despacho nº 26205/2009 de 30 de Novembro (Portugal, 2009), o qual estabelece a estrutura curricular e o plano de estudos da licenciatura em Estudos de Segurança, ministrada na Universidade Lusófona de Humanidades e Tecnologias, mas tendo também em devida consideração o Despacho do Departamento de Segurança Privada da Polícia de Segurança Pública, com data de 28 de Março de 2013, é reconhecida ao licenciado em Estudos de Segurança, embora com as definidas unidades curriculares obrigatórias, a habilitação para o exercício da actividade de director de segurança, nos termos previstos no regime jurídico do exercício de segurança privada. Assim sendo, os licenciados em Estudos de Segurança estarão na linha da frente para exercer a função de agente de ligação de segurança, possibilitando uma abordagem mais profunda em matéria de segurança das infra-estruturas críticas. É certo que o regime jurídico da segurança privada não obriga o titular do cargo de director de segurança a ser detentor de um grau académico. No entanto, para além da eventual experiência obtida em anos de trabalho na área de segurança, o estudo aprofundado em termos académicos confere aos licenciados uma visão holística da segurança que, com toda a certeza, trará benefícios aos operadores de infra-estruturas críticas, aos cidadãos nacionais e, por que não, aos europeus.

2.3. Responsabilidade na Protecção

Sabendo que a maioria das infra-estruturas críticas em Portugal é do domínio privado, isto é, os donos/operadores são empresas privadas, de quem será a responsabilidade de proteger os cidadãos de riscos inaceitáveis? Certamente que, em primeira instância, caberá ao Estado. «Daí que seja hoje incontornável que a implementação de políticas

PIC passa, cada vez mais, por uma intensa e contínua cooperação entre os Sectores Público e Privado, onde ambas a partes (Estado e donos/operadores ou stakeholders) devem reconhecer e aceitar a sua quota de responsabilidade no reforço de um bem comum como a Segurança» (Pais, Sá & Gomes, 2007: 74).

Podemos sempre esperar que a cooperação exista, mas, para além dela, tem de existir responsabilidade. Se o Estado não pode actuar na propriedade privada, tem de encontrar a forma de levar esses privados a atingirem o nível adequado de segurança. É o Bem-Estar da Nação que está em causa.

De acordo com António Almeida (2011), numa das metodologias possíveis de utilizar, que não nos interessa desenvolver para este artigo, em função do índice de criticidade apurado, a urgência em proteger determinada infra-estrutura pode ser classificada em quatro categorias:

1. urgência absoluta: a infra-estrutura, no caso de sofrer um impacto destrutivo ou disruptivo, apresenta consequências catastróficas que põem em causa o Bem-Estar da Nação, pelo que a sua protecção é indispensável e urgente;
2. urgência alta: a infra-estrutura, no caso de sofrer um impacto destrutivo ou disruptivo, apresenta consequências imprevisíveis que podem pôr em causa o Bem-Estar da Nação, pelo que a sua protecção é necessária e urgente;
3. urgência intermédia: a infra-estrutura, no caso de sofrer um impacto destrutivo ou disruptivo, apresenta consequências potencialmente significativas que podem pôr em causa o Bem-Estar da Nação, pelo que a sua protecção deve ser monitorizada;
4. urgência baixa: a infra-estrutura, no caso de sofrer um impacto destrutivo ou disruptivo, não apresenta consequências que possam pôr em causa o Bem-Estar da Nação, pelo que a sua protecção deve ser adequada aos seus propósitos.

Efectivamente, conforme se pode concluir da tabela anterior, numa determinada infra-estrutura em que a sua protecção seja classificada com categoria de urgência absoluta ou alta, as mais graves, no caso de sofrer um impacto destrutivo ou disruptivo, em que as consequências podem ser imprevisíveis ou garantidamente catastróficas, de quem será a responsabilidade do resultado no caso de nada ter sido feito em

termos de protecção? Já vimos, anteriormente, que a directiva europeia estabelece a responsabilidade da protecção das infra-estruturas críticas europeias aos Estados-membros e aos operadores. Mas em que percentagem? Será maior a responsabilidade do Estado ou do operador?

É natural que uma parte dos operadores, por sua própria iniciativa e em função da consciência individual, tenha dado início à sua protecção. Mas de que forma? Qual será a metodologia mais adequada? Estarão todos em sintonia ou cada um faz o que achar suficiente?

Atendendo ao facto de 10% das infra-estruturas críticas nacionais estarem concentradas no Complexo Industrial de Sines, foi em 2011 apresentado um conjunto de propostas vocacionado para a redução do risco sísmico. Entre estas, uma delas desperta especial atenção, quando falamos em matéria de responsabilidade do Estado: «proceder a uma revisão e melhoria profunda da capacidade do Estado para cumprir e fazer cumprir a regulamentação que ele próprio criou» (Pais et al., 2011: 21). Embora o artigo em que se apresentam estas propostas seja vocacionado para o risco sísmico, esta, em especial, encaixa perfeitamente em qualquer outro risco de que as infra-estruturas já deveriam estar protegidas.

Reflexões / Conclusões

Enquanto os países europeus não estiverem, de igual forma, sensíveis ao problema, dificilmente o resultado será satisfatório. O esforço desenvolvido por um determinado Estado-membro poderá resultar de modo inglório, caso não exista, por parte de outro, um cuidado adequado na implementação da protecção das suas infra-estruturas críticas europeias. Como refere a directiva europeia de 2008, a cooperação entre os Estados-membros constitui um meio adequado e eficaz no tratamento de infra-estruturas críticas transfronteiriças. É nessa cooperação que assenta o Programa Europeu para a Protecção das Infra-estruturas Críticas. Também neste campo, o agente de ligação de segurança de cada infra-estrutura crítica tem um papel a desempenhar, como elemento facilitador da cooperação e comunicação com as autoridades nacionais competentes nesta área.

Os desafios que se afiguram para implementar uma verdadeira protecção de infra-estruturas críticas são de vária ordem. Provavelmente, a inexistência em Portugal de uma autoridade nacional que determine «procedimentos reguladores, fiscalizadores, consultores e de coordenação/cooperação bilateral (e.g. com Espanha) e com a UE» (Pais & Candeias, 2010: 34) implica um atraso no processo de implementação do programa nacional para a protecção de infra-estruturas críticas. A título de exemplo, já em Espanha, a legislação criada a partir da directiva europeia deu origem ao «Centro Nacional para la Protección de las Infraestructuras Críticas como órgano de asistencia al Secretario de Estado de Seguridad en la ejecución de las funciones que se le encomiendan a éste como órgano responsable del sistema» (Espanha, 2011a).

O sector privado, sendo o maior detentor/operador das infra-estruturas críticas, denota alguma relutância em investir em segurança. Uma hipótese a considerar seria a existência de um incentivo financeiro por parte da União Europeia para a implementação e manutenção de medidas de protecção de infra-estruturas críticas. Se, numa primeira fase de implementação, o investimento em equipamentos de segurança poderá ser de alguma forma mais elevado, é certo que a protecção é contínua, implicando um contínuo investimento, a bem da Comunidade.

Provavelmente existirão infra-estruturas que, pela sua localização, implicam um maior esforço e investimento para se operar a sua protecção. Naturalmente, nalgumas destas, a deslocalização resultaria num menor risco e, consequentemente, num menor investimento. «É necessário renovar as infra-estruturas existentes e, se possível, deslocar as infra-estruturas críticas para zonas onde os potenciais danos seriam menores» (Almeida, 2013: 23).

Por fim, sensibilizar é a palavra de ordem. Tal como dissemos no início, é objectivo deste artigo sensibilizar não só os especialistas em segurança, mas a sociedade em geral. Tal como foi apelado no primeiro Congresso Nacional de Segurança e Defesa, em 2009, a estratégia nacional de segurança e defesa tem de ser um problema de todos, ou seja, é também um assunto da sociedade. Todos os portugueses são chamados a contribuir para a optimização dos recursos existentes (João, Lobo & Bação, 2013: 177). Assim, Portugal poderá ser um país mais seguro.

Referências Bibliográficas

Almeida, A. (2011). *Metodologia Multicritério de Identificação e Priorização de Infra-estruturas*. Online: <https://dspace.ist.utl.pt/bitstream/2295/937257/1/Dissertacao.pdf> (referência de 18-03-2013).

Almeida, P.P. (2013). "Políticas de Segurança Nacional". In: P.P. de Almeida (ed.), *Como Tornar Portugal um País Seguro? Segurança Nacional e Prevenção da Criminalidade*. [S.l.]: Bnomics, pp. 11-34.

ANPC [Autoridade Nacional de Proteção Civil] (2013). *Infraestruturas Críticas*. Online: <http://www.proteccaocivil.pt/RiscosVulnerabilidades/Pages/InfraestruturasCriticas.aspx> (referência de 18-03-2013).

CCU [Comissão das Comunidades Europeias] (2004). *Comunicação da Comissão ao Conselho e ao Parlamento Europeu - Protecção das infra-estruturas críticas no âmbito da luta contra o terrorismo*. Online: <http://www.umic.pt/images/stories/publicacoes6/Comunicacao_COM(2004)%20702% 0final.pdf> (referência de 18-03-2013).

CCU (2005). *Livro Verde - Relativo a um Programa Europeu de Protecção das Infra-estruturas Críticas*. Online: <http://eur-lex.europa.eu/LexUriServ/site/pt/com/2005/com2005_0576pt01.pdf> (referência de 18-03-2013).

CCU (2006). *Comunicação da Comissão - relativa a um Programa Europeu de Protecção das Infra-estruturas Críticas*. Online: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:PT:PDF> (referência de 18-03-2013).

Espanha (2011a). *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*. Online: <http://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf> (referência de 10-05-2013).

Espanha (2011b). *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas*. Online: <http://www.boe.es/boe/dias/2011/05/21/pdfs/BOE-A-2011-8849.pdf> (referência de 10-05-2013).

Fonseca, J.N. (2011). "Conceito de Segurança Nacional perspectivado para 2030". *Boletim Ensino / Investigação*, nº 11, pp. 81-115.

João, P.; Lobo, V. & Bação, F. (2013). "Modelo Preditivo da Criminalidade". In: P.P. de Almeida (ed.), *Como Tornar Portugal um País Seguro? Segurança Nacional e Prevenção da Criminalidade*. [S.l.]: Bnomics, pp. 139-182.

Pais, I. & Candeias, J. (2010). "O Significado da Transposição para Portugal da Directiva Europeia". *Planeamento Civil de Emergência*, nº 22, pp. 30-37.

Pais, I. & Sá, F.M.; (2009). "Paradigmas da Protecção de Infra-estruturas Críticas e o Estado da Arte em Portugal". *Planeamento Civil de Emergência*, nº 21, pp. 36-42.

Pais, I.; Sá, F.M. & Gomes, H. (2007). "Protecção de Infra-estruturas Críticas - A Cooperação Público-Privada". *Riscos Públicos e Industriais*, vol. I, pp. 65-83.

Pais, I.; Sá, F.M.; Lopes, M. & Oliveira, C.S. (2011). "Infraestruturas Críticas: Propostas para a Redução do Risco Sísmico". *Planeamento Civil de Emergência*, nº 23, pp. 16-21.

Portugal (2009). "Despacho nº 26205/2009 de 30 de Novembro". *Diário da República*, 2ª série, n.º 232, 30 de Novembro, pp. 48908-48910.

Portugal (2011). "Decreto-Lei nº 62/2011 de 9 de Maio". *Diário da República*, 1ª série, n.º 89, 9 de Maio, pp. 2624-2627.

Portugal (2013). "Resolução do Conselho de Ministros n.º 19/2013". *Diário da República*, 1ª série, n.º 67, 5 de Abril, pp. 1981-1995.

União Europeia (2005). *Recomendação do Parlamento Europeu ao Conselho Europeu e ao Conselho sobre a protecção das infra-estruturas críticas no âmbito da luta contra o terrorismo (2005/2044(INI)*. Online: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:124E:0250:0253:PT:PDF (referência de 18-03-2013).

União Europeia (2008). *Directiva 2008/114/CE do Conselho, de 8 de Dezembro de 2008, relativa à identificação e designação das infra-estruturas críticas europeias e à avaliação da necessidade de melhorar a sua protecção*. Online: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:PT:PDF> (referência de 08-03-2013).