Cultura de la información

Quando o direito à informação colide com a segurança nacional

Maria João Albuquerque
Universidade Nova de Lisboa
Portugal · mjdalb@gmail.com

Rui Moura
Guarda Nacional Republicana, Revista Militar
Portugal · ruimoura.ri14@gmail.com

Resumo: Existe um equilíbrio, difícil de alcançar, entre o direito à informação e a segurança da sociedade. O primeiro diz respeito à liberdade de criar, armazenar e partilhar conhecimento, fator essencial para o desenvolvimento civilizacional. Mas o livre acesso à informação pode colocar em risco a segurança do Estado, das populações, das instalações críticas e do território. A civilização apenas terá futuro se for resiliente às ameaças e ataques de espiões, terroristas e criminosos.
Enquanto o assunto é amplamente debatido nos EUA, Canadá e Reino Unido, existindo regras para o tratamento de informação sensível mas não classificada, ao restante nível Europeu pouco ou nada existe.
Pretende-se nesta comunicação analisar os desafios que se colocam aos profissionais de informação na forma de tratar e difundir informação sensível mas não classificada, em termos de confidencialidade, integridade e disponibilidade, de forma abrangente tendo em consideração os riscos que ameaçam a sociedade.

Palavras-chave: Direito à Informação; Segurança Nacional; Política de Informação; Terrorismo; Portugal.

Abstract: There is a fine balance, difficult to achieve, between the right to information and national security. The former concerns the freedom to create, store and share knowledge, an essential factor for civilization development. But free access to information can jeopardize national, community, people, critical infrastructure and territorial securities. Civilization has a future only if it is resilient to threats and attacks from spies, terrorists and criminals.
While these issues are widely debated in the US, Canada and the UK, with standing rules for the treatment of information sensitive but unclassified, at the continental European level there is little or nothing.
It is intended in this paper to analyse the challenges faced by information professionals in the processing and dissemination of sensitive information, but not classified in terms of confidentiality, integrity and availability, in a comprehensive way taking into account the risks to society.

Keywords: Right to Information; National Security; Information Policy; Terrorism; Portugal.

Introdução

O terrorismo como fenómeno global afeta todas as Nações e todas as comunidades. A utilização da internet com fins terroristas não tem em consideração as fronteiras nacionais, amplificando o impacto potencial nas suas vítimas (ONU 2012, p.v). Assim deve ser incrementada a colaboração entre os Estados de forma a promover um melhor conhecimento das más utilizações da internet no recrudescimento, desenvolvimento e apoio de atos terroristas, garantindo respostas coordenadas ao nível da justiça criminal.

Propomo-nos nesta comunicação abordar as questões relativas ao acesso à informação, excluindo dessa análise as matérias classificadas que, em Portugal, são devidamente tratadas no âmbito da Lei do Segredo de Estado, das Resoluções do Conselho de Ministros (RCM) que aprovaram as várias Normas SEGNAC e as matérias de segurança relacionadas com as Forças Militares que aplicam, no seu universo, o SEGMIL[1], para além de outros normativos de organizações internacionais de que Portugal é membro, como por exemplo a Organização do Tratado do Atlântico Norte e União Europeia[2].

Efetuou-se o levantamento da legislação portuguesa referente ao Acesso à Informação Administrativa e à Proteção de Dados, inserindo-a no contexto mundial, estudaram-se os normativos e os Códigos de Ética dos profissionais da informação, efetuou-se o levantamento dos principais desafios e ameaças dos Estados no âmbito da segurança interna face ao desenvolvimento da sociedade da informação, procurando identificar as medidas que Portugal está a adotar no âmbito da segurança da informação. Finalmente, procedeu-se à análise de todas as reflexões feitas sobre as questões levantadas pelo objeto de estudo, procurando apontar pistas para o tratamento e difusão de informação considerada sensível em termos de segurança nacional e internacional.

O acesso à informação e o pós 11 de setembro

A tendência generalizada no mundo ocidental, ao longo do século XX, para a promoção de administrações abertas, reconhecendo aos cidadãos o direito de consultarem toda a documentação que diga respeito à sua pessoa, bem como qualquer informação existente sobre questões do seu interesse, levou a que se criassem leis nacionais que garantissem o acesso à informação administrativa, das quais é exemplo o Freedom of Information Act (FOIA) dos EUA (1967).

Por outro lado, o desenvolvimento da internet alterou completamente o paradigma da comunicação científica e da circulação do conhecimento, permitindo veicular de forma fácil e ampla informação sensível para a segurança das populações, das instalações críticas e do território, inclusive para quem, com intuitos malignos, pretende por em causa essa segurança através de atos terroristas ou criminosos.

O movimento do acesso aberto tem por missão aumentar a visibilidade, acessibilidade e difusão dos resultados da atividade académica e da investigação científica, de uma forma gratuita e online, englobando documentos como artigos de revistas científicas, comunicações em conferências, relatórios técnicos, teses e documentos de trabalho, estando o seu acesso limitado apenas pelo código dos direitos de autor, não sendo o seu conteúdo escrutinado em termos de sensibilidade dos dados, isto apesar do regime jurídico de instituições de investigação científica (DL nº125/99, de 20 de abril) referir que a divulgação dos resultados da atividade científica e tecnológica deve estar sujeita à "reserva de confidencialidade" (al a., nº 1, artº 13º - A difusão da cultura científica e tecnológica).

Igualmente tem-se verificado a nível das organizações uma exposição na net das suas características e vulnerabilidades, a par da exposição nas redes sociais dos

[1] Aprovado por despacho conjunto, de 16 de Outubro de 1986, do Conselho de Chefes de Estado-Maior (CCEM), para substituir o publicado pela Portaria nº 17128, de 17 de Abril de 1959 (SEGMIL, 1986)

[2] De acordo com o SEGNAC 1 a matéria classificada é definida como "toda a informação, notícia, material, ou documento que, se for do conhecimento de indivíduos não autorizados, pode fazer perigar a segurança nacional dos países aliados ou de organizações de que Portugal faça parte." (Anexo A).

indivíduos, que podem ser aproveitadas por criminosos ou terroristas no âmbito das suas finalidades.

Face a esta conjuntura, e aos recrudescimentos do crime organizado internacional e da ameaça terrorista das últimas décadas, a Administração americana tomou medidas de restrição no acesso à informação, como são os casos das leis designadas por "USA Patriot Act de 2001" e "Homeland Security Act de 2002", no âmbito da preocupação acrescida para assegurar a segurança interna do Estado.

Depois do 11 de setembro [de 2001] o Governo federal norte-americano retirou do acesso público mais de 6600 documentos técnicos, que tinham estado disponíveis, no domínio público, desde a década de 1960, por conterem dados que poderiam hipoteticamente fornecer pistas a terroristas para a produção de armas biológicas e químicas. Simultaneamente pediu ainda à Sociedade Americana de Microbiologia que restringisse a publicação de informação sensível que pudesse ser utilizada por grupos terroristas (Abbas, 2006). Estas medidas que chocaram a comunidade científica, que argumentou que as mesmas colocavam em causa a partilha de novas descobertas que poderiam permitir avanços científicos, sugerem-nos uma reflexão sobre os desafios que o desenvolvimento da sociedade da informação trouxe para a segurança dos Estados, face às ameaças da espionagem, do terrorismo e do crime organizado, colocando na ordem do dia a questão relativa ao equilíbrio que é necessário estabelecer entre a preocupação de um governo em controlar a informação passível de colocar em risco a segurança do Estado, das populações, das instalações críticas e do território, e também os dados pessoais e a privacidade dos cidadãos, com o direito em aceder livremente à informação.

Enquanto o assunto tem sido amplamente debatido nos EUA, existindo regras para o tratamento de informação não classificada com necessidade de controlo de acesso [Controlled Unclassified Information - CUI], ao nível Europeu pouco ou nada existe. Ao nível Comunitário foi criada uma Agência – a Agência Europeia para a Segurança das Redes e da Informação (ENISA) – com o objetivo de garantir a segurança dos utilizadores das redes e sistemas de informação, preocupada essencialmente com a vulnerabilidade dos canais de transmissão mas não com o conteúdo da informação em si [site ENISA]. Portugal está representado nesta agência através do Diretor-Geral do Gabinete Nacional de Segurança (GNS), entidade que tem por missão principal de garantir a segurança da informação classificada[3], regulamentando o tratamento de informação oficial classificada, inclusivamente a veiculada através de redes informáticas, sem no entanto abordar a questão da classificação e tratamento de possíveis conteúdos sensíveis mas não classificados contidos nessa mesma informação.

Em Portugal foi estabelecida uma designada Estrutura Nacional de Segurança da Informação (ENSI), iniciativa do XVI Governo, de que decorreu a elaboração em 2005 de três documentos: "Política Nacional de Segurança da Informação", "Carta de Segurança de Informação", "Política de Segurança da Informação da Entidade", mas cujas matérias se situam essencialmente no âmbito de segurança das TIC, no entanto nunca foram desenvolvidos nem publicados os documentos propostos, nem efetuada a promoção de uma cultura nacional de segurança como era sugerido.

O Acesso aos Documentos Administrativos em Portugal

No caso dos documentos administrativos existe todo um universo de documentos que contêm matérias sensíveis mas não classificadas ao abrigo das normas existentes, cujo conteúdo obsta a que o seu acesso seja universal e a sua difusão aberta, são disto exemplo matérias que englobam informação em segredo de justiça, dados pessoais de cidadãos e da sua privacidade, reserva da propriedade intelectual ou segredos comerciais, industriais ou sobre a vida interna de empresas, entre outras.

Portugal regulou o acesso e a reutilização dos documentos administrativos através da Lei n.º 46/2007, Lei de Acesso aos Documentos Administrativos (LADA), de 24 de agosto, revogando a norma anterior cuja primeira versão é de 1993 (Lei n.º 65/93, de 26 de agosto), transpondo para a ordem jurídica nacional a Diretiva n.º 2003/98/CE, do

[3] Despacho 16792/2013, de 27 de Dezembro

Parlamento e do Conselho, que estabelece um conjunto mínimo de regras aplicáveis à reutilização e aos meios práticos de facilitar a reutilização de documentos na posse de organismos do setor público dos Estados-Membros.

A LADA define documento administrativo de forma muito ampla "como qualquer suporte de informação sob forma escrita, visual, sonora, eletrónica ou outra forma material", na posse dos órgãos e entidades públicas, ou detidos em seu nome. (alínea a) do art.º 3º e art.º 4º).

O regime de acesso privilegia valores como a publicidade, a transparência, a igualdade, a justiça e a imparcialidade (art.º 1.º), conferindo: a opção ao cidadão pelo meio de acesso; o acesso à informação efetuado pelo próprio; o de ser assegurada a publicidade da informação; a garantia de que a aplicação das reservas de acesso são feitas com caráter de excecionalidade e proporcionalidade; a marcação de prazos adequados para o acesso; e a reserva da vida pessoal ser confinada aos registos de privacidade (Afonso 2011, p.10), cabendo à CADA, na dependência da Assembleia da República (AR), zelar pelo cumprimento das disposições da LADA (art.º 25.º a 32.º).

Já a Constituição da República Portuguesa, ao referir-se aos direitos e garantias dos administrados, consagra o direito dos cidadãos a serem informados sobre os processos em que sejam diretamente interessados e assegura o direito de acesso à informação administrativa (art.º 268.º).

Por outro lado o novo Código do Procedimento Administrativo de 2015 regula, no seu art.º 17.º, o princípio da administração aberta, definindo que "todas as pessoas têm o direito de acesso aos arquivos e registos administrativos, mesmo quando nenhum procedimento que lhes diga diretamente respeito esteja em curso, sem prejuízo do disposto na lei em matérias relativas à segurança interna e externa, à investigação criminal, ao sigilo fiscal e à privacidade das pessoas." Acrescentando nos artigos 82.º a 85.º os preceitos que regulam os direitos de acesso aos atos da Administração, agregados sob o título de "direito à informação" num capítulo autónomo (art.º 82.º-85.º).

Por outro lado a lei 67/98 de 26 de Setembro – Lei de Proteção de Dados (LPD), que orienta a ação da Comissão Nacional de Proteção de Dados (CNPD), apresenta uma posição mais restritiva no que diz respeito ao acesso a informação respeitante a dados pessoais que, de acordo com este normativo legal, consiste em: "qualquer informação [...] relativa a uma pessoa singular, identificada ou identificável direta ou indiretamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social." (art. 3.º)

Esta definição entra em contradição com aquela apresentada pela LADA, que considera como "«Documento nominativo» o documento administrativo que contenha, acerca de pessoa singular, identificada ou identificável, apreciação ou juízo de valor, ou informação abrangida pela reserva da intimidade da vida privada." (art.º 3.º alínea b)).

Ou seja, enquanto para a CNPD as informações de caráter pessoal, nomeadamente números de identificação, moradas, números de telefone, etc. não podem ser acessíveis ao público, para a CADA ficam resguardadas do acesso apenas por exemplo aquelas respeitantes à vida familiar, conjugal, amorosa e afetiva da pessoa. Esta contradição verificada entre estes dois organismos, e respetiva legislação de suporte, acaba por limitar realmente o acesso à informação, pois obriga o cidadão a recorrer à justiça para encontrar um parecer consensual, com o acréscimo de tempo e encargos financeiros que tal acarreta e, por outro lado, não cumpre verdadeiramente o desígnio da equidade e transparência no acesso à informação, pois este acesso fica dependente de um veredito singular.

Este problema agrava-se quando percebemos que o entendimento sobre as restrições no acesso à informação administrativa também difere entre ambas. Para a CADA estão limitados os documentos contendo informação que coloque em risco a segurança interna e externa do Estado, contendo matérias em segredo de justiça, dados pessoais de terceiros, segredos comerciais, industriais ou sobre a vida interna de uma empresa. Mas mesmo nestes casos os documentos podem ser acedidos parcialmente, depois de expurgada a informação sujeita a restrição, ou, no caso dos

documentos nominativos ou contendo segredos comerciais/industriais, se o interessado demonstrar interesse direto, pessoal e legítimo suficientemente relevante segundo o princípio da proporcionalidade. (art.º 6.º).

Pelo seu lado a CNPD pugna pela reserva quase total, garantia de segurança e controlo escrupuloso no tratamento dos dados pessoais (art.º 15, 16.º e 17.º), constituindo crime a sua violação.

Se para o acesso à documentação de caráter administrativo encontramos esta ambivalência, para o acesso a outro tipo de informação, como por exemplo a de caráter científico ou informação de descrição de funcionamento dos serviços, cujos conteúdos poderão ser igualmente sensíveis e que no momento presente o seu veículo de difusão é o acesso aberto na internet, não existe qualquer documento normativo que o regulamente, prevalecendo apenas os códigos de ética dos profissionais de informação, que na sua generalidade promovem uma difusão aberta e sem restrições de acesso.

Os profissionais da informação e o acesso ao conhecimento

Um profissional de informação tem como principal missão servir o público e a comunidade, garantindo-lhe o acesso à informação, no respeito do artigo 19.º da Declaração Universal dos Direitos do Homem.

O código de ética para os profissionais da informação em Portugal, adotado, em 1999, pela BAD, INCITE e APDIS, defende como valor essencial o acesso à informação, atribuindo a estes profissionais a responsabilidade de prevenir, através de uma atitude de alerta, contínua e exigente, todas as formas de censura (2001). De uma forma geral a maioria dos códigos de ética dos profissionais de informação refletem estes princípios, considerando como sua missão garantir o acesso à informação, ideias e obras de arte, ao conhecimento, pensamento e cultura, enquanto salvaguarda dos valores fundamentais da democracia e dos direitos civis universais, opondo-se a qualquer forma de censura e garantindo a privacidade e o anonimato dos seus utilizadores.

Em sentido contrário à generalidade o Código de Ética da BID - Bibliothek & Information Deutschland Federation - ressalva a divulgação de informação, dados e texto integral, dentro dos limites legais (2007), colocando neste articulado um limite ao acesso, que é o de base legal.

Entendido na primeira forma o papel dos profissionais da informação, resulta numa enorme responsabilidade a tarefa que lhes cabe enquanto promotores do acesso à informação, face aos desafios da sociedade contemporânea, tendo ainda como pressuposto fundamental a emergência das novas tecnologias e a generalização do acesso à informação, graças à banalização do uso da internet.

Face à conjuntura atual de ameaças terroristas, bem como do crime organizado transfronteiriço[4], o contexto português não tem tido sensibilidade para esta questão do controlo do acesso a informação de conteúdo sensível, sendo os normativos muito abrangentes, remetendo os critérios de confidencialidade para a lei geral. No entanto, importa questionar se esta atitude de maior leniência poderá ter consequências negativas ao nível da segurança nacional.

Desafios e ameaças dos Estados no âmbito da segurança interna

O conceito de Segurança Interna tal como é definido na lei portuguesa é a "atividade desenvolvida pelo Estado para garantir a ordem e a segurança públicas, proteger pessoas e bens e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática" (5 Cfr. Nº1 do artigo 1º da Lei nº53/2008, de 29 de Agosto - Lei da Segurança Interna.).

A segurança interna compreende assim da segurança das fronteiras à ordem pública, da proteção civil (prevenir riscos coletivos inerentes a situações de acidente grave ou catástrofe) ao contra terrorismo, da vigilância e obtenção de informações à

[4] Entre outros o narcotráfico, o tráfico de armas, o tráfico de seres humanos, o cibercrime e a pedofilia.

prevenção e combate ao crime, do combate ao narcotráfico à segurança de infra-estruturas críticas, etc.

No entanto a globalização aumentou também os riscos e ameaças, e a noção de pertença dos países a Comunidades mais vastas fazendo com que a segurança interna passando a ser vista de uma forma mais abrangente e ampla, olhando para além-fronteiras. Não é pois de estranhar que a própria União Europeia tenha desenvolvido um conceito e Estratégia de Segurança Interna (ESI), em 2010, complementando assim a estratégia europeia de segurança no que diz respeito à dimensão externa da segurança na Europa de 2003. Nesta ESI foram identificadas uma série de ameaças importantes comuns aos países membros: o terrorismo, em todas as suas formas; as graves formas de criminalidade organizada; a cibercriminalidade; a criminalidade transfronteiras; a violência em si mesma; as catástrofes naturais e as catástrofes provocadas pelo homem (Doc. 7120/10 CO EUR-PREP 8 JAI 182), definindo um modelo de segurança europeu, que integra, nomeadamente, a ação da cooperação entre autoridades policiais e judiciais, a gestão das fronteiras e a proteção civil, no respeito dos valores comuns europeus, como os direitos fundamentais.

Na implementação da estratégia europeia foram colocados vários desafios, desde logo pela crise financeira e as limitações orçamentais daí resultantes. As novas tecnologias forneceram novas oportunidades, mas ao mesmo tempo criaram novas ameaças, incluindo a rápida e crescente ameaça do cibercrime e a necessidade de formulação de uma abordagem abrangente para enfrentar o problema. Paralelamente, as alegações acerca de programas de recolha de informações em grande escala provocaram um intenso debate sobre as condições sob as quais a segurança deve ser atingida, facto que tem, de alguma forma, limitado a adoção de algumas medidas legislativas com impacto direto nesta área. Esta problemática conduziu a uma resolução para salvaguardar a confiança mútua, à definição de políticas de segurança mais inclusivas e à necessidade de reforçar a integração dos direitos fundamentais nas políticas de segurança interna.

A Comissão desenvolveu muito recentemente os passos finais para a revisão da ESI com a definição de uma Agenda Europeia para a Segurança (COM(2015) 185 final, 28 Abr 2015), na qual se pretende reforçar o intercâmbio de informações, a confiança mútua e a cooperação operacional, a partir de toda a gama de instrumentos e políticas da UE, visando também assegurar uma articulação entre as dimensões interna e externa da segurança dando prioridade ao combate ao terrorismo, à criminalidade organizada e à cibercriminalidade como domínios interligados e com forte dimensão transnacional, nos quais a ação da UE pode ter um impacto decisivo. Mas para combater estas prioridades é necessário que as forças e os serviços de segurança dos estados-membros tenham, por um lado, acesso controlado a informação que é normalmente do âmbito da reserva da proteção de dados pessoais, e por outro, que a informação do âmbito da segurança do Estado, da sociedade e do cidadão seja protegida de grupos terroristas e criminosos.

Assim sendo é urgente clarificar a forma como pode ser efetuado pelos cidadãos o acesso a informação produzida, ou na posse da Administração, de conteúdo sensível para a segurança do Estado, da sociedade e do cidadão, tendo em conta a ambiguidade legal que preside a esse acesso. Esta informação cuja sensibilidade de divulgação apenas pode ser avaliada pelo seu produtor não tem em Portugal, nem sequer na Europa, uma estruturação e organização do controlo de acesso semelhante ao caso dos EUA.

Referencial do conceito de informação sensível mas não classificada

Em Portugal, o legislador criou normativos específicos para sustentar as reservas de acesso a informação, onde são exemplo a Lei do Segredo de Estado (LSE), o SEGNAC e o SEGMIL. Complementarmente, colocou normas de excepção na legislação produzida, nomeadamente na do acesso aos documentos administrativos, bem como nas que enquadram setores específicos de atividade ou que pela sua natureza tratam matérias que exigem especial reserva, como as que são reguladas pela LSI e pelo Sistema de Informações da República Portuguesa (SIRP). Mas o país está muito aquém

nos procedimentos de controlo de acesso de informação sensível aos níveis do produtor da informação e da gestão da sua distribuição e acesso, que já são praticados nos EUA.

Na América do Norte verificou-se uma proliferação de marcas de segurança de informação não classificada atingindo cerca de cem designações diferentes: Sensitive But Unclassified (SBU), For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Protected Critical Infrastructure Information (PCII), Sensitive Security Information (SSI), etc., etc. Esta proliferação de marcas gerou disfunções, confusão e dificuldades, sendo inclusivamente uma barreira à difusão de informação aos organismos que dela necessitavam. Disfunções entre organismos estatais, mas também não-estatais, confusão na sua utilização e dificuldades na gestão da proteção de informação sensível mas não classificada. Em 2008, a Administração Bush iniciou um processo normalizador de atribuição de classificação de informação sensível e partilha da mesma, através do Memorando de 7 de maio, definindo a marca Controlled Unclassified Information (CUI), atribuindo a responsabilidade pelo seu desenvolvimento, gestão e controlo, ao departamento federal designado por National Archives and Records Administration (NARA) [http://goo.gl/q7pNUh].

Os procedimentos de salvaguarda e tratamento de informação sensível ficaram assim regulados e normalizados, independentemente do meio suporte de difusão de informação, através da definição e parametrização das possibilidades de classificação, marcação, tratamento, arquivo, e difusão da informação. O desenvolvimento do sistema CUI levou à segmentação das áreas de informação em diferentes categorias, num total de vinte e três (de agricultura a transportes), e cada uma delas subdividida, se necessário, num total de oitenta e duas subcategorias, cada uma destas com uma entidade responsável pela sua gestão de acordo com as orientações gerais da NARA.

Conclusões

Com este estudo pretendemos lançar a discussão para uma temática que envolve não só a comunidade dos profissionais da informação[5], a quem cabe a responsabilidade de facilitar o acesso "a todo o género de informações publicadas sob qualquer suporte" e de "não permitir interferências exteriores, que possam impedir ou dificultar o acesso à informação disponível nos seus serviços" (APDIS; BAD; INCITE, 2001), mas também a entidades governamentais com competência sobre as diversas vertentes da segurança nacional. Uns e outros, que se encontram atualmente apartados, deveriam refletir em conjunto sobre o assunto de forma a estabelecer diretrizes comuns de gestão da segurança da informação e do controlo do seu acesso, através do estabelecimento de uma categorização para a segurança da informação sensível mas não classificada, a criação de planos de formação e sensibilização destinados a vários níveis de utilizadores, e a promoção da correta aplicação destas medidas.

Em decorrência das presentes reflexões, este estudo evidenciou a importância do estabelecimento de uma Política Nacional de Informação que contemple um sistema de categorização e de controlo do acesso a informação sensível. Por outro lado pretendeu alertar, simultaneamente, os profissionais de informação e os especialistas em segurança nacional, para a necessidade de contemplarem em conjunto as questões da segurança da informação e do controlo do seu acesso como uma prática decorrente do seu desempenho.

Existe pois a necessidade de encontrar um equilíbrio, difícil de alcançar, entre o direito à informação, por um lado, e a segurança da sociedade e da privacidade do cidadão, por outro. O estabelecimento de uma verdadeira Política Nacional de Informação será muito importante para a garantia destas duas obrigações do Estado, sendo fundamental que o acesso à designada "informação sensível mas não classificada" seja definido por equipas multidisciplinares, constituídas pelas entidades produtoras da informação em conjugação com os especialistas em segurança e os profissionais de informação, de forma clara e transparente, com as salvaguardas

[5] Como por exemplo as associações de bibliotecários, arquivistas, documentalistas e todos os profissionais de informação.

adequadas, assegurando que a informação é controlada exclusivamente quando é necessário.

Referências bibliográficas

Abbas, June (2006) – Security, Access, Intellectual Freedom : Achieving Balance in a Global World. *Forum on Public Policy: A Journal of the Oxford Round Table* [Em linha]. Vol. 1. [Consult. 15 jun. 2015]. Disponível na Internet: ‹URL: https://goo.gl/Zplpse›

Afonso, Carlos Baía (2011) - *O direito de acesso aos documentos administrativos e a salvaguarda da segurança nacional*. Lisboa : IESM. Trabalho Individual de Investigação. Curso de Promoção a Oficial General

Bad, Apdis & Incite (2001) - *Código de Ética para os Profissionais de Informação em Portugal*. Lisboa: BAD, APDIS, INCITE

CADA (2014) - *Comissão de Acesso aos Documentos Administrativos: 19º Relatório de Actividades: 2013*. Lisboa: CADA

Cook, Michael (2010) - Freedom of Information: Legislation that has Radically Changed Archival Practice. *Atlanti*. Vol. 20, pp. 117-122

Estrutura Nacional de Segurança da Informação (ENSI) (2005a) - Política Nacional de Segurança da Informação: versão 1.0. [em linha] [Consult. 21 Abr. 2015] Disponível na Internet:‹URL:https://goo.gl/1zhMYL›

Estrutura Nacional de Segurança da Informação (ENSI) (2005b) - Carta de Segurança de Informação: versão 1.0. [em linha] [Consult. 21 Abr. 2015] Disponível na Internet:‹URL: https://goo.gl/9oVffo›

Estrutura Nacional de Segurança da Informação (ENSI) (2005c) - Política de Segurança da Informação da Entidade: versão 1.0. [em linha] [Consult. 21 Abr. 2015] Disponível na Internet:‹URL: https://goo.gl/QoM2Em›

European Union Agency for Network and Information Security (ENISA) [em linha] Consult. em 10 jun. 2015] Disponível na Internet: ‹URL:https://www.enisa.europa.eu/›

Knezo, Genevieve J. (2003) - *"Sensitive But Unclassified" and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy*. CRS Report for Congress. Congressional Research Service: The Library of Congress

Portugal. Assembleia da República - *Constituição da República Portuguesa, 7ª Revisão*.[em linha] Assembleia da República.pt.[Consult. 15. Jun. 2015] Disponível na Internet:‹URL: http://goo.gl/rilyAd

Portugal. Assembleia da República - *Lei da Protecção de Dados Pessoais:* 67/98 de 26 de Outubro. Lisboa: INCM

Portugal. Assembleia da República - *Constituição da República Portuguesa, 7ª Revisão*.[em linha] Assembleia da República.pt.[Consult. 15. Jun. 2015] Disponível na Internet:‹URL: http://goo.gl/rilyAd

Portugal. Assembleia da República - *Lei da Protecção de Dados Pessoais:* 67/98 de 26 de Outubro. Lisboa: INCM

Portugal. Assembleia da República - Lei n.º 46/2007, de 24 de Agosto: *Regula o Acesso aos Documentos Administrativos e a sua Reutilização*. Lisboa: INCM

Portugal. Assembleia da República - Lei Nº 41/2004, de 18 de Agosto: *Tratamento de dados pessoais e protecção da privacidade no sector das comunicações electrónicas*. Lisboa: INCM

Portugal. Assembleia da República - Lei Nº 53/2008, de 29 de Agosto: *Lei de Segurança Interna*. Lisboa: INCM

Portugal. Assembleia da República - Lei Nº 6/94, de 7 de Abril: *Lei do Segredo de Estado*. Lisboa: INCM

Portugal. Ministério da Justiça - Decreto-Lei 4/2015: *Código de Procedimento Administrativo*. Lisboa: INCM

Portugal. Presidência do Conselho de Ministros - Decreto-Lei 16/93 de 23 de janeiro: *Regime geral dos arquivos e do património arquivístico*. Lisboa: INCM

Portugal. Presidência do Conselho de Ministros - Decreto-Lei 125/99 de 20 de abril: *Regime jurídico de instituições de investigação científica*. Lisboa: INCM

Portugal. Presidência do Conselho de Ministros - *Gabinete Nacional de Segurança* [em linha] Consult. em 10 jun. 2015] Disponível na Internet:‹URL:www.gns.gov.pt/›

Pratas, Sérgio (2007) - *Acesso à Informação Administrativa no século XXI*. [Em linha] [Consult. 10. Jun. 2015] Disponível na Internet: URL:‹ http://goo.gl/oj7nJj›

Rafael, António & Proença, Luísa, coord. (2014) – *A gestão documental na governança da informação* [em Linha]. Lisboa: APDSI. [Consult. 15 jun. 2015] Disponível na Internet:‹URL:http://goo.gl/r75JFR

RCAAP – Repositório Científico de Acesso Aberto de Portugal. *O Acesso Aberto*. [em Linha]. [Consult. 1 set. 2015] Disponível na Internet:‹URL:http://goo.gl/loFZkq›

Swartz, Nikki (2003) - Information at a price: Liberty vs. security. *Information Management*. Vol. 37, n.º 3, p. 14

United States Department of Justice. *FOIA.gov*. [Em linha] [Consult. 21 Jun. 2015] Disponível na Internet: ‹URL:http://www.foia.gov/›

Unlu, Ali, et al (2012) - The Impact of 9/11 on Information Policy in the United States: A Current Perspective on Homeland Security and Emergency. *Management.Journal of Applied Security Research*. Vol. 7, n.º 3, pp. 320-340

USA. 107.TH CONGRESS (2001) - Public Law 107–56—Oct. 26, 2001: *The Usa Patriot Act: Preserving Life and Liberty* [em linha] [Consult. 14 Jun. 2015]. Disponível na Internet:‹URL: http://goo.gl/vkcZbQ›

USA. 107.TH CONGRESS (2002) - PUBLIC LAW 107–296—NOV. 25, 2002 : *Homeland Security Act* [em linha] [Consult. 14 Jun. 2015]. Disponível na Internet:‹URL: http://goo.gl/jv0yhU›

Usa. National Archives. *Controlled Unclassified Information (CUI)* [em linha] [Consult. em 10 jun. 2015] Disponível na Internet:‹URL:http://www.archives.gov/cui/›

Vieira, Ricardo & Borbinha, José (2011) – MoReq2010 : Uma apresentação. 10.º Encontro Nacional de Arquivos Municipais. *Gestão da Informação na Administração Municipal: passado, presente e futuro* [em linha]. 4 e 5 de Novembro de 2011, Leiria - Teatro Miguel Franco. Actas [Consult. 15 jun. 2015] Disponível na Internet:‹URL:http://goo.gl/RNNa6d