Disponível em www.bad.pt/publicacoes

PAPER

12º CONGRESSO NACIONAL BAD

Direito à Informação vs. Segurança: sobre a necessidade de uma política nacional de informação

Maria João Albuquerque[a], Rui Moura[b]

[a] Universidade Nova de Lisboa. INET-md, mjdalb@gmail.com

[b]Revista Militar, Portugal, ruimoura.ri14@gmail.com

Resumo

A liberdade de acesso à informação é um direito inalienável das sociedades democráticas. Mais de 95 países no mundo, entre os quais se inclui Portugal desde 1993, têm vindo a implementar legislação sobre liberdade de informação, no sentido de garantir o acesso a informações ou documentos detidos por órgãos governamentais. No entanto, a resposta dos governos à crescente ameaça terrorista tem posto em causa os direitos de livre acesso à informação. Nesta comunicação propomos refletir sobre este equilíbrio tão frágil entre a segurança e a liberdade de acesso à informação governamental, numa situação de crescente ameaça terrorista, procurando identificar que medidas Portugal está a adotar neste âmbito, integrado no contexto internacional.

Palavras-chave: Direito à Informação, Segurança, Política de Informação, Terrorismo, Portugal

Introdução

Em 2011, de acordo com o jornal online International Business Times, foi efectuado um atendado bombista numa estância de inverno na República Russa de Kabardino-Balkaria, na região do Cáucaso, que destruiu um teleférico numa estância de esqui, tendo provocado o afastamento de turistas da região do monte Elbrus, a montanha mais alta da Europa (http://goo.gl/R7L4Cd).

Uma notícia da Agência Lusa, a 21 de março de 2014, relatava queixas de pais, reforçadas por denúncias da FENPROF, sobre o uso de escolas públicas para acções de marketing de empresas privadas. Os pais dos discentes, conforme relataram à Lusa, eram contactados por telefone para "assinar contratos de fidelização de três anos com empresas privadas que se oferecem para ensinar inglês aos alunos que este ano realizam pela primeira vez o exame do 9.º ano do Cambridge". Segundo a mesma notícia existia "conivência de alguns directores de escolas públicas", indiciando que os mesmos partilhavam os contactos das famílias, o que fez com que o Ministério de Educação abrisse quatro processos de averiguações através da Inspecção-geral da Educação e Ciência. (in Jornal de Negócios online, http://goo.gl/B0lLLx).

Analisando o 19º Relatório da Comissão de Acesso aos Documentos Administrativos (CADA), respeitante aos processos apreciados em 2013, detetamos dois exemplos em que foi dado parecer favorável a pedidos de acesso à informação, que face aos exemplos anteriores podemos qualificar de sensível.

O primeiro caso menciona a autorização de cedência de "informação contratual, fotografias, projectos, imagens do teleférico da Penha e outra documentação" (Parecer 23/2013, de 2013.01.15). A CADA registou este pedido com o descritor "informação contratual; segredo comercial; segredo de Estado", e manteve o anonimato do requerente.

Num segundo caso autorizou também a cedência dos contactos dos pais dos alunos do Agrupamento de Escolas das Colmeias, Marrazes-Leiria, ficando apenas excluídos os pais "de que se conheça vontade de manter sigilo" (Parecer 209/2013, de 2013.07.16).

Em ambas as situações as entidades requeridas acataram o parecer da CADA, disponibilizando a informação. Num caso, referente a um equipamento de utilização pública passível de ser sabotado, como aconteceu na região do monte Elbrus, noutro referente a dados pessoais de contacto dos pais dos alunos que viram a sua privacidade devassada.

Estes dois exemplos são paradigmáticos da complexidade da gestão do acesso a informação de conteúdo sensível na posse do sector público, não passível de uma classificação de segurança nos termos do SEGNAC[1] ou do SEGMIL[2], cuja divulgação sem controlo poderá colocar em risco a segurança do Estado, da sociedade ou do cidadão, comprometer a privacidade das pessoas e a protecção de dados pessoais, ou violar os direitos de propriedade intelectual, industrial e comercial. Perante estas situações de risco verifica-se que em Portugal não existe uma verdadeira política nacional de informação que contemple a segurança dos conteúdos que a Administração tem à sua guarda, nem sequer uma grande sensibilidade para a matéria.

Propomo-nos nesta comunicação abordar as questões relativas ao acesso à informação detida pela Administração Pública, 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[3], 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[4].

Tendo por base o método quadripolar proposto por Silva (2014) formularam-se as seguintes questões:

- Como conseguimos equilibrar conceitos tão fundamentais ao Estado de Direito, como Segurança e Privacidade, como Acesso à Informação e Liberdade Intelectual?
- Como se pode proporcionar em simultâneo Liberdade e Segurança (individual e colectiva)?
- Será importante para a garantia destas duas obrigações do Estado o estabelecimento de uma Política Nacional de Informação?
- Que tipo de informação deve ser considerado "informação sensível mas não classificada"?

Para responder a estas questões, efetuou-se inicialmente 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, tendo em vista o estabelecimento de uma Política Nacional de Informação, abrangente e atenta aos riscos que ameaçam a sociedade.

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 de acesso à informação administrativa, dos quais é exemplo o Freedom of Information Act (FOIA) dos EUA (1967).

No entanto, a ameaça terrorista das últimas décadas e a preocupação acrescida de assegurar a segurança interna dos Estados levaram os mesmos governos à tomada de 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".

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 o mesmo colocava 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 à ameaça 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, como o direito em aceder livremente à informação.

Enquanto o assunto é 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 [5], 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, e não foram desenvolvidos nem publicados os documentos propostos, nem efectuada a promoção de uma cultura nacional de segurança como era sugerido. Também em 2011 a PSP publicou um documento intitulado "Política de Informação", que pretende estabelecer uma política de informação da PSP, "no respeito do dever de informação que não colida com o seu dever de reserva" (p.3), mas que não aborda a questão do tratamento da informação sensível não classificada.

O Acesso aos Documentos Administrativos em Portugal

Na Administração Pública 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 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 sector 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 carácter 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 acção 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 directa ou indirectamente 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 carácter 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 afectiva 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 directo, 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.

Os profissionais da informação e o acesso à documentação administrativa

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 desta 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.

Tendo como objetivo deste estudo o acesso à informação de caracter administrativo, considerou-se como necessário estudar ainda quais os limites legais a que está sujeita a comunicação de documentos de arquivo, os quais estão expressos no DL 16/93 de 23 de janeiro, que define o regime geral dos arquivos e do património arquivístico, restringindo à consulta pública os documentos que "contenham dados pessoais de carácter judicial, policial ou clínico, bem como os que contenham dados pessoais que não sejam públicos ou de qualquer índole que possa afetar a segurança das pessoas, a sua honra ou a intimidade da sua vida privada e familiar e a sua própria imagem" (art.º 17º).

O mesmo artigo refere que estes mesmos documentos poderão ser abertos ao público caso lhes tenha sido expurgada a informação atrás referida, ou haja consentimento dos titulares dos interesses

legítimos, ou desde que já tenham decorrido 50 anos sobre a data de morte da pessoa (75 anos sobre a data do documento, nos casos em que a data da morte é desconhecida). O mesmo se aplica para as pessoas coletivas, às quais é colocado um período de 50 anos após a sua extinção.

Por esta leitura pode-se verificar que apenas estão aqui contempladas as matérias relativas aos dados pessoais, estando ausente, neste dispositivo legal, a regulamentação do acesso à informação de carácter sensível respeitante às seguranças do Estado e da coletividade, cuja responsabilidade é assegurada pela legislação geral, com conceitos não consensuais e pouco objetivos.

Toda a legislação e normas publicadas no âmbito da gestão documental de arquivo tem-se preocupado exclusivamente com a gestão do ciclo de vida do documento, contemplando o fluxo de produção e a avaliação da documentação, tendo em vista a sua organização e destino final (eliminação/ conservação), esquecendo-se do controlo do seu acesso, mesmo quando a tendência atual aponta para uma gestão contínua dos documentos, que encara a avaliação como um processo integrado com as demais funções arquivísticas, prevendo a elaboração de instrumentos de referência no momento da produção da informação.

O projeto da Macro Estrutura Funcional (MEF) que pretende uniformizar a classificação[6], a avaliação e a seleção dos documentos produzidos pela Administração Central e Local, através de um modelo de classificação único que garanta a interoperabilidade semântica nas trocas de documentos entre os serviços, bem como a criação de Folhas de Recolha de Dados para a seleção documental a aplicar a cada grupo de classificação, com vista à implementação de políticas de avaliação documental, tem apenas em consideração a facilidade na recuperação da informação e a racionalização dos procedimentos de eliminação, esquecendo totalmente as questões de segurança relativamente ao acesso a essa mesma informação (DGLAB, 2013).

A nível internacional a ISO 15489 que visa normalizar a gestão de documentos de arquivo (IPQ trad, NP 4438), no seu volume 2, considera importante o desenvolvimento de uma classificação de acesso, por forma a garantir a proteção de dados pessoais e a privacidade, os direitos de propriedade intelectual e confidencialidade comercial, a segurança da propriedade, a segurança do Estado e a salvaguarda de privilégios legais e profissionais (art 4.2.5 Security and access classification scheme, p. 12). No entanto a aplicação desta norma numa classificação de acesso na gestão de documentos de arquivo não tem paralelo em Portugal.

Também o projeto europeu MoReq2010 (2011), que contém os requisitos para sistemas de gestão de documentos de arquivos, prevê um requisito não funcional para a privacidade, que contempla a proteção de dados pessoais em contextos governamentais e os direitos individuais de acesso à informação pública.

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, e não contemplando estas preocupações nos novos projectos em desenvolvimento que visam uniformizar os procedimentos de gestão de documentos de arquivo.

Desafios e ameaças dos Estados no âmbito da segurança interna

O conceito de Segurança Interna tal como é definido na lei é a "actividade 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 protecção civil (prevenir riscos colectivos inerentes a situações de acidente grave ou catástrofe) ao contra terrorismo, da vigilância e obtenção de informações à prevenção e combate ao crime, do narcotráfico à segurança de infra-estruturas críticas, etc.

No entanto a globalização aumenta também os riscos e ameaças, e a noção de pertença dos países a Comunidades mais vastas faz com que a segurança interna seja 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 acção da cooperação entre autoridades policiais e judiciais, a gestão das fronteiras e a protecção civil, no respeito dos valores comuns europeus, como os direitos fundamentais.

Na implementação da estratégia 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 EU, 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 protecção 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 efectuado 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 sectores específicos de actividade 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 é praticado nos EUA.

Neste País 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. Esta proliferação de marcas gerou disfunções, sendo inclusivamente uma barreira à difusão de informação aos organismos que dela necessitavam, mas também confusão na sua utilização e dificuldades na gestão da protecção 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 a comunidade dos profissionais da informação, 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), tomando como central a necessidade do estabelecimento de uma Política Nacional de Informação, de forma a assegurar a equidade no livre acesso à informação, garantindo, simultaneamente, a segurança do Estado, da sociedade e dos cidadãos.

Neste sentido, a DGLAB no âmbito do projecto Macro Estrutura Funcional (MEF), que uniformiza processos na gestão de arquivos, deveria 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 os profissionais da informação das Bibliotecas e Arquivos da Administração Central, para a necessidade de contemplar 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 a designada "informação sensível mas não classificada" seja definida e categorizada pelas entidades produtoras da informação, com a coordenação da DGLAB, de forma clara e transparente, de modo a que a partilha da informação se realize de forma consciente e melhorada com as salvaguardas 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

DIREÇÃO GERAL DE ARQUIVOS (2010) – *Orientações para a elaboração e aplicação de instrumentos de avaliação documental: Portarias de gestão de documentos e relatórios de avaliação* [em linha] Lisboa: DGARQ. [Consult. 15 jun. 2015]. Disponível na Internet:<URL: http://goo.gl/2T4o1W>

DIREÇÃO GERAL DE ARQUIVOS (2010) - *Orientações para a gestão de documentos de arquivo no contexto de uma reestruturação da Administração Central do Estado*. 2.ª ed. revista e atualizada. [em linha]. Lisboa: DGARQ. [Consult. 15 jun. 2015]. Disponível na Internet: <URL:http://goo.gl/IQDpri>

DIREÇÃO GERAL DO LIVRO, DOS ARQUIVOS E DAS BIBLIOTECAS (2013) – *Macroestrutura Funcional (MEF) : V.2.0* [Em linha]. Lisboa: DGLAB. [Consult. 15 jun. 2015]. Disponível na Internet: <URL: http://dgarq.gov.pt/files/2012/01/MEF-1_0_v02_01_2012.pdf>

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

LUSA (2014) - Ministério da Educação investiga utilização abusiva de escolas por privados. *Negócios Online* [em linha]. 21 Março 2014 [Consult. 21 Jun. 2015] Disponível na Internet: URL:http://goo.gl/B0lLLx

POLÍCIA DE SEGURANÇA PÚBLICA. Direção Nacional (2011) – Política de Informação. [em linha] [Consult. 11 mai. 2015] disponível na Internet <URL: http://goo.gl/tHqOcK>

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. PRESIDENCIA 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

SILVA, Armando Malheiro da (2014) – O método quadripolar e a pesquisa em ciência da informação. *Prisma.com.* nº26, pp. 27-44

SINHA, Sanskrity (2011) - Politics. Terror in tourism: Russia stops receiving tourists at ski resort after attack. *International Business Times* [em linha]. 22/Fev./2011. [Consult. 21 Jun. 2015] Disponível na Internet: <URL:http://goo.gl/R7L4Cd>

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

[1] SEGNAC - Resoluções do Conselho de Ministros (RCM) que aprovaram as várias Normas para a Segurança e Salvaguarda das Matérias Classificadas

[2] SEGMIL - Matérias de segurança relacionadas com as Forças Militares que aplicam, no seu universo, as Instruções para a Segurança Militar, Salvaguarda e Defesa de Matérias Classificadas

[3] 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)

[4] 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).

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

[6] Classificação aqui entendida como distribuição temática e não como classificação de segurança