A Proteção de Dados Pessoais na Nova Era Tecnológica

Maria de Fátima Cordeiro Oliveira

Biblioteca Municipal de Leiria

Largo Cândido dos Reis, nº 6

2400-112 Leiria

Tel: 244839666

E-mail: fatima_cordeiro77@hotmail.com

José António Calixto

Biblioteca Pública de Évora

Centro Interdisciplinar de História Cultura e Sociedades

da Universidade de Évora

Faculdade de Ciências Sociais e Humanas da

Universidade de Lisboa

Largo Conde Vila Flor

7000-804 ÉVORA

Tel: 266769330

E-mail: jacalixto2000@gmail.com

RESUMO:

Esta comunicação aborda a questão da privacidade na nova era tecnológica, um tema que coloca diversos desafios éticos aos profissionais de informação, e resulta de uma revisão literatura sobre este tema. São apresentadas e discutidas em primeiro lugar as definições existentes de privacidade, e uma reflexão sobre as necessidades regulatórias da Internet e os seus limites. Apresenta-se de seguida uma breve análise comparativa das legislações de proteção de dados europeia e norte-americana, bem como uma referência às especificidades da legislação portuguesa e ao papel das autoridades reguladoras, sendo destacado o caso português. A questão do anonimato é alvo de um reflexão e serão abordados os conflitos entre direitos, nomeadamente entre privacidade e direito à informação, por um lado, e direito à segurança, por outro. Discutir-se-á também sobre a possibilidade de o titular dispor do seu direito à privacidade. Concluir-se-á com a necessidade de recolocação de um conjunto de questões éticas aos profissionais da informação.

PALAVRAS-CHAVE: Ética Profissional, Dados Pessoais, Autodeterminação Informativa, Direito à Informação, Direito à Segurança

ABSTRACT:

This paper issues the question of privacy in the new technological age, an issue that poses several ethical challenges to the information profissionals, and results of a literature review on this topic. Firstly there are discussed the existing definitions of privacy, and made a reflection on the regulatory needs of the internet and its limits. We present below a brief comparative analysis of the data protection laws in Europe and the U.S., as well as a reference to the specificities of Portuguese law and the role of regulators, prominent being the portuguese case. The issue of anonymity is a reflection target and will be dealt with conflicts between rights, particularly among privacy and right to information on the one hand, and the right to security on the other. It will discuss also about the possibility of the owner to dispose of his right to privacy. It will conclude with the need for replacement of a set of ethical issues for information professionals.

KEYWORDS: Professional Ethics, Personal Data, Informational Self-Determination, Right to Information, Right to Safety

INTRODUÇÃO

Nos nossos dias, os profissionais de informação são colocados perante novos desafios, com a emergência da interoperacionalidade, dos metadados, da administração pública eletrónica, da computação na nuvem, entre outros. Nessas circunstâncias voltam a colocar-se velhas questões éticas, uma aos quais saber qual o espaço que o direito à privacidade tem.

O Código de Ética dos Profissionais de Informação, adotado pela BAD, APDIS e INCITE em 1999 dedica a sua segunda sessão à privacidade, logo a seguir à liberdade intelectual, o que sugere a importância deste assunto para a construção de uma boa imagem do profissional. O código começa por ensaiar uma definição de privacidade e o seu valor: a afirmação de que privacidade vale por si mesma e que os profissionais a devem respeitar em cada cidadão, pois cada um é um ser singular e irrepetível. As alíneas seguintes são listados um conjunto de responsabilidades / deveres éticos de todo o profissional da informação.

Esta preocupação com a salvaguarda dos dados pessoais

está presente nas organizações profissionais de nível internacional, como a IFLA (na Declaração de Glasgow de 2002, no Manifesto da IFLA sobre a internet do mesmo ano) ou o Conselho Internacional de Arquivos (na Declaração Universal sobre Arquivos, de 2010). Todos estes códigos e legislação atribuem deveres ao profissional de informação. Contudo, apesar do esforço, falham em especificar como o profissional deve proceder no quotidiano. É certo que os deveres éticos podem ser estabelecidos para além da lei (e mesmo contra a lei). Por exemplo, em Portugal actualmente o Governo pretende ção das regras das associações públicas profissionais(édicos, advogados, arquitetos ou biólogos, entre outras profissões) através da criação da figura do provedor com poderes para colocar um processo disciplinar (DIÁRIO DIGITAL, 2012).

As leis são portanto um reflexo das perceções das sociedades, cujos efeitos se reproduzem no quotidiano dos cidadãos bem como no dos profissionais, não devendo ser ignoradas. Por isso optou-se neste estudo por apresentar o problema da privacidade de um ponto de vista jurídico e legislativo.

Neste comunicação fez-se uma revisão da literatura mais relevante. Partiu-se de uma pesquisa geral na internet, utilizando-se o Google e as palavras-chave: dados pessoais; dados pessoais na internet; personal data; Internet privacy; personally identifiable data e anonimity. Procuraram-se textos recentes, preferencialmente escritos a partir do ano 2000. Foram também consultados os sítios na Internet de associações profissionais relevantes e de autoridades da administração pública de vários países. Utilizaram-se preferencialmente artigos de publicações periódicas mas também algumas monografias recentes.

PRIVACIDADE, INTERNET E DIREITO

O direito à privacidade é tutelado em Portugal por toda a ordem jurídica: Constituição da República Portuguesa (CRP), direito administrativo, direito penal e direito civil (DIAS, 2001, 11). A privacidade e proteção de dados é assim uma preocupação importante para o legislador.

Apesar disso, o legislador não conseguiu encontrar uma definição unívoca de "vida privada", por isso torna-se difícil delimitar o seu âmbito. Canotilho e Moreira (apud GUERRA, 2001, 159) defendem que o direito à intimidade da vida privada se analisa em dois direitos menores: «(a) o direito a impedir o acesso de estranhos a informação sobre vida privada e familiar e (b) o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem (art. 80 do Código Civil (CC))». Marques (2004, 24) vida privada de forma mais flexível e ampla, como «aquele conjunto de atividades, situações, atitudes ou comportamentos individuais que, não tendo relação com a vida pública (*privada* entendida como *separado da coisa pública*), respeitam estritamente à vida pessoal e familiar de uma pessoa». Trata-se de uma interpretação mais flexível e ampla que a de Canotilho e Moreira.

No direito alemão são reconhecidos três níveis de privacidade: a esfera pública (dados que o titular está disposto a apresentar voluntariamente), a esfera privada (a informação que ele não pretende disponibilizar, relacionada com as relações sociais) e por último a esfera íntima (dados relacionados com ideias filosóficas ou políticas, religiosas, a origem racial ou étnica, e os dados relativos à intimidade sexual, e ao estado de saúde, incluindo dados genéticos) (SILVA, 2006, 7). Para Silva é esta última esfera que mais deve preocupar os titulares do direito à privacidade.

De fato, o direito alemão influencia o direito europeu de várias formas. O direito à autodeterminação informativa, direito relacionado com a proteção da privacidade e dados pessoais nasceu de uma decisão do Tribunal Constitucional alemão em 1983 (CASTRO, 2010, 11), na República Federal Alemã, relativa à Lei do Recenseamento da População, que compelia todos os habitantes a responder a um questionário que iria servir tanto para fins estatísticos como para fornecer dados pessoais a um conjunto de entidades administrativas. O tribunal entendeu suspender provisoriamente o censo, autonomizando na sua decisão um *Recht auf informationelle Selbstimmung* (Direito à Autodeterminação Informativa) como «um direito fundamental que garante ao indivíduo a competência para em princípio ser ele próprio a decidir sobre a utilização e divulgação dos seus dados pessoais» (DIAS, 2001, 14). Este é um direito de conteúdo independente, e não apenas uma salvaguarda em relação ao direito à reserva da vida privada. É um dos direitos de personalidade, pois é dirigido à defesa de novos aspetos da personalidade que é necessário defender (CASTRO, 2006b, 4; CASTRO, 2010, 11), em consequência da nova sociedade tecnológica, e sobretudo do aumento do uso da internet como meio de divulgação de dados e factos pessoais (CASTRO, 2006b, 4). É reconhecido no artigo 35º da CRP.

Segundo Castro (2010, 11) este direito deve ser encarado numa dupla perspetiva: subjetiva e objetiva. A perspetiva subjetiva refere-se à capacidade dos seus titulares gozarem de capacidade jurídica para se defenderem da utilização abusiva de informações pessoais por parte do Estado. A perspetiva objetiva impõe ao Estado a defesa contra agressões de terceiros a este direito.

Pinto (2002, 1-2) lembra que o CC no artigo 81º dá possibilidade ao titular de direitos de limitar voluntariamente o exercício de direitos de personalidade, desde que estes não sejam contrários aos princípios da ordem pública. Pinto (2002, p. 1-2) e Marques (2004, 24) defendem o carácter não absoluto do direito à reserva da vida privada. Essa visão tem consequências em termos de jurisdição, como veremos a seguir.

Silva (2005b, p. 4) defende que a internet não é um espaço sem leis. Marques (2004, p. 43) e Ascensão (1999, citado por VERDELHO, 2003, 356) postulam que os direitos e obrigações para proteção da vida privada são os mesmos fora ou dentro do espaço virtual.

Dias (2004, p. 30-32) enumera aquelas que considera serem as características do direito da informática: o seu carácter evolutivo (resultante de uma tecnologia em contínuo desenvolvimento), a dimensão internacional (o carácter transnacional acaba por fazer parte dos regulamentos, bem como o facto da participação de organizações internacionais, como as Nações Unidas, nessa regulamentação), a sua originalidade (que se manifestaria através da publicação de normas particulares para certos domínios, da adaptação de regras

antigas a novos contextos e mistura de normas antigas com novas) e por fim a sua pluridisciplinaridade (trata-se de um "direito de encruzilhada", pelo que se aconselha o trabalho em equipa, com colaborações de outras disciplinas).

PROTEÇÃO DE DADOS PESSOAIS NA PERSPECTIVA DO DIREITO COMPARADO

Em termos de direito comparado, existem duas visões maioritárias do direito da internet: uma do direito continental europeu, que aposta em formas de hetero-regulação, outra do direito norte-americano, centrada na autorregulação.

Em 1980 a Organização para a Cooperação e Desenvolvimento Económico, através do documento Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, estabeleceu um conjunto de princípios deviam nortear a proteção de dados: o princípio de limitação da coleta, o princípio de qualidade dos dados, o princípio de definição da finalidade, o princípio de limitação de utilização, o princípio do *back-up* para segurança dos dados, o princípio de abertura, o Princípio de participação do indivíduo e do principio da responsabilidade (BAUMER, EART e POINDEXTER, 2004, 402).

Embora a maioria dos países europeus e americanos fizessem parte da OCDE, a aplicação destas directivas variou muito, sobretudo entre os estados da União Europeia (direito continental europeu) e os Estados Unidos.

Para Couto (2004) estas diferenças baseiam-se tanto em tradições culturais, que levam a formas diferentes de encarar o direito, uma baseada na ideia de "interesse geral" e "ordem pública", outra baseada em interesses económicos. No primeiro predomina a iniciativa legislativa, no segundo é são as decisões dos tribunais e a autorregulação que se tornam na fonte de legislação a aplicar em casos semelhantes (COUTO, 2004).

A Diretiva 96/46/CE de 24 de Outubro de 1995 procurou aplicar os princípios da OCDE mas também outros, de criação europeia. Isto porque em 1980 a Convenção nº 108 do Conselho da Europa (MARQUES, 2004, 27; LEVIN e NICHOLSON, 2005, 374) estabelecia os seguintes princípios: princípio da recolha leal e lícita de dados, princípio da finalidade, princípio da qualidade, princípio da limitação quantitativa e o princípio da conservação por tempo limitado. No entanto já em 1973 o Comité de Ministros do Conselho da Europa havia aprovado a Recomendação nº (73)22 para proteção dos indivíduos face aos bancos de dados eletrónicos do setor privado (GUERRA, 2001, 146).

A Diretiva 96/46/CE define dados pessoais como «qualquer informação relativa a uma pessoa singular identificada ou identificável ("pessoa em causa"); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por um número de identificação ou a um ou mais elementos específicos da sua identidade física, psicológica, psíquica, económica, cultural ou social» (art. 2º da Diretiva). Trata-se de uma definição que se baseia na proteção em vários aspectos da personalidade de um indivíduo, incluindo alguns públicos mas que podem ser usados para o prejudicar (BAUMER, EART e POINDEXTER, 2004, 403).

A Diretiva impõe também a obrigação de um aviso prévio das recolhas de dados, mas vai mais longe, pois exige às organizações que os recolhem que avisem dos propósitos de tal recolha. Baumer, Earp e Poindexter (2004, 410) afirmam que a proteção dada na União Europeia é maior.

Nos Estados Unidos a legislação sobre a proteção da privacidade é um conjunto de leis desconexas e publicadas uma de cada vez, sem ordem lógica (LEVIN e NICHOLSON, 2005, p. 361). Existem leis tanto para proteger o a privacidade do Estado como do sector privado (LEVIN e NICHOLSON, 2005, 362). No entanto, com tanta dispersão legislativa, é difícil encontrar alguma jurisprudência coerente desse emaranhado. Existem várias definições de privacidade no país, mas não uma definição única e com caráter federal (BAUMER, EART e POINDEXTER, 2004, 402).

Em 1998 a Comissão Federal de Comércio dos Estados Unidos emitiu um relatório ao Congresso dos Estados Unidos onde propunha os seguintes princípios para recolha e tratamento de dados pessoais: aviso prévio, escolha, acesso e segurança. Para além disso, submetia à apreciação a ideia de criação de um organismo que aplicasse sanções aos incumpridores (COMISSÃO FEDERAL DE COMÉRCIO, 2000, i). Mas estes princípios são vistos como meras recomendações e a legislação proposta nunca foi criada. Assim, o direito norte-americano sobre privacidade é na autorregulação.

Por exemplo, apesar do princípio do aviso prévio, a legislação norte-americana não obriga os sítios de internet a notificar os seus utilizadores quanto aos dados que vão recolher (BAUMER, EART e POINDEXTER, 2004, 403-404). Earp e Poindexter (2004, p. 410) concluem que os sítios baseados nos Estados Unidos não são efectivamente regulados, podendo colectar informações pessoalmente identificáveis sem o conhecimento dos internautas. «Alguns analistas políticos enfatizam a importância de uma "ética profissional" na arena da privacidade, mas a história recente da internet e a teoria económica básica sugerem que, se há lucro a obter através da compra, venda e transmissão de informações pessoalmente identificáveis (PII), alguém aproveitará a oportunidade» (BAUMER, EART e POINDEXTER, 2004, 410).

Entretanto, em junho de 2001, o Ato Patriota (tradução de PATRIOT Act, abreviatura de Act to Provide Appropriate Tools Required to Intercept and Obstruct Terrorism) anulou e emendou muita legislação existente sobre privacidade, permitindo ao Estado um acesso quase ilimitado aos dados eletrónicos dos seus cidadãos sem necessidade de autorização de um juiz (LEVIN e NICHOLSON, 2005, 362).

Por outro lado, os Estados Unidos propuseram o Acordo Porto Seguro (Safe Harbor Agrement) em resposta à Diretiva de 1995. O acordo foi realizado entre a Comissão Europeia e os Estados Unidos em 21 de julho de 2000. Estabelece que os Estados Unidos devem respeitar os princípios europeus de proteção de dados, ao mesmo tempo que permite a transferência de dados de europeus para empresas norte-americanas. Para Farinho (2006, 94) este acordo significou a superação entre a

autorregulação norte-americana e a legislação europeia. Até 2005 foram os serviços de informação, serviços de computação (por exemplo, empresas que permitam guardar dados em servidores externos, ou seja, de serviços na Cloud) e de *software* quem mais beneficiaram com este acordo (LEVIN e NICHOLSON, 2005, 377-378).

Por fim, há que referir que a Comissão Europeia propôs recentemente uma reformulação da Diretiva 96/46/CE de 24 de Outubro de 1995. As propostas incluem: um conjunto único de regras válidas em toda a União Europeia; os requisitos administrativos, como a exigência de notificação às comissões de proteção de dados de cada país, desaparecem para as empresas; prevê uma maior responsabilidade e responsabilização das empresas; a Comissão Europeia promete reforçar os poderes das comissões de proteção de dados de cada país, aumentando o limite monetário das coimas (COMISSÃO EUROPEIA, 2012).

A Transposição da Diretiva para a Legislação Portuguesa

Em Portugal a preocupação com a proteção da privacidade apareceu a primeira vez no artigo 35º da CRP de 1976 (GUERRA, 2001, 149; GOMES, 2006, 143-144), bem como pela Lei nº 10/91 (Lei da Proteção de Dados Pessoais face à Informática), que já consagrava alguns dos principios da Diretiva.

Baseada na Diretiva 96/46/CE, foi criada em Portugal a Lei nº 67/98, de 26 de Outubro, aplicando os princípios da mesma. Mas esta lei vai um pouco mais longe que a Diretiva no estabelecimento dos direitos dos titulares de dados pessoais e na exigência de sigilo profissional.

Assim, segundo a Lei nº 67/98 o titular de dados pessoais possui o direito ao esquecimento, que impõe que os dados sejam conservados apenas durante o período estritamente necessário aos fins para os quais foram recolhidos. Este aspeto voltou a ser questionado aquando das inúmeras leis de conservação de dados para faturação de serviços eletrónicos e mais tarde acerca da cibercriminalidade, sendo atualmente mais difícil de assegurar (CASTRO, 2006a, 16; ver art. 5º, nº 1 da lei).

Outros direitos do titular de dados: o direito à curiosidade (o direito de saber se uma entidade possui dados pessoais) e o direito à informação (direito de conhecer as finalidades para as quais os dados vão ser usados e da identidade de quem os recolhe), o direito de acesso aos dados pessoais, que permite que sejam exercidos outros direitos, como o direito de obter certificação de dados errados, a sua atualização, clarificação e completude. Para além destes, o direito a requerer o seu apagamento ou bloqueio, quando os dados expirem o prazo para o qual foram requeridos; o direito de oposição ao tratamento dos seus dados, bem como o direito a requerer que não sejam tratados dados sensíveis, como dados relativos à saúde, vida sexual, pontos de vista políticos e filosóficos, entre outros. Esta lei consagra ainda que o titular de dados pessoais não ficar sujeito a uma decisão baseada no tratamento automatizado de dados relativos a determinados aspetos da sua personalidade e vida pessoal ou profissional (CASTRO, 2006a, 17-18; ver art. 10, 11, 12º e 13º da Lei nº 67/98, de 26 de Outubro).

Pelo artigo 17º da lei, qualquer profissional que seja responsável pelo tratamento de dados, fica obrigado a sigilo profissional. Foi provavelmente neste contexto que nasceram os principios éticos adotados pela BAD, APDIS e INCITE em 1999.

Apesar das boas intenções, esta lei tem limites ao ser aplicada. Castro (2006b, 5) aponta como grande deficiência da lei o facto de não contemplar os dados pessoais de pessoas coletivas, isto apesar da Diretiva não o impedir. O artigo 12º da CRP postula que «as pessoas coletivas gozam dos direitos e estão sujeitas aos deveres compatíveis com a sua natureza» (CASTRO, 2006b, 6). Assim, as pessoas coletivas (empresas, fundações, entidades da administração pública, municípios) ficam sem legislação que contemple os seus dados (os dados dos seus empregados, clientes, fornecedores) estando em casos de conflito dependentes da decisão de um tribunal, que interpreta a lei de um determinado modo, enquanto outro a interpretará de outra forma.

Silveira (2002, 51-56) denota-lhe a falta de uma definição clara de conceitos e de conflitos entre esta e a Lei de Acesso aos Documentos Administrativos (na altura regulada pela Lei nº 65/93).

Silva (2006, 14) considera que a legislação existente no que diz respeito à privacidade e proteção de dados pessoais é boa, falta é ser cumprida. Por um lado, é necessária cooperação internacional para que a lei tenha efeitos práticos (CASTRO, 2006a, 29; MARQUES, 2004, 63).

O PAPEL DAS AUTORIDADES REGULADORAS

A Diretiva 96/46/CE previa a existência em cada estado-membro de uma autoridade responsável pela aplicação da mesma (artigo 28º e seguintes), independente e de caracter administrativo. Entre as suas competências estão a emissão de pareceres, regulamentação da conservação de dados e respetivas medidas de segurança, investigação e inquirição no âmbito das suas atividades e a resolução de casos - ordenação de eliminação de bases de dados ilegais, aplicação de coimas, entre outras (GUERRA, 2001, 150-153; DIAS, 2001, 27).

Para Dias (2001, 13) o direito administrativo leva vantagem sobre o direito penal no que diz respeito aos atentados à privacidade, pois tem maior facilidade e rapidez em exercer a punição. Segundo este autor, as autoridades administrativas independentes distinguem-se por terem como atribuições a vigilância de sujeitos públicos e privados nestas matérias e são independentes face à administração pública (DIAS, 2001, 20).

Em Portugal essa autoridade é a Comissão Nacional de Proteção de Dados (CNPD), que começou a exercer funções em 1994 (CNPDa, 2012), na sequência da Lei nº 10/91. A Lei nº 67/98, de 26 de Outubro apenas vem alargar a sua esfera de ação e os seus poderes (CNPDa, 2012).

Dias (2001, 26), de forma otimista, afirma que a sua composição (um presidente e dois vogais eleitos pela Assembleia da República; 2 magistrados com mais de 10 anos de carreira designados pelo Conselho Superior de Magistratura; 2 vogais designados pelo Governo) é garantia de independência, dado que esta é assegurada pela lei.

No entanto Guerra (2001, 169) já aponta os limites deste

regime e que havia de ponderar bem a decisão de ordenar um bloqueio, apagamento ou destruição de dados. A questão é saber se uma autoridade administrativa terá o mesmo peso de uma decisão de um trobunal ou de um governo.

Segundo Castro (2006b, 13-14) a transferência de dados entre estados membros da União Europeia deve ser feita mediante autorização da autoridade de proteccional de dados do estado-membro (no caso português a CNPD). O facto de um país não ter um nível semelhante ao europeu de proteção de dados não impede a transferência, desde que haja consentimento do titular dos dados ou ser fundamentado com o interesse público importante. Em Portugal a Lei 2/94 de 19 de Fevereiro o controlo da CNPD de dados trocados no Espaço de Schengen e a Lei 68/98, de 26 de Outubro no âmbito da Europol. Mas esta regra já teve uma exceção.

Em 2009 o Governo português fez um acordo bilateral com os Estados Unidos para transferência de dados pessoais (que incluem dados biométricos e genéticos). Em 2011 a CNPD deu um parecer negativo, alegando que o acordo «não contempla as necessárias garantias exigidas pela lei nacional e pela legislação europeia para a transferência de dados pessoais, a fim de suprir a falta de um nível de protecção adequado nos EUA». Mesmo assim o acordo foi rectificado em Assembleia da República. A rectificação deste acordo pôs em causa as funções da CNPD.

Pode-se questionar então se as comissões de proteção de dados conseguem de facto cumprir o seu papel regulador. Para responder a essa pergunta foram estudados os relatórios anuais da CNPD portuguesa e da Commission Nationale de l'Informatique et des Libertés (CNIL) francesa, com atribuições semelhantes à portuguesa.

Analisando o relatório da CNPD relativo a 2011 (CNPD, 2012b, p. 4) vemos que a notificação electrónica às instituições e empresas acelerou os procedimentos administrativos. Aumentou o número de processos e notificações, tendo aumentado também o número de processos concluídos relativamente a anos anteriores (CNPD, 2012b, p. 5). Estes processos partem tanto de autoridades judiciárias e fiscalizadoras do Estado, bem como de identidades e cidadãos a nível particular. As queixas mais frequentes dizem respeito à videovigilância, recolha excessiva de dados pessoais, tratamento de dados sem consentimento do titular e utilização abusiva de dados (CNPD, 2012b, p. 6-7). Para além das actividades já referidas anteriormente, a CNPD levou a cabo uma campanha de sensibilização aos cidadãos (CNPD, 2012b, p. 12-13).

No caso do relatório de 2011 CNIL francesa (Le Moullec, 2012) dá de igualmente um panorama de aumento da procura destas instituições reguladoras: duplicaram os quadros nos últimos sete anos (atualmente são 159 pessoas), aumentaram os telefonemas e as queixas.

A comparação entre estas duas comissões, concluir-se-á que o cidadão europeu está cada vez mais interessado na proteção dos seus dados pessoais. Estas autoridades têm a vantagem, em comparação com os tribunais, de serem mais céleres, têm por outro lado a desvantagem de ser meros órgãos administrativos (independentes, por certo) com poderes limitados.

A CNPD aprovou em 27 de janeiro de 2000 uma autorização de isenção de dados para a gestão de utentes de bibliotecas e arquivos. Segundo esta permissão, as bibliotecas podem ser armazenados e tratados pelas bibliotecas. No entanto, caso as bibliotecas pretendam transmitir os dados a outras entidades (da administração pública, por exemplo) ou usá-los para outros fins, esta isensão deixa de ter efeitos e passam a ter de pedir autorização a esta entidade (SILVEIRA, 2002, p. 49).

A QUESTÃO DO ANONIMATO

Marques (2004, p. 61-62) considera que o anonimato é um direito na internet, ligado a direitos constitucionais como a liberdade de expressão, o sigilo da correspondência e das comunicações, entre outros. «O anonimato, além de garantir a intimidade, reforça a liberdade de expressão, uma vez que os utilizadores podem participar livremente na rede sem receio de que os seus rastos sejam seguidos» (MARQUES, 2004, 62).

Silva (2005b, 6) abre a porta para o anonimato, mas afirma que este não é um direito absoluto, antes deve ser relativizado em relação a um caso concreto. Para este autor (SILVA, 2005b, 4) é necessário compatibilizar privacidade, o anonimato e a responsabilização, acreditando na existência de um anonimato responsável. Nesse texto o autor afirma que a a navegação anónima se encontra sustentáculo legal no direito à privacidade, bem como na defesa dos seus direitos da personalidade do individuo (SILVA, 2005b, 8-9).

No entanto, num texto subsequente (SILVA, 2006, 9) considera o anonimato total como um fator de comportamentos traiçoeiros e pérfidos, impulsionando as pessoas a comportar-se de forma contrária ao que são depois de desligarem o computador. Assim, este autor acaba por fazer a distinção entre privacidade e anonimato. Já para Lopes e Cabreiro (2006, 79) o anonimato, no sentido de possibilidade garantida pela internet e de nomadismo no que diz respeito aos locais de acesso, é um fator potenciador de atos ilícitos.

Como consequência do anonimato na internet as operadores de serviços (*internet service providers*) tornam-se responsáveis civilmente pelos danos causados por aqueles que usam as suas plataformas. Essa opção legislativa deveu-se a motivos económicos (têm mais possibilidades económicas que os verdadeiros infratores) e pragmáticos (porque é mais fácil responsabiliza-los a eles que aos verdadeiros autores) levou a que elas passassem a ser responsabilizados por danos de terceiros. Exemplo disso é o Decreto-Lei nº 7/2004, que transpõe a Diretiva 2000/31/CE para a legislação portuguesa. Esta lei exige que as operadoras satisfaçam os pedidos judiciais de identificar os destinatários dos serviços com quem tenham acordos de armazenagem, bem como fornecer listas de titulares de sítios que alberguem, quando lhes for pedido.

Segundo Frada (2001, 12) as operadores possuem responsabilidade aquiliniana, ou seja, responsabilidade extracontratual resulta da violação de um dever geral de abstenção. Neste tipo de responsabilidade o ónus da prova cabe ao lesado, por oposição à responsabilidade contratual onde o ónus da prova cabe ao infrator. Por exemplo, no caso de um *hacking* de mensagens por parte

de terceiros, estas só podem ser responsabilizadas se o contrato tiver algumas cláusulas que estipulem tal. Independentemente disso, elas devem estar apetrechadas tecnologicamente e vigiar os seus utilizadores para evitar tais condutas, embora só a podendo facultar esses dados nos termos da lei (FRADA, 2001, 25).

CONFLITO ENTRE DIREITOS FUNDAMENTAIS

Existem portanto conflito entre direitos em situações quotidianas, que a lei não consegue resolver. Nessas situações, são as interpretações da lei que tomam dianteira. Ao nível jurídico uma dessas interpretações é a teoria dos limites imanentes dos direitos constitucionais. Farinho (2006, 56-57) reconhece esta teoria e duas posições opostas sobre ela. Uma desfavorável, que objeta que a sua aplicação pode levar «a uma diminuição da força jurídica ou da extensão dos direitos, liberdades e garantias» (Miranda, 2000 citado por FARINHO, 2006, 57). Outra favorável, argumentando que cada direito tem limites quanto ao seu conteúdo, «na medida em que a proteção constitucional não abranja todas as situações, formas, ou modos de exercício pensáveis para cada um dos direitos» (Andrade, 2001, citado por FARINHO, 2006, 57). Estas questões jurídicas são também questões éticas, como veremos.

Privacidade e Direito à Informação

A liberdade de expressão e o direito à informação fazem parte dos direitos de participação na vida pública. Para além de serem direitos individuais, têm garantia constitucional. Ambos fazem parte da procura de transparência na vida pública, fundamental no estado moderno (DIAS, 2001, 4-5). Marques (2004, 41) menciona que a elaboração da Diretiva 95/46/CE teve por base a procura de um equilíbrio entre a proteção dos direitos de personalidade e o direito à informação, estabelecendo no seu artigo 9º exceções para quem faça esse tratamento para fins exclusivamente jornalísticos, de expressão artística ou literária.

Dias (2001, 2) afirma ainda que o direito fundamental dos cidadãos à informação administrativa, corolário de uma administração que se quer aberta aos cidadãos poderá colidir por vezes com o direito à reserva de intimidade e vida privada dos mesmos, visto que a divulgação de informação pessoal tem vindo a tornar-se, com o desenvolvimento tecnológico um dever para os cidadãos. Esta informação pessoal é depois armazenada, muitas vezes num computador (DIAS, 2001, 6).

Existem divergências doutrinais entre os juristas portugueses sobre a possibilidade de extensão dos limites ao direito à informação procedimental, ou seja, informação contida em factos, atos ou documentos de um concreto procedimento administrativo em curso. Canotilho (apud DIAS, 2001, 8) defende que a transferência do artigo nº 2 para o nº 1 do artigo 268º feita na última revisão constitucional (1997) é inconstitucional pois o direito à informação pela administração pública é um direito sem restrições. Por outro lado, Correia (citado por DIAS, 2001, 8) considera que o direito à informação procedimental e ao acesso aos arquivos administrativos configuram um único direito fundamental – o direito à informação dos administrados – que pode ser limitado pela lei em matérias de segurança interna e externa, investigação policial e à intimidade das pessoas, sendo o nº 1 do artigo 268º da CRP uma garantia do consentimento dos cidadãos.

É neste contexto podem surgir conflitos, sobretudo entre profissionais de arquivo, sobre que documentos deve ser dado o acesso. O artigo 268º da CRP estipula que as leis sobre a intimidade das pessoas devem ser consideradas fator de acesso aos documentos. Essa intimidade inclui os seus dados pessoais, supõe-se. Mas a Lei do Acesso aos Documentos Administrativos (LADA) – Lei nº 65/93 e, posteriormente, a Lei nº 46/2007 - não têm qualquer disposição sobre o assunto.

Privacidade e Segurança

Para Castro (2010, 1) até ao 11 de Setembro as preocupações dos Estados centravam-se na proteção da vida privada, designadamente dos dados pessoais e depois dos atentados às Torres Gémeas a segurança tornou-se no problema central. No entanto, a autora contradiz-se nesse mesmo artigo (CASTRO, 2010, 20) ao lembrar que já antes dos atentados o Conselho da Europa tinha preparado uma Convenção sobre Cibercriminalidade, que 36 países, incluindo Portugal, assinaram. Já para Silva (2006, 4) o 11 de Setembro foi apenas o pretexto para a ascensão de uma preocupação obsessiva com a segurança, incrementada num contexto de insegurança da opinião pública, criando um clima propício a legislação onde os direitos individuais, incluindo o direito à reserva da vida privada, passaram para segundo plano.

Não se pode negar que a segurança é também um direito fundamental. Segundo Castro (2010, p. 21) embora este direito seja visto hoje como um direito negativo, enquanto direito de defesa dos Estados em relação ao cidadão, assume hoje, num contexto de aparecimento de novas formas de terrorismo, grande relevância enquanto direito positivo, enquanto lei protetora contra terceiros. Para Castro (2010, 22 e seguintes) há que criar um equilíbrio entre estes dois direitos, pois o direito à segurança pode afetar de várias formas o direito à autodeterminação informativa e o direito à segurança tem enfraquecido o direito à proteção de dados no pós-11 de Setembro.

Um exemplo desse enfraquecimento é a criação de nova legislação para a conservação de dados a nível europeu, nomeadamente da Diretiva 2006/24/CE. Nascida no contexto dos atentados de Londres em 2005, esta directiva obriga os Estados-Membros a conservarem os dados por períodos não inferiores a seis meses e não superiores a dois anos, pelo que a a legislação anterior sobre apagamento de dados quando deixassem de cumprir a sua função fica sem efeito. e Cabreiro (2006, 74-75) estabelecem uma tipologia de dados de prova com quatro categorias: de localização (dados que indiquem a posição geográfica do utilizador, obtidos nas redes wireless); dados de tráfego (dados informáticos ou técnicos indicando a origem da comunicação, o destino, os trajetos, a hora, a data, o tamanho, a duração e o tipo de serviço subjacente; por exemplo o endereço IP, o endereço do correio eletrónico); dados de base (dados pessoais relativos à conexão de rede, designadamente o número, identidade e morada do cibernauta, bem como a listagem dos movimentos de comunicações; dados de

conteúdo (dados relativos ao conteúdo de uma comunicação). Todos estes dados são designados de prova digital, e servem como pretexto para uma investigação policicial ou prova de um crime.

Para Lopes e Cabreiro (2006, 73) esta legislação é necessária, pois em 2006 tornava-se urgente encontrar soluções para o acesso rápido a informações no âmbito de investigação penal. Para Lopes e Cabreiro (2006, 72) a prova digital deve obedecer às mesmas regras gerais de admissibilidade, autenticidade, precisão e integridade, cujos limites são fornecidos pela lei processual penal e pela CRP.

À luz da interpretação da Diretiva 2006/24/CE, estes autores sustentam que não existe violação das leis de proteção de dados pessoais quando se tem acesso a estes dados, sem autorização judicial ou culpa formada, desde que o cidadão não tenha expresso o desejo previamente destes não serem divulgados, sendo os operadores de internet obrigados a fornecê-los salvo se haja pedido expresso de confidencialidade. Só no caso do titular ter requerido a confidencialidade é que este pedido terá de ser feito através da sentença de um tribunal. No caso de se tratar apenas de prevenção, vigoram os mesmos princípios, embora este caso esteja limitado a uma lista de crimes (LOPES e CABREIRO, 2006, 76). Encontramos aqui todo o espirito do Ato Patriota dos Estados Unidos de 2001.

Lopes e Cabreiro (2006, 78) sugerem ainda que a conservação de dados seja feita por um ano, justificando que no nosso ordenamento jurídico a maioria dos crimes não tem natureza publica, sendo o prazo máximo de apresentação de queixa de seis meses, sendo que este se conta não a partir da data do crime mas da data em que o autor da queixa tiver conhecimento dele.

O conflito entre a necessidade de proteger os dados pessoais e o direito à segurança está cada vez mais presente no dia-a-dia dos profissionais de informação. Por exemplo, a aprovação do Ato Patriota levou as bibliotecas universitárias canadianas a deixar de subscrever a RefWorks, uma popular ferramenta de pesquisa académica, que para além disso fornecia citações e referências bibiográficas. Isto porque as pesquisas de qualquer estudante ou docente das universidades canadianas podia ser encontrada e depois armazenada em bases de dados norte-americanas. Karen Lippold, bibliotecária da Memorial University em St. John's (localidade do estado de Newfoundland and Labrador, no Canadá) afirmou em 2006: «O Ato Patriota dos Estados Unidos - qualquer tipo de notificação - pode ter acesso a informações pessoais das pessoas, e emergiu o sentimento de vulnerabilidade. As suas pesquisas podem ser investigadas pelo Governo dos EUA» (CBS NEWS, 2006).

Privacidade e Consentimento

Pinto (2002, 4-6), que considera que o direito à reserva sobre a vida privada, embora seja considerado na CRP (art. 26º, nº 1) e no CC (art. 80º) como um direito absoluto e intransmissível, é um direito que permite o controlo da informação por parte do seu titular no âmbito do direito à autodeterminação informativa, logo está dependente da sua atuação. Assim, ao tornar-se em direito à autodeterminação informativa, este direito ganha uma componente de liberdade individual, que assim pode modelar o «próprio objeto de proteção» (PINTO, 2002, 5).

Olhando-o como um direito não absoluto, tal como vários autores citados ao longo deste comunicação, Pinto (2002, 7) pensa que o titular pode dispor dele, bastando portanto um mero acordo. Ou seja, o titular de dados pessoais, ao fazer um acordo com outro indivíduo ou organização para fornecer os seus dados pessoais, automaticamente abdica de direitos sobre a sua vida privada. Este autor considera que qualquer consentimento tem valor de um negócio jurídico, aparecendo como um "contrato de autorização", não obstante a sua natureza unilateral (PINTO, 2002, 9-11). Deve apenas tem-se em atenção a integridade do consentimento (se foi sujeito a pressão externa ou não) e que a autorização é limitada temporalmente, podendo ser revogada a qualquer momento (PINTO, 2002, 12-13). acodo com este autor os incapazes (menores e deficientes físicos ou psíquicos) também podem dispor do seu direito à autodeterminação informativa, bastando para tal inferir se no momento em que dispõem dele têm capacidade para aferir as suas consequências, ou seja, têm maturidade suficiente. Só no caso de ser provada a imaturidade do titular é que os tutores terão uma palavra a dizer.

Dentro da perspectiva norte-americana, Pinto (2002, p. 19) chama a qualquer interferência do Estado para proteger a privacidade dos cidadãos, através de legislação, uma «"proteção" paternalista, que se volveria afinal, em tirania – ainda que "tirania da dignidade", em nome de determinada concretização substancial desta» (PINTO, 2002, 19). Para este autor, a comercialização de informações sobre a vida privada é perfeitamente admissível, não considerando, por exemplo, as entrevistas pagas sobre a vida privada como contrárias à ordem pública e aos bons costumes. O direito à vida privada tem uma dimensão patrimonial que pode ser explorada (PINTO, 2002, 22). Trata-se então de olhar a privacidade como uma coisa, mais do que um direito.

Não foram encontradas até hoje quaisquer contestações a estes argumentos por parte de juristas portugueses. Marques (2004, 23) critica de uma maneira geral os autores que em vista dos perigos da informática e da internet para os direitos do homem, se limitam a olhar tais ameaças apenas como ofensas à intimidade da vida privada. Este autor defende que proger a vida privada é também favorecer os outros fundamentais, isto apesar dos conflitos já referidos.

CONCLUSÃO

Como ficou demonstrado, existe uma tradição continental de proteção da privacidade em geral, e da proteção de dados pessoais. Na Europa não existe uma definição de "vida privada" mas existe uma definição de "dados pessoais", trazida pela Diretiva 96/46/CE de 24 de outubro, e depois transposta para as legislações nacionais, enquanto que nos Estados Unidos não existe uma definição consensual de nenhum destes conceitos. A legislação europeia também sofreu várias influências do direito alemão, nomeadamente os três níveis de privacidade e a autodeterminação informativa.

A lei que resultou da transposição da Diretiva reconhece

ao titular de dados inúmeros direitos e contempla o sigilo profissional, superando nesse campo a legislação que lhe teve de base. Mas também tem inúmeras dificiências: não contemplar os dados pessoais de pessoas coletivas, ambiguidade de conceitos e conflitos com a LADA.

A Diretiva 96/46/CE criou também autoridades nacionais de carater administrativo para a proteção dos dados pessoais. Estas autoridades continuam a cumprir um importante papel junto dos cidadãos, empresas e de outras autoridades do Estado. No entanto o seu papel tem vindo a ser posto em causa, como se pode observar no caso do acordo bilateral entre Portugal e os Estados Unidos.

A tendência é, aliás, uma aproximação entre a legislação europeia e norte-americana. Essa aproximação começou logo depois da aprovação da diretiva, com a aprovação do Acordo Porto Seguro. Depois do 11 de setembro os acordos aumentaram ao mesmo tempo que a legislação cada vez se preocupava menos com a proteção dos dados pessoais e vida privada.

Os profissionais de informação devem recolocar então um conjunto de questões éticas relacionadas com a proteção de dados pessoais: até onde deve ser cumprida a Constituição em matéria de proteção da vida privada? Até onde devem ser cumpridos os deveres resultantes da isensão, concedida pela CNPD? Até onde deve ser o direito à privacidade daqueles que requisitam um livro ou, por exemplo, consultam a internet na biblioteca? Deve ser defendido o anonimato? Que direito à informação deve ser dado aos cidadãos pelos profissionais de informação? A modernização administrativa significa o fim do sigilo profissional? O Ato Patriota deve ser considerado uma preocupação ou uma segurança? A privacidade de uma pessoa é vendável? A discussão destes tópicos tem de ser considerada importante agora, e não deixada para o futuro.

REFERÊNCIAS:

BAUMER, David L.; EARP, Julia B. ; POINDEXTER, J. L. - Internet privacy law: a comparison between the United States and the European Union, Computers & security [em linha], Vol. 23, nº. 5 (jul. 2004), p. 400-412 [Consult. 10 de setembro 2012]. Disponível em www: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1823713

CASTRO, Catarina Sarmento e – Protecção de dados pessoais na internet. Sub Júdice. Nº 35 (Set. 2006). Páginas 11-29.

CASTRO, Catarina Sarmento e - Globalização, circulação de pessoas e bens e privacidade [em linha]. [Consult. 2 de Novembro 2011]. Disponível em www: www.estig.ipbeja.pt/~ac_direito/Catarina-Glob.doc . Também disponível em versão PDF em: http://www.buscalegis.ufsc.br/revistas/files/anexos/29731-29747-1-PB.pdf . Conferência proferida oralmente no XXIII Seminário de Plásticos, organizado pela Associação Portuguesa da Indústria de Plásticos, realizado na Póvoa de Varzim, de 25 a 27 de Maio de 2006.

CASTRO, Catarina Sarmento e – O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro [em linha]. [Consult. 30 de novembro de 2011]. Disponível em www: http://www.estig.ipbeja.pt/~ac_direito/CatarinaCastro.pdf

CBS NEWS - Patriot Act fears prompt universities to patriate computers. CBS News Newfoundland and Labrador [em linha]. 31/10/2006. [Consult. 30 de novembro 2011]. Disponível em www: http://www.cbc.ca/news/canada/newfoundland-labrador/story/2006/10/31/patriot-act.html.

COMISSÃO EUROPEIA - A Comissão propõe uma reforma global das regras de proteção de dados para reforçar o controlo exercido pelos utilizadores sobre os seus dados e reduzir os custos para as empresas. Official website of European Union [em linha]. 25/01/2012 [Consult. 23 de setembro 2012]. Disponível em www: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&language=PT .

COUTO, Rute Isabel Esteves Ferreira – Regulação do comércio electrónico [em linha]. [Consult. Em 1 de dezembro 2011]. Disponível em www: http://www.estig.ipbeja.pt/~ac_direito/rcouto.pdf . Artigo baseado em tese de mestrado, defendida em 2004.

DIÁRIO DIGITAL - Ordens profissionais: alterações de regras debatidas hoje na AR. Diário digital [em linha]. 20/09/2012 [Consult. 21 de setembro 2012]. Disponível em www: http://diariodigital.sapo.pt/news.asp?id_news=592670

DIAS, José Eduardo Figueiredo – Direito à informação, à protecção da intimidade e autoridades administrativas independendentes [em linha]. [Consult. Em 1 de dezembro 2011]. Disponível em www: http://www.estig.ipbeja.pt/~ac_direito/proteccao.pdf . Texto publicado originalmente na obra Estudos em Homenagem ao Prof. Doutor Rogério Soares,em 2001.

ESTADOS UNIDOS. Federal Trade Commission – Privacy online fair informatio practices in the electronic marketplace : a report to Congress. Washington : Federal Trade Commission, 2000. [Consult. Em 20 de setembro 2012]. Disponível em www: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf .

FARINHO, Domingos Soares – Intimidade da vida privada e media no ciberespaço. Coimbra : Almedina, 2006.

FRADA, Manuel A. Carneiro da (2001) – gVinho novo em odres velhos?h: a responsabilidade civil das goperadoras da Internet h e a doutrina comum de imputação de danos. In MELO, Alberto de Sá e [et al.] – Direito da sociedade da informação. Coimbra : Coimbra Editora, 2001. Vol. II, p. 7-32.

GOMES, Mário Manuel Vargas (compil.) – O código da privacidade e a protecção de dados pessoais : na lei e na jurisprudência : nacional e internacional. Lisboa : Centro Atlântico, 2006.

GUERRA, Amadeu (2001) – A lei da proteção de dados pessoais. In MELO, Alberto de Sá e [e tal.] – Direito da sociedade da informação. Coimbra : Coimbra Editora, 2001. Vol. II, p. 145-169.

LE MOULLEC, Marianne (2012) – One year of data protection enforcement in France : what the CNIL's

Activity Report Reveals. Privacy law blog [em linha] 14/09/2012. [Consult. 16 de setembro 2012]. Disponível em www: http://privacylaw.proskauer.com/2012/09/articles/workplace-privacy/one-year-of-data-protection-enforcement-in-france-what-the-cnils-activity-report-reveals/#more.

LEVIN, Avner ; NICHOLSON, Mary Jo – Privacy law in the United States, EU and Canada: the allure of the middle ground. University of Ottawa law & technology journal [em linha]. Vol. 2, nº 2 (2005), p. 357-395. [Consult. 2012-09-10]. Disponível em WWW: <URL:http://papers.ssrn.com/sol3/papers.cfm?abstract_id=894079&http://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CBwQFjAA&url=http%3A%2F%2Fpapers.ssrn.com%2Fsol3%2FDelivery.cfm%3Fabstractid%3D894079&ei=P0hWUPLDMcenhAffyIC4BA&usg=AFQjCNEGdFngs1PRl6sq4NNYy6f0zNFRJg>

LOPES, José Mouraz Lopes; CABREIRO, Carlos Antão (2006) – A emergência da prova digital na investigação da criminalidade informática. Sub Júdice. Nº 35 (Set. 2006), p. 71-79.

LUSA - Comissão de Protecção de Dados espera que AR atente às suas recomendações. Público[em linha] 18/08/2011. [. 22 de setembro 2012]. ível em www: http://publico.pt/Sociedade/comissao-de-proteccao-de-dados-espera-que-ar-atente-as-suas-recomendacoes-1508181.

MARQUES, José Augusto Sacadura Garcia (2004) – Internet e privacidade. In MELO, Alberto de Sá e [et al.] – da sociedade da informação. Coimbra : Coimbra Editora, 2004. Vol. IV, p. 23-64.

MARTINS, Agostinho de Castro – O acesso aos documentos da administração pública. Cadernos BAD. Nº 1(2002), p. 20-33.

ORDEM DOS MÉDICOS – Código deontológico [em linha]. [Consult. 22 de setembro 2012]. ível em www: https://www.ordemdosmedicos.pt/?lop=conteudo&op=9c838d2e45b2ad1094d42f4ef36764f6&id=cc42acc8ce334185e0193753adb6cb77.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÓMICO (OCDE) OECD Guidelines on the protection of privacy and transborder flows of personal data [em linha]. [Consult. Em 15 de setembro 2012]. Disponível em www: http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

PINTO, Paulo Mota - A limitação voluntária do direito à reserva sobre a intimidade da vida privada [em linha]. [Consult. 2 de novembro 2011]. Disponível em www: https://woc.uc.pt/fduc/getFile.do?tipo=6&id=2027.
Artigo originalmente publicado In: FIGUEIREDO, Jorge Dias de [et al.] - Estudos em homenagem a Cunha Rodrigues. Coimbra : Coimbra Editora, 2002.

PORTUGAL. Comissão Nacional de Proteção de Dados (CNPD) - Autorização de isenção n.º 2/99. [Consult. 27 de setembro 2012]. Disponível em www: http://www.cnpd.pt/bin/decisoes/1999/htm/ise/ise002-99.htm.

PORTUGAL. Comissão Nacional de Proteção de Dados (CNPD) – Comissão Nacional de Proteção de Dados [em linha] [Consult. 16 de setembro 2012-]. Disponível em www: http://www.cnpd.pt/.

PORTUGAL. Comissão Nacional de Proteção de Dados (CNPD)- Relatório de actividades da CNDP 2011 [em linha]. Lisboa : CNDP, 2012. [Consult. 2012-09-16]. Disponível em www: http://www.cnpd.pt/bin/relatorios/anos/relat2011.pdf.

PORTUGAL. Tratados, etc. - Acordo entre os Estados Unidos da America e a República Portuguesa para reforçar a cooperaçao no dominio da prevenção e do combate ao crime. [Consult. 2012-09-26]. Disponível em www: http://www.dhs.gov/xlibrary/assets/dhs_portugal_crimeagreement_port.pdf . Acordo assinado em 2009.

SILVEIRA, Luís – Os dados pessoais e os arquivos. Cadernos BAD. Nº 1 (2002), p. 46-56.

SILVA, Hugo Lança - O Direito no mundo dos blogues: aproximação à problemática numa perspetiva da responsabilidade civil pelos conteúdos [em linha]. [Lisboa] : Verbojuridico, 2005. [Consult. 30 de outubro 2011]. Disponível em www: http://www.verbojuridico.com/doutrina/tecnologia/blogues.html. Ficheiro ZIP para download, contendo um ficheiro Word.

SILVA, Hugo Lança - Os Internet Service Providers e o direito: são criminosos, são cúmplices, são parceiros da justiça, polícias ou juízes? [em linha]. [Lisboa] : Verbojuridico, 2005. [Consult. 30 de outubro 2011]. Disponível em www: http://www.verbojuridico.com/doutrina/tecnologia/isp.pdf

SILVA, Hugo Lança - Monitorização da internet: onde fica o direito à privacidade? [em linha]. [Lisboa] : Verbojuridico, 2006. [Consult. 30 de outubro 2011]. Disponível em www: http://www.verbojuridico.com/doutrina/tecnologia/monitorizacaointernet.pdf

VERDELHO, Pedro – Cibercrime. In MELO, Alberto de Sá e [et al.] – Direito da sociedade da informação. Coimbra : Coimbra Editora, 2003. Vol. IV, p. 347-383.

Legislação referida:

Constituição da República Portuguesa (CRP)
Código Civil (CC)
Diretiva 96/46/CE de 24 de Outubro de 1995
Diretiva 2006/24/CE de 15 de Março de 2006
Lei nº 10/91 de 29 de Abril de 1991
Lei nº 65/93, de 26 de Agosto
Lei nº 67/98 de 26 de Outubro
Lei n.º 46/2007, de 24 de Agosto