Segurança da Informação, Protecção da Privacidade e dos Dados Pessoais

Ana Vaz
Administradora da Empresa de Gestão Partilhada de Recursos da Administração Pública (GeRAP)

Resumo

As tecnologias da informação conheceram grande desenvolvimento nas últimas décadas, com particular ênfase já no início do século XXI, tornando cada vez mais imperiosa a necessidade de se proteger a informação para que a sua utilização abusiva não venha a servir interesses ilegítimos e atentatórios dos direitos, liberdades e garantias dos cidadãos.
Diversas instituições como a União Europeia, o Conselho da Europa, a OCDE e as Nações Unidas iniciaram e intensificaram o estudo e divulgação de instrumentos que consagram princípios de segurança da informação e de protecção da privacidade, tendo em vista prevenir a ilegítima utilização das tecnologias da informação. O presente artigo estuda os instrumentos mais recentes que cobrem estas áreas, com especial ênfase no que respeita a Portugal.
Este artigo visa reflectir sobre a questão da definição dos limites para a protecção da privacidade face à necessidade de utilização da informação de carácter pessoal a fim de garantir a segurança dos Estados e consequentemente das pessoas: o respeito pelo princípio da proporcionalidade poderá ser a chave do problema.

Abstract
Information Security, Privacy Policy and Personal Data Protection

The information technologies have developed significantly in the past decades, especially since the beginning of the 21st century. However, it is necessary to make sure that the information is used properly, without risking serving illegitimate interests or questioning the rights, liberties and guarantees of citizens.
Several institutions, such as the EU, the Council of Europe, the OSCD and the United Nations have already started studying and developing the tools to assure a balance between information security rights and privacy policy, in order to prevent the illegitimate use of these technologies. This article analyses the more recent tools, especially on what concerns the Portuguese case.
This article reflects on the definition of the limits to protect privacy when what is at stake are the state's (and people) security. Our conclusion tends to advise to apply the proportionality principle, in order to get a balanced solution.

1. Introdução

Portugal, tal como os restantes Estados-Membros da União Europeia e os demais países democráticos, defende os valores da democracia e do respeito pelos direitos humanos. Só é possível beneficiar de liberdade e de justiça num ambiente de segurança, tal como previsto no art. 28º da Declaração Universal dos Direitos do Homem, de 10 de Dezembro de 1948: "Toda a pessoa tem direito a que reine, no plano social e no plano internacional, uma ordem capaz de tornar plenamente efectivos os direitos e as liberdades enunciados na presente Declaração".

Também a Constituição da Republica Portuguesa, no seu artigo 273º, mostra preocupação pela segurança das pessoas nos seguintes termos:

"1. É obrigação do Estado assegurar a defesa nacional.

2. A defesa nacional tem por objectivos garantir, no respeito da ordem constitucional, das instituições democráticas e das convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações contra qualquer agressão ou ameaça externas."

A defesa nacional abrange também, como se vê, a segurança das pessoas que tem naturalmente a ver com a defesa dos seus direitos, liberdades e garantias a que se referem os artigos 2º, 18º e 19º da Constituição da República Portuguesa: aí se define a República Portuguesa como um Estado de Direito Democrático em que se garantem os direitos e liberdades fundamentais, só limitados em caso de estado de sítio ou de emergência.

Por isso, os objectivos estratégicos da segurança e defesa nacional são a independência nacional, a integridade do território e a segurança e liberdade dos cidadãos.[1]

A defesa dos direitos fundamentais envolve também a protecção da privacidade, preocupação constitucional quando se prevê que todos têm direito à reserva da intimidade da vida privada e à sua imagem.

1 Lei de Defesa Nacional e das Forças Armadas – Lei nº 29/82, de 11 de Dezembro. **A segurança nacional** define-se como a condição da nação que se traduz pela permanente garantia da sua sobrevivência em paz e liberdade; assegurando a soberania, independência e unidade, a integridade do território, a salvaguarda colectiva de pessoas e dos valores espirituais, o desenvolvimento normal das tarefas do estado, a liberdade de acção política dos órgãos de soberania e o pleno funcionamento das instituições democráticas.(Instituto da Defesa Nacional).

A liberdade tem pois, como pressuposto necessário, tanto o *direito à segurança* como o *reconhecimento de direitos fundamentais.*

Se bem que no mundo actual se tenham atenuado as tradicionais ameaças de cariz militar, surgem agora novos riscos e ameaças potenciais de que são exemplo os trágicos acontecimentos do 11 de Setembro, em Nova Iorque, bem como os de Londres e Madrid. Assim, foi alterada a situação político-estratégica internacional, criando-se novos desafios no contexto internacional e eliminando-se fronteiras definidas, o que leva a falar mesmo em "riscos multifacetados e multidimensionais". [2]

Aos Estados cabe resolver o problema das ameaças à segurança dos cidadãos, protegendo-os inclusive da criminalidade organizada, mesmo a transnacional, sem deixar ao mesmo tempo de prover a que os dados pessoais não sejam utilizados indevidamente, nem a privacidade das pessoas injustificadamente atingida.

A necessidade de protecção da privacidade e dos dados pessoais conheceu notável agravamento pelo facto de as tecnologias da informação terem registado grande desenvolvimento nas últimas décadas, com particular ênfase já no início do século XXI, tornando cada vez mais imperiosa a necessidade de se proteger a informação para que a sua utilização abusiva não venha a servir interesses ilegítimos e atentatórios dos direitos, liberdades e garantias dos cidadãos.

De facto, estas novas tecnologias, sendo dinamizadoras de desenvolvimento, segurança e bem-estar, vieram também a revelar-se como potencialmente atentatórias do direito à privacidade de cada indivíduo, uma vez que permitem conhecer e divulgar os movimentos das pessoas, os seus gostos, as suas características e até a sua saúde física e mental.

A segurança e a privacidade são assim valores que devem estar associados à utilização dos sistemas de informação uma vez que é nestes sistemas que se baseiam as actividades dos Estados, das instituições, das empresas e dos cidadãos.

Diversas instituições como a União Europeia, o Conselho da Europa, a OCDE e as Nações Unidas iniciaram e intensificaram o estudo e divulgação de instrumentos que consagram princípios de segurança da informação e de protecção da privacidade, tendo em vista prevenir a ilegítima utilização das tecnologias da informação.

A Internet começou por ser um meio de comunicação livre em que não havia interferência por parte dos governos e a liberdade de expressão e a privacidade eram garantidas. Hoje a Internet é o suporte de infra-estruturas vitais como as da segurança,

2 Conceito Estratégico de Defesa Nacional RCM nº 6/2003.

energia, transportes e actividades financeiras, e como tal, alvo de ameaças à liberdade dos cidadãos e segurança dos Estados trazendo à ribalta questões sobre a privacidade que antes não eram importantes.

Pretende-se efectuar uma análise do tema, a partir dos estudos e instrumentos regulamentadores no âmbito nacional, comunitário e internacional e reflectir sobre a questão da definição dos limites para a protecção da privacidade face à necessidade de utilização da informação de carácter pessoal para finalidades que podem ser consideradas com um valor objectivamente maior, como é o caso da segurança dos Estados e consequentemente das pessoas.

No desenvolvimento são analisadas as ameaças que impendem sobre a segurança da informação e sobre a defesa da privacidade, bem como as correspondentes medidas de protecção e o estabelecimento do necessário equilíbrio entre a segurança da informação e a protecção da privacidade e dos dados pessoais. Para tanto, estudam-se os instrumentos mais recentes que cobrem estas áreas, com especial enfoque para Portugal, sempre com a preocupação de pôr em evidência o estado da arte do tema objecto deste trabalho.

Visa-se efectuar uma reflexão que relacione a segurança da informação com a protecção da privacidade e dos dados pessoais, salientando aspectos que evidenciem o indispensável equilíbrio entre os dois temas objecto deste artigo, e sugerindo mais adequada divulgação e consciencialização dos direitos fundamentais e dos riscos em que a sociedade globalizada os faz incorrer.

2 . Segurança da Informação

A informação é um recurso que tem valor essencial para as organizações, incluindo-se nesta acepção os Estados: é um valor decisivo e fundamental nos dias em que vivemos e assume um aspecto relevante na segurança e defesa das nações. Qualquer interrupção de serviço público, utilização indevida de informação classificada ou destruição de dados de cariz importante pode pôr em causa a confiança dos cidadãos e os interesses – e até a própria soberania – dos Estados.

Em contrapartida os sistemas de segurança da informação devem também ter em conta as ameaças que hoje se colocam às liberdades individuais, à protecção dos dados pessoais e consequentemente à privacidade.

Face aos desenvolvimentos das tecnologias atrás salientados, os problemas da segurança da informação dizem hoje sobretudo respeito à protecção da informação

armazenada, processada ou transmitida sob forma electrónica, contra ameaças deliberadas ou acidentais.[3]

As mudanças tecnológicas das últimas décadas vieram dar importância crescente à informação, quer ela seja utilizada a nível pessoal, quer nas organizações ou nos Estados. É nestes níveis que se deve ponderar a exigência de segurança e o seu impacto nos sistemas de Segurança e Defesa.

A informação é crucial nos âmbitos político, social e económico e daí a sua importância crescente no sector de Defesa, quer entendida em sentido lato[4] quer no sentido restrito de cariz militar.

Ao Estado Português cabe *garantir em todos os momentos a funcionalidade dos sistemas vitais de segurança nacional, nomeadamente as redes de energia, comunicações, transportes, abastecimentos e informação*.[5]

Haverá ainda que ter em conta não só os Sistemas de Informação em geral mas também, em particular, os sistemas de Informações *(intelligence*) definindo-se estes como os sistemas que processam informação classificada, isto é, de acesso restrito a pessoas credenciadas para o efeito.

Um sistema de informação é considerado seguro se reunir as seguintes características:

- Confidencialidade, no sentido de permitir o acesso apenas a utilizadores autorizados;
- Integridade, ou seja, a garantia de que a informação é a correcta;
- Disponibilidade, o que significa a possibilidade de utilizar a informação quando ela é necessária.

Na base dos sistemas de informação relevam actualmente os sistemas informáticos, pelo que a segurança informática assume particular importância visando salvaguardar a sua integridade funcional e prevenir a divulgação, distorção ou destruição ilícita de

3 Comissão Europeia, *Livro Verde sobre a segurança dos sistemas de informação, 1994*.

4 Por *Defesa Nacional* entende-se o conjunto de medidas, tanto de carácter militar como político, económico, social e cultural que, adequadamente integradas e coordenadas, e desenvolvidas global e sectorialmente, permitem reforçar as potencialidades da nação e minimizar as suas vulnerabilidades, com vista a torná-la apta a enfrentar todo o tipo de ameaças que, directa ou indirectamente, possam pôr em causa a segurança nacional (IDN).

5 Resolução do Conselho de Ministros nº 6/2003 que aprova o Conceito Estratégico de Defesa Nacional.

informação, fazendo apelo à utilização de técnicas físicas e lógicas, tendo em conta as características do *hardware*, do *software*, das instalações e dos procedimentos.

Pensando hoje numa sociedade global há que tomar medidas a nível internacional que incluam organizações, Estados e também empresas privadas, para que seja possível a partilha de informação e o seu tratamento de acordo com critérios estabelecidos e aceites por todos.

A Organização das Nações Unidas estabeleceu o dia 17 de Maio como dia Mundial da Sociedade da Informação que, em 2006, foi dedicado à promoção da cibersegurança. Nas comemorações deste dia o Secretário-Geral das Nações Unidas, Kofi Annan, salientou que "num mundo crescentemente interligado e em rede, defender os nossos sistemas e infra-estruturas vitais contra o ataque de cibercriminosos e ao mesmo tempo promover a confiança em transacções electrónicas assume uma importância crítica, para promover as trocas, o comércio, as relações bancárias, a telemedicina, a administração pública electrónica e outras aplicações electrónicas".

O Conselho da Europa, reconhecendo a importância de responder ao desafio da criminalidade informática que, na grande maioria das vezes, tem um carácter transfronteiriço, desenvolveu esforços no sentido de harmonizar as legislações e práticas a nível internacional. Em consequência, aprovou em 1989 a Recomendação nº R(89)9 sobre a criminalidade relacionada com os computadores.

Também a Organização de Cooperação e de Desenvolvimento Económico (OCDE), que, em 1992, tinha estabelecido linhas directrizes para a segurança dos sistemas de informação, face ao desenvolvimento que estes sistemas sofreram, procedeu à sua reanálise em 1997. Para tanto incumbiu um Grupo de Trabalho[6] de estudar a nova situação face ao aumento crescente de ameaças, designadamente a tragédia do 11 de Setembro e, em 25 de Julho de 2002, o Conselho da OCDE aprovou novas Linhas Directrizes para a Segurança dos Sistemas de Informação e das Redes.

No âmbito da União Europeia, foi criada, em 2004, a Agência Europeia para a Segurança das Redes e da Informação[7] com o objectivo primordial de reforçar a capacidade dos Estados-Membros na área da prevenção, tratamento e resposta aos problemas de segurança da informação e das redes.

Por sua vez, também a International Standardization Organization (ISO) revelou preocupação em definir normas para os padrões de segurança, destacando-se a ISO

6 Grupo sobre a segurança da informação e a vida privada do Comité de Política da Informação, da Informática e das Comunicações (PIIC) da OCDE.

7 Regulamento (CE) n.º 460/2004, de 10 de Março de 2004.

17799:2000[8] que trata aspectos como a política de segurança, a segurança da organização, a segurança pessoal, física e ambiental, o controlo de acessos e o desenvolvimento de sistemas e manutenção, e a ISO 15443[9] mais dirigida para a segurança na informática.

Também em Portugal houve a preocupação de definir normas de segurança, designadamente para informação reservada, para que os tratamentos automatizados estejam em conformidade com a classificação de segurança, tendo em vista a defesa do Estado e de organizações de que Portugal faça parte, como sejam:

- SEGNAC 1 – Instruções para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas com normas de segurança informática dirigidas a elementos da Administração Pública;[10]
- SEGNAC 2 – Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas: Segurança Industrial, Tecnológica e de Investigação;[11]
- SEGNAC 3 – Instruções para a segurança Nacional: Segurança das Telecomunicações;[12]
- SEGNAC 4 – Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas: Segurança Informática.[13]

Os programas de computador, tal como os documentos, devem ser classificados, segundo critérios estabelecidos, em "Muito Secreto", "Secreto", "Confidencial" ou "Reservado", e esta é uma responsabilidade atribuída aos directores de empresas, organismos e serviços. Os documentos classificados de "Muito Secreto" e "Secreto" só podem ser objecto de tratamento informático se a entidade que lhes deu origem não se opuser.

Para garantir a segurança das matérias classificadas, foi criada a Autoridade Nacional de Segurança, no âmbito da Organização do Tratado do Atlântico Norte (OTAN). O Instituto de Informática do Ministério das Finanças e a Autoridade Nacional de Segurança publicaram, em 1995, o "Manual Técnico de Segurança dos Sistemas e Tecnologias de Informação" que reúne os princípios de segurança da informação a ter

8 ISO 17799:2000 – Code of Practise for Information Security Management.
9 ISO 15443 – Information Technology – Security Techniques.
10 Resolução do Conselho de Ministros n.º 50/88, de 3 de Dezembro.
11 Resolução do Conselho de Ministros n.º 37/89, de 24 de Outubro.
12 Resolução do Conselho de Ministros n.º 16/94, de 22 de Março.
13 Resolução do Conselho de Ministros n.º 5/90, de 28 de Fevereiro.

em conta pelos responsáveis dos sistemas informáticos, quer da Administração do Estado, quer de organizações privadas.

Pelo Decreto-lei nº 217/97, de 20 de Agosto, o serviço do Ministério da Defesa Nacional designado por Autoridade Nacional de Segurança passou a designar-se por Gabinete Nacional de Segurança. Entre as suas competências cabe salientar a de inspeccionar periodicamente os órgãos de segurança com vista a verificar o cumprimento de disposições de segurança, designadamente das comunicações, da informática e dos sistemas de informação.

2.1 Ameaças à segurança da informação

Face à sua crucial importância, a informação e o saber passaram também a ser parte nevrálgica dos conflitos actuais, chegando mesmo a falar-se em Guerra de Informação que enquadra "aspectos de segurança que devem preservar os interesses de cidadãos, Estados e organizações nacionais e supranacionais de interesse público, contra acções que os pretendam prejudicar," enquanto que, em sentido restrito, "corresponde à utilização da informação que apresente aspectos de conflitual idade entre actores da sociedade".[14] A Guerra do Golfo foi considerada a primeira guerra da Era da Informação.

A transmissão de dados através da Internet é já essencial para a vida em sociedade mas apresenta uma grande vulnerabilidade porque existem múltiplas hipóteses de actuação de *hackers* e *crackers* para atacarem deliberadamente os sistemas informáticos. Por vezes actuam por conta própria e noutras situações enquadrados em organizações terroristas.

A forma de comunicação possibilitada pelo uso da Internet faz desta um novo "Teatro de Guerra", como referiu o General Loureiro dos Santos no âmbito de conferência ao Curso de Defesa Nacional de 2005/2006, altura em que também salientou que a Internet é a grande *madrassa* da guerra santa, pois os ensinamentos e comando de operações terroristas são feitos através dela.

As ameaças à segurança da informação visam desencadear um incidente que venha a provocar danos num sistema de informação ou entidade e podem ser deliberadas ou involuntárias, de natureza física ou lógica.

14 Dinis, José António Rodrigues, *Guerra de Informação*, edição Silabo, 2005.

A informação está armazenada em suportes: edifícios, cofres de segurança, dispositivos electrónicos. Todos estes suportes podem estar sujeitos a ameaças físicas tanto naturais (terramotos, inundações, incêndios), como por acção humana (fogo posto, bombardeamentos, disseminação de gases, cortes nas redes de abastecimento público).

De entre as ameaças lógicas relevam o acesso e utilização ilegítima da informação, a intercepção de comunicações e outras acções criminosas, tais como a fraude informática, a falsidade informática, a espionagem informática, danos em dados ou programas, sabotagem informática, acesso ilegítimo a dados ou programas e a intercepção ilegítima.

Uma das formas mais correntes de obter ilegitimamente segredos militares ou comerciais é a intercepção de comunicações. A ligação de sistemas de informações à Internet constituiu um factor de risco acrescido para a vulnerabilidade desses sistemas, uma vez que a comunicação pode ser mais facilmente interceptada e os dados desviados.

2.2 Protecção da segurança da informação

Perante o elenco de ameaças enunciadas, os Estados e outras entidades têm vindo a preocupar-se com a adopção de medidas que permitam anular os efeitos das ameaças referidas e das agressões delas consequentes. Tal como as ameaças, também as medidas de protecção têm carácter físico ou lógico a que se vão somar as medidas de carácter legislativo. As medidas de protecção físicas devem incidir sobretudo nas instalações dos sistemas informáticos, incluindo os edifícios e equipamentos em que estão sedeados. As medidas de segurança lógica têm particularmente a ver com a segurança dos dados, dos programas e das redes.

Das várias medidas que têm vindo a ser tomadas para defender sistemas de informação, figuram, entre as mais divulgadas, o uso de códigos de acesso *(passwords*), de *firewalls* e de programas *antivírus*, cada vez mais sofisticados de harmonia com a importância da informação cujo acesso se pretende proteger e a eventual permeabilidade a ataques de *hackers* e *crackers*.

A SEGNAC 4 inclui um capítulo dedicado à segurança física das instalações e um outro à segurança lógica onde indica procedimentos de prevenção para controlo lógico de acessos, tais como a utilização de *passwords* e seu controlo posterior, bem como medidas a observar na recolha, tratamento e divulgação de resultados ou no desenvolvimento e aquisição de suportes lógicos.

Outra das protecções tradicionais para evitar o conhecimento do conteúdo das mensagens transmitidas é a utilização da criptografia, disciplina que inclui os princípios,

meios e métodos de transformação de dados, com a finalidade de ocultar o seu conteúdo: este torna-se ininteligível, salvo para pessoas autorizadas.

A OCDE, tendo em vista o uso seguro das tecnologias da informação para garantir a confidencialidade e integridade dos dados e especialmente a protecção da vida privada, elaborou as Linhas de Orientação para uma Política de Criptografia[15] adoptadas pelo Conselho em 1997, e que visam, entre outros:

"– Promover a utilização da criptografia de forma a aumentar a confiança nas tecnologias e assim proteger a informação, designadamente os dados pessoais e consequentemente a vida privada;

– Tomar medidas para que a criptografia não ponha em risco a segurança pública, o cumprimento das leis e a segurança nacional;

– Fomentar a existência de políticas e legislações compatíveis e a troca de experiências entre os diversos Estados e organizações."

No domínio das comunicações escritas é essencial recorrer também à assinatura electrónica,[16] um meio criptográfico de assegurar a integridade e a autenticidade dos documentos.

As assinaturas electrónicas podem assumir várias modalidades: biométricas, quando se baseiam em características físicas da pessoa; holográficas, quando construídas a partir de características constantes da assinatura; ou digitais, quando são baseadas num sistema criptográfico assimétrico constituído por duas chaves, uma pública e outra privada.

Para que uma assinatura digital cumpra o objectivo previsto na legislação portuguesa deve ser fornecida por uma entidade certificadora. Estas entidades fazem acompanhar as assinaturas de um certificado digital que garante a titularidade da chave pública e a data da sua validade. As entidades certificadoras são credenciadas na União Europeia por autoridades credenciadoras. Em Portugal, a autoridade credenciadora é a Autoridade Nacional de Segurança.[17]

Em Portugal tem havido medidas para introduzir formas avançadas de segurança em sistemas de informação mais sensíveis: existindo várias entidades com atribuições no

15 Anexo à Recomendação do Conselho da OCDE adoptada na 895ª Sessão.
16 Seabra Lopes, *Direito dos Registos e do Notariado*, Almedina., 2005.
17 Decreto-Lei nº 116-A/2006, de 16 de Junho.

âmbito da segurança, tais como as Forças Armadas, a Polícia de Segurança Pública, a Guarda Nacional Republicana, a Polícia Judiciária, o Serviço de Informações de Segurança, a Direcção-Geral dos Serviços Prisionais, o Serviço Nacional de Bombeiros e Protecção Civil, entre outros, foi sentida a necessidade de criar uma rede nacional única, em tecnologia *trunking* digital, partilhada por estas forças e serviços de segurança e emergência. Assim, o Governo aprovou, em Maio de 2006, a adjudicação da parceria público-privada para o projecto SIRESP – Sistema Integrado das Redes de Emergência e Segurança de Portugal, que engloba serviços especiais de telecomunicações para garantir a eficácia dos sistemas de segurança, designadamente em situações de crise, por ocorrência de terramotos, incêndios, atentados terroristas, etc.

2.3 Medidas legislativas de protecção da segurança da informação

Atendendo à importância crescente dos sistemas informáticos e das redes de comunicações nos Estados e a preocupação com o número de violações da sua segurança, também em crescimento, o Conselho da União Europeia e o Parlamento têm vindo a estabelecer um enquadramento jurídico que permita regulamentar a segurança dos sistemas informáticos, designadamente das redes e dos serviços de comunicações.

Já em 1992, atendendo à importância crescente da informação nas actividades económicas e sociais, o Conselho das Comunidades Europeias decidira adoptar um instrumento[18] para enquadrar a acção no domínio da segurança dos sistemas de informação.

No seguimento desta preocupação, foi aprovada, especificamente na área das comunicações electrónicas, a Directiva 2002/21/CE, de 7 de Março de 2002, que define as atribuições de autoridades reguladoras nacionais de forma a garantir a harmonia e a coerência das práticas dos diversos Estados-Membros em matéria de redes e serviços de comunicações electrónicas.

Foi também aprovada a Directiva 2002/58/CE de 17 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, que enumera as condições em que os Estados-Membros podem restringir os direitos e obrigações dos prestadores dos serviços de comunicações para salvaguardar a segurança nacional, a defesa, a segurança pública no sentido de prevenir e investigar infracções penais ou a utilização ilegítima das comunicações electrónicas.

18 Decisão do Conselho 92/242/CEE, de 31 de Março de 1992, no domínio da segurança dos sistemas de informação.

Já a Convenção de Aplicação do Acordo de Schengen, de que Portugal é parte contratante, indicou[19] as medidas a tomar para garantir a segurança do Sistema de Informação Schengen relativas a controlo da entrada nas instalações, controlo dos suportes de dados, controlo da inserção, controlo da utilização, controlo de acesso, controlo de transmissão, controlo da introdução, e controlo do transporte.[20] No caso de transmissão de dados ou de serviços situados fora dos territórios das partes contratantes devem ser tomadas medidas específicas para garantir a sua segurança.

Face aos atentados terroristas, o Conselho e o Parlamento da União Europeia, em Dezembro de 2002, tendo em conta que os dados gerados no sistema de comunicações são um instrumento muito útil para combater a criminalidade organizada, aprovaram a Directiva 2006/24/CE, de 15 de Março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações.

As matérias protegidas pelo segredo de Estado estão submetidas a um regime particular de protecção, nos termos da Lei n.º 6/94, de 7 de Abril: todos os documentos e informações cujo conhecimento por pessoa não autorizada ponha em risco ou prejudique a independência nacional, a unidade e integridade do Estado e a sua segurança interna e externa são abrangidos pelas normas que configuram o segredo do Estado. Os documentos submetidos a este regime são objecto de adequadas medidas de protecção contra acções de sabotagem e de espionagem e contra fugas de informação.[21] À Comissão para a Fiscalização do Segredo de Estado cabe velar pelo cumprimento da lei.

Em Portugal, tal como noutros países europeus, os ataques à segurança da informação, em respeito aliás pela Recomendação 89 (9) do Conselho da Europa, atrás referida, são sancionados criminalmente. Assim, a Lei nº 109/91, de 17 de Agosto, sobre a criminalidade informática, sanciona com penas de prisão os crimes de falsidade informática, danos relativos a dados ou programas informáticos, sabotagem informática, acesso e intercepção ilegítimos; por sua vez, o Código Penal prevê no art. 221º a punição criminal da burla informática.

A protecção das comunicações em documentos escritos, garantida pelo uso da assinatura digital, foi objecto em Portugal, do Decreto-Lei nº 290-D/99, de 2 de Agosto,

19 Decreto do Presidente da Republica nº 55/93, art. 118º.

20 Este dispositivo inspirou o legislador português que fez reflectir estas medidas no artigo 15º sobre medidas especiais de segurança da Lei n.º 67/98, de 26 de Outubro, relativa à protecção de dados.

21 Lei n.º 6/94, de 7 de Abril, art. 8.

alterado pelos Decretos-Lei nº 62/2003, de 3 de Abril, 165/2004, de 6 de Julho e 116-A/2006, de 16 de Junho, e ainda pelo Decreto Regulamentar nº 25/2004, de 15 de Julho, que regulam a assinatura electrónica e a validade dos documentos electrónicos. Face à aprovação da Directiva 1999/93/CE, de 13 de Dezembro, que trata o quadro legal comunitário para as assinaturas electrónicas, o Decreto-Lei nº 62/2003 veio compatibilizar o regime jurídico português da assinatura digital com as disposições comunitárias.

Ainda no domínio da protecção legislativa da segurança da informação, a Lei n.º 67/98, de 26 de Outubro, não obstante ter como primeiro objectivo a protecção de dados pessoais, e a que adiante se fará referência detalhada, prevê, nos seus artigos 14º e 15º normas para a segurança dos tratamentos da informação que envolvem dados pessoais.

O acesso aos documentos administrativos que possam pôr em risco ou causar danos à segurança interna e externa do Estado ficam sujeitos à interdição de acesso ou a acesso condicionado, nos termos previstos pela Lei nº 65/93, de 26 de Agosto, alterada pela Lei n.º8/95, de 29 de Março.

3. Protecção da Privacidade e dos Dados Pessoais

A defesa da privacidade ou da reserva da intimidade da vida privada e familiar,[22] como se lhe refere a Constituição da República Portuguesa, é uma preocupação relativamente recente.

A noção de privacidade passou a ter mais pertinência quando começaram a surgir as grandes cidades e com elas os desconhecimentos mútuos das pessoas que nelas habitam. A possibilidade de se esconder quem se é na realidade, ou obter benefícios por se descobrirem determinadas situações da vida privada de outros, passou a ser um factor a ter em conta na vida moderna, sobretudo devido ao aparecimento de meios de comunicação, como a imprensa e mais tarde a televisão, que permitem a divulgação imediata, e a um número muito elevado de pessoas, de acontecimentos de índole íntima. Passou assim a ser possível destruir a reputação de uma pessoa ou divulgar dados da sua vida íntima.[23]

22 CRP, art. 26º, nº 1.

23 Cf Seabra Lopes, *A protecção da privacidade e dos dados pessoais na sociedade da informação: tendências e desafios numa sociedade em transição* em Estudos em homenagem ao Prof. Almeida Costa, Universidade Católica Portuguesa.

Em 1890, esta noção de privacidade era já uma preocupação tendo Samuel Warren publicado o artigo intitulado *The right to privacy*[24] em que se defendia pela primeira vez o reconhecimento do direito à privacidade e à reserva da vida privada.

Mas só em 1948 a Assembleia Geral das Nações Unidas proclamou a Declaração Universal dos Direitos do Homem que refere no art.12º – "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicilio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques, toda a pessoa tem direito à protecção da lei.", consagrando assim o princípio do respeito pela vida privada.

Logo a seguir, em 1950, foi reafirmado na Convenção Europeia dos Direitos do Homem que "toda a pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência".[25]

Por sua vez, o desenvolvimento da informática e a possibilidade de efectuar pesquisas em grandes bases de dados – bancos, serviços fiscais, segurança social – e consequente acesso a dados pessoais, possibilitou a utilização abusiva e ilícita desses dados; o progresso das novas tecnologias permite hoje conhecer os movimentos das pessoas, não só desde que saem de casa, mas até no seu interior, através de vigilância electrónica e da utilização da Internet.

No conceito de dados pessoais são abrangidos os elementos que usualmente servem para identificar uma pessoa (nome, apelido, morada, data, lugar de nascimento...) bem como qualquer conjunto de informações que permitam identificar uma pessoa por referência a um número de identificação ou através de elementos específicos relativos à sua identidade física, fisiológica, psíquica, económica, cultural ou social, incluindo a voz e a imagem da pessoa.[26]

O Conselho da Europa sempre manifestou preocupação pelo estudo desta matéria, pelo que, em 1981, submeteu à assinatura dos Estados membros a Convenção 108 para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados Pessoais, dando especial atenção aos dados sensíveis, como são os relativos à saúde, vida sexual ou condenações penais. Esta Convenção consagra princípios de protecção de dados que vieram posteriormente a ser desenvolvidos.

---

24 Samuel Warren e Louis D. Brandeis, Harvard Law Review, citado em J. de Seabra Lopes, *A protecção da privacidade e dos dados pessoais na sociedade da informação: tendências e desafios numa sociedade em transição.*

25 Art. 8º, n.º 1.

26 Directiva 95/46/CE, de 24 de Outubro de 1995, art. 2º al a) e Lei nº 67/98, de 26 de Outubro, art. 3º al) a).

Também, tendo em vista a livre circulação da informação entre os Estados membros de forma a desenvolver as relações económicas e sociais, a OCDE, já aprovara, no ano anterior, as linhas directrizes relativas à protecção da vida privada e dos fluxos transfronteiriços de dados de carácter pessoal.[27]

No mesmo sentido, a Assembleia Geral das Nações Unidas aprovou, em 1990, as linhas directrizes relativas aos ficheiros automatizados de dados pessoais, referindo pela primeira vez em instrumentos internacionais a necessidade de previsão de uma autoridade responsável em cada país pelo cumprimento dos princípios de protecção de dados pessoais.

Em 1995, a União Europeia aprovou uma directiva sobre a protecção de dados pessoais,[28] inspirada em instrumentos já existentes, designadamente a Convenção 108, mas ampliando o campo de aplicação aos dados tratados manualmente e prevendo a obrigatoriedade de uma autoridade independente que em cada Estado membro velasse pelo cumprimento dos princípios.

Face ao crescente desenvolvimento da Internet e aos novos problemas criados pela sua utilização, o Conselho da Europa aprovou, em 1999, a Recomendação R(99)5 que estabelece as Linhas Directrizes para Protecção das Pessoas face à Recolha e Processamento de Dados Pessoais nas Auto-estradas da Informação, tendentes a assegurar uma utilização correcta da Internet e chamando também a atenção dos fornecedores de serviços de acesso à rede.

Em 2000, o Conselho de Nice proclamou a Carta dos Direitos Fundamentais da União Europeia que, nos seus artigos 7º e 8º, confirma o direito ao respeito pela vida privada e à protecção dos dados pessoais.

3.1 Ameaças à privacidade e aos dados pessoais

Já foi referida a possibilidade de tanto o direito à privacidade, como os dados pessoais, serem objecto de actuações ilegítimas por parte de terceiros. De facto, o aparecimento dos grandes sistemas informáticos em 1970 e sobretudo a sua conjugação com novos meios de comunicação, veio potenciar o acesso indevido a dados pessoais e a sua utilização sem conhecimento do seu titular. Todos recebemos publicidade, nas

27 Recomendação do Conselho da OCDE relativa às Linhas Directrizes sobre protecção da vida privada e dos fluxos transfronteiriços de dados pessoais, aprovada em 23 de Setembro de 1980.

28 Directiva 95/46/CE de 24 de Outubro de 1995, transposta pela Lei nº 67/98, de 26 de Outubro.

caixas de correio, que nos é endereçada sem que tenhamos fornecidos os dados para tal ou vemo-nos invadidos com "*spam*" que pode até ser agressivo para os valores que nos são caros de que são exemplo as mensagens electrónicas de publicidade a certos produtos.

É corrente a instalação de *cookies* que pode ser utilizada para estabelecer um perfil do utilizador e desta forma vir a desvendar mesmo aspectos da vida íntima ou de *web bugs*, que ficam também registados no disco do computador, por exemplo através de uma mensagem de correio electrónico, e que permitem dar a conhecer ao servidor a que o computador está ligado as pesquisas efectuadas, dia e hora.

A recolha e interconexão de dados pessoais, particularmente de dados sensíveis, são outra das ameaças mais correntemente citadas: os serviços da administração do Estado, bem como grandes empresas e instituições financeiras, recolhem informações sobre as pessoas e com elas constituem grandes bases de dados pessoais, necessárias ao cumprimento das suas atribuições. Ao estabelecer uma interconexão entre essas bases é possível obter informações de carácter privado, como a religião ou a saúde, que se podem revelar discriminatórias em situação de candidatura a emprego ou outras similares.

A recolha de dados pessoais é facilitada pelo uso da telemetria e da videovigilância, novas potenciais ameaças de invasão da privacidade e de uso indevido de dados pessoais. Actualmente existem câmaras que permitem filmar as pessoas e os seus comportamentos em estações ferroviárias ou de metro, armazéns, ruas ou parques de estacionamento, muitas vezes sem as pessoas se aperceberem. É público que, em Londres, um cidadão pode ser filmado, em média, 300 vezes durante o dia.[29]

Cada vez mais modernas tecnologias vão constituindo potenciais novas ameaças. Os detectores de som permitem escutar conversas no interior de edifícios ou supostamente mantidas na privacidade do lar. O sistema GPS (*Global Positioning System)* permite que um utilizador de telefone celular seja localizado; nada impede até que um dispositivo de localização com este sistema seja colocado num carro ou no bolso de uma pessoa, dando informações sobre a localização de alguém que desconhece que está a ser vigiado, como foi contado no romance "Código da Vinci".

Por sua vez, os cartões electrónicos com dados de carácter pessoal, designadamente dados biométricos,[30] permitem controlar o acesso a instalações, bem como as deslocações

29 William Underhill, *Big Ben or Big Brother?,* Newsweek, 28 de Fevereiro de 2000 citado por Seabra Lopes.

30 O dado biométrico como a impressão digital é um dado pessoal uma vez que permite a identificação do seu titular.

dentro da organização, até para utilização de instalações sanitárias,[31] como já aconteceu com uma empresa de calçado no norte do país.

Outros aspectos da vida privada podem ser ameaçados pelos sistemas informáticos no local de trabalho, na medida em que é possível ter conhecimento de todos os telefonemas efectuados (dia, hora, número chamado e duração), os sítios da Internet a que acede ou até medir a produtividade do trabalhador através da recolha de dados automática (tempo de utilização do computador, registos efectuados, etc.).

Nas residências privadas, a utilização de sensores de fluxos de fluidos que permitem medir e registar no computador os consumos de gás, electricidade e água dão, por exemplo, indicação sobre a desocupação de casas ou sobre os hábitos e comportamentos dos residentes. Foi através do controlo de consumo de gás que a polícia alemã conseguiu localizar a célula terrorista *Baader-Meinhof*. Os sensores de temperaturas até já permitiram detectar pela polícia norte-americana a existência de *grow lights* utilizadas para cultivar marijuana dentro de casa.

Em Portugal, de 2004 para 2005 houve um aumento de 25% de crimes de devassa da vida privada através da Internet,[32] tendo-se registado neste ultimo ano, 70 inquéritos policiais. O autor deste tipo de crime divulga na Internet informações sobre a vítima com quem, usualmente, tem uma relação de proximidade.

3.2 Medidas de protecção da privacidade e dos dados pessoais

Tal como acontece na segurança da informação, as medidas de carácter físico e lógico já referidas a esse propósito são igualmente aplicáveis à protecção da privacidade e dos dados pessoais.

Para além destas, são especialmente relevantes as medidas de carácter legislativo a seguir mencionadas.

Recorde-se a este propósito o já citado artigo 8º da Convenção Europeia dos Direitos do Homem, ratificada pela maioria dos Estados membros do Conselho da Europa, entre os quais Portugal, e que, consequentemente, constitui direito interno. Esta Convenção prevê que qualquer pessoa tem direito ao respeito da sua vida privada e da sua correspondência só podendo haver interferência se estiver em causa a segurança nacio-

31 Relatório da CNPD de 1996.

32 Dados da Policia Judiciária. Cf. jornal *O Público* de 24 de Agosto de 2006.

nal ou a defesa da ordem e a prevenção das infracções penais ou ainda a protecção dos direitos e liberdades de terceiros.

Também a Constituição da República Portuguesa prevê no art. 26º:

"1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de descriminação.

2. A lei estabelecerá garantias efectivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias."

Também o Código Penal nos seus artigos 192º e 193º se refere à devassa da vida privada e à devassa por meio de informática, respectivamente.

Como se referiu acima, a videovigilância é uma das técnicas que mais podem atingir o direito à privacidade. Por isso, o Decreto-Lei nº 35/2004, de 21 de Fevereiro, sobre a actividade de segurança privada, dispõe que a utilização da videovigilância para assegurar a protecção das pessoas e dos seus bens depende de autorização da Comissão Nacional de Protecção de Dados (CNPD) que julga, caso a caso, atendendo à finalidade face ao direito à privacidade. O seu artigo 13º sobre meios de vigilância electrónica, dispõe que a autorização destes meios deverá ter em atenção o regime de protecção de dados previsto na Lei nº 67/98, designadamente em matéria de direito de acesso, informação, oposição de titulares e regime sancionatório.

No particular aspecto das relações laborais, o Código de Trabalho, no seu art. 27º refere-se a dados biométricos e o art. 28º à utilização de meios de vigilância à distância, referindo que a sua utilização só é permitida se os dados utilizados forem necessários, adequados e proporcionais aos fins a atingir.

Em termos mais gerais, o Código de Trabalho prevê disposições em matéria de protecção da privacidade e dos dados pessoais (art. 16º) e na área do teletrabalho (art. 237º).

No que respeita ao uso do correio electrónico e ao acesso à Internet no local de trabalho, a CNPD considera que não se devem restringir a fins exclusivamente profissionais e afirma ainda que se afigura ilícito o acesso ou a divulgação dos conteúdos das mensagens recebidas ou dos sítios visitados, excepto para efeitos criminais e na sequência de despacho de autoridade judicial ou com o consentimento do próprio.[33]

33 Relatório de actividades da CNPD 2001/02.

A CNPD proibiu a videovigilância em infantários com a finalidade de permitir aos pais conhecer em cada momento o estado dos seus filhos e o que faziam, tendo considerado desproporcional esta finalidade face ao direito à privacidade das crianças e dos trabalhadores dos infantários que estariam permanentemente em observação.[34]

No que toca à utilização de câmaras de vídeo, fixas ou móveis, por forças e organismos de segurança, a Lei nº 1/2005, de 10 de Janeiro, permite-a apenas para protecção de edifícios, instalações públicas ou outras com interesse para a defesa nacional e para segurança das pessoas e bens públicos ou privados, bem como para a prevenção de crimes.

A utilização das câmaras em vias de comunicação terrestre é sujeita a autorização do Ministério da Administração Interna, sob condição de que o parecer prévio da CNPD não seja negativo. Esta lei prevê ainda que a utilização da videovigilância seja regida pelo principio da proporcionalidade, ou seja, a sua utilização tem que mostrar-se adequada à manutenção da segurança e ordem pública e à prevenção de crimes, no pressuposto da existência de riscos objectivos e de que é respeitada a intimidade das pessoas.

Pelo que respeita particularmente à protecção dos dados pessoais, salienta-se que a Constituição da República Portuguesa foi mesmo a primeira, de entre as dos países europeus, a tratar este problema no seu artigo 35º.

A Convenção 108 do Conselho da Europa constituiu o primeiro instrumento internacional vinculativo nesta matéria. Posteriormente, foi aprovado um protocolo adicional que prevê a necessidade de uma Autoridade de Controlo Independente em cada Estado membro para garantia do cumprimento dos princípios de protecção de dados, bem como define as condições em que podem ser efectuadas transferências de dados pessoais entre Estados.

O Conselho da Europa, ainda na sequência da Convenção 108, aprovou várias recomendações sectoriais, designadamente sobre protecção de dados nos sectores de investigação científica e estatísticas, bancos de dados médicos, segurança social, sector polícia e emprego, que detalham medidas a ter em conta em cada um destes domínios.

Como já foi referido, o Conselho e o Parlamento da União Europeia aprovaram directivas em matéria de protecção de dados – a Directiva 95/46/CE do Parlamento

34 8º Relatório do Grupo de Trabalho Artigo 29, Comissão Europeia

Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

No sector da protecção de dados na área das telecomunicações foi aprovada a Directiva 2002/58/CE, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas para alargar o seu âmbito a todas as comunicações electrónicas, incluindo a Internet.

O Conselho e o Parlamento da União Europeia consideraram que os princípios da protecção de dados deveriam ser também respeitados no âmbito das próprias instituições da União Europeia, em consequência do que aprovaram o Regulamento (CE) nº 45/2001 do Parlamento e do Conselho, de 18 de Dezembro de 2000.

A primeira lei portuguesa de protecção de dados foi a Lei nº 10/91, de 29 de Abril, que dizia respeito apenas a dados pessoais informatizados; veio a ser alterada pela Lei nº 28/94, de 29 de Agosto, no sentido de reforçar a protecção dos dados pessoais, ambas entretanto substituídas pela Lei nº 67/98, de 26 de Outubro, relativa à protecção de dados pessoais.

Esta lei aplica-se ao tratamento,[35] automatizado ou não, de dados pessoais e abrange a videovigilância e ainda o tratamento de dados que tenham por objectivo a segurança pública, a defesa nacional e a segurança do Estado, excepto se existir legislação específica ou normas de direito internacional que vinculem Portugal.

São definidas as qualidades dos dados pessoais e as condições de legitimidade do tratamento, proibindo-se o tratamento de dados sensíveis como as convicções filosóficas ou políticas, a filiação partidária ou sindical, a religião, a vida privada, a origem racial ou étnica, a sexualidade, a saúde e ainda o tratamento de dados genéticos, com as excepções previstas na lei (artigos 5º e 6º).

A constituição de ficheiros relativos a pessoas suspeitas de actividades ilícitas, a infracções penais ou a medidas de segurança só pode ser efectuada por organismos cuja lei orgânica lhes dê essa competência. O tratamento de dados para efeitos de investigação policial deve restringir-se à prevenção de um perigo concreto ou à repressão de uma determinada infracção (artigo 8º).

35 O art. 3º define tratamento como quaisquer operações de recolha, registo, organização, conservação adaptação ou alteração, recuperação, consulta, utilização, comunicação por transmissão ou difusão ou ainda a comparação, interconexão, bloqueio, apagamento ou destruição de dados pessoais.

Por motivos de segurança do Estado e de prevenção ou investigação criminal é dispensado o direito de informação do seu titular, mediante disposição legal adequada ou deliberação da CNPD, sendo, em qualquer caso, o direito de acesso exercido através da CNPD. Se o conhecimento destes dados prejudicar os motivos invocados, a CNPD limita-se a informar os titulares dos dados das diligências efectuadas (artigos 10º e 11º). Assim, o acesso pelos titulares a dados policiais, só é possível com recurso à intermediação da CNPD. O mesmo acontece com o acesso aos dados constantes do Sistema de Informação de Schengen.[36]

A segurança do Estado, a segurança pública ou a prevenção, investigação e repressão de infracções penais são também os motivos invocados para que a CNPD possa autorizar a transferência de dados, se houver legislação específica ou constituir obrigação em convenção ou acordo internacional de que Portugal faça parte (art. 23º).

Por sua vez, a Lei de Acesso aos Documentos da Administração[37] acautela no art. 8º o direito de acesso a dados pessoais contidos em documentos administrativos, bem como no art. 9º a possibilidade da sua correcção. Os dados relativos a saúde só são comunicados ao interessado através de um médico por ele designado.

A Lei n.º 41/2004, de 18 de Agosto, transpõe a directiva nº 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas, assegurando a protecção dos dados pessoais e os interesses dos assinantes. Das medidas de protecção são excepcionados os procedimentos necessários para a protecção de actividades relacionadas com a segurança pública, a defesa, a segurança do Estado e a prevenção, investigação e repressão de infracções penais que sejam definidos em lei especial.

Com este diploma proíbe-se a escuta ou a intercepção de comunicações ou a vigilância de comunicações e ainda a utilização dos dados de tráfego[38] sem o consentimento dos utilizadores. Os dados de tráfego devem ser eliminados ou tornados anónimos quando deixam de ser necessários para a transmissão da comunicação, sendo que os tribunais podem obter informações sobre estes dados com vista à resolução de litígios no âmbito de processos.

---

36 É a Lei n.º 2/94, de 19 de Fevereiro, que estabelece os mecanismos de controlo e fiscalização do Sistema de Informação Schengen, tendo em vista preservar a segurança do Estado e a segurança pública, bem como a aplicação da Convenção nos territórios das partes.

37 Lei n.º 65/93, de 26 de Agosto, alterada pela Lei n.º 8/95 de 29 de Março.

38 A Lei nº 41/2004, de 18 de Agosto, define "dados de tráfego" como "quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónica ou para efeitos da facturação da mesma".

No âmbito comunitário, a directiva 2006/24/CE vem também definir condições específicas para que os dados das comunicações possam ser úteis no combate e prevenção do terrorismo e da criminalidade organizada.

A protecção dos dados pessoais é o objectivo principal da CNPD que tem difundido orientações específicas sobre determinadas matérias. O recurso a sistemas biométricos tem constituído uma das suas preocupações porquanto tem vindo, recentemente, a apresentar-se como um meio tecnológico que visa substituir ou reforçar a segurança dos meios tradicionais de controlo de entradas e saídas. Daí a aprovação e difusão de "Princípios sobre a utilização de dados biométricos no âmbito do controlo de acessos e de assiduidade".

Ainda no que toca às relações laborais, a CNPD aprovou os "Princípios sobre a privacidade no local de trabalho", abrangendo recomendações sobre o tratamento de dados em centrais telefónicas, o controlo do e-mail e do acesso à Internet.

O emprego da videovigilância tem sido também objecto de preocupação da CNPD nos "Princípios sobre o tratamento de dados por videovigilância", em que se recomenda, designadamente que os sistemas de videovigilância se apresentem como medida preventiva e de dissuasão para a prática de infracções penais, podendo servir de prova nos termos da lei processual, sendo o acesso às imagens restrito às entidades que delas precisem para as finalidades estipuladas.

4. Segurança da Informação *Versus* Protecção da Privacidade e dos Dados Pessoais

A segurança da informação é, como dissemos no início, pressuposto necessário da liberdade e da justiça: qualquer pessoa deve ter o direito de comunicar livremente, sem que as suas comunicações sejam interceptadas e muito menos censuradas, de ver garantido o seu direito à identidade pessoal, sem que os seus dados de identificação sejam furtados e utilizados indevidamente por terceiros. Deve, assim, ter a possibilidade de exercer os seus direitos de cidadania sem qualquer interferência indevida dos Estados, designadamente na vigilância e controlo dos seus comportamentos, particularmente no âmbito da sua vida privada, e ter a segurança de que os seus dados pessoais não são usados sem o seu consentimento, de forma ilícita.

No binómio *segurança da informação – privacidade e protecção dos dados pessoais,* parece suficientemente demonstrado que o primeiro elemento é fundamental para a consecução do segundo mas, em contrapartida, o segundo pode ser afectado significativamente pela

consecução do primeiro. Todas as recomendações internacionais e disposições legislativas nisso coincidem.

A liberdade de circulação da informação, de forma segura, é um bem essencial à preservação dos direitos fundamentais e consequentemente ao funcionamento regular da sociedade.

Não se atinge todavia esse objectivo sem regulação adequada: como disse já o Comissário Europeu para a Sociedade da Informação e Empresas "precisamos de um mínimo de regras e de regulação para que os benefícios da Sociedade da Informação cheguem a todos e para que se crie um quadro de protecção dos direitos dos cidadãos e das empresas, sem que isso condicione a inovação e provoque barreiras técnicas desnecessárias".

Por sua vez, como bem acentuou o Secretário-Geral da União Internacional de Telecomunicações, na Cimeira Mundial sobre Sociedade da Informação, "muitos foram os benefícios do desenvolvimento massivo da informação e das tecnologias da comunicação, especialmente ao nível dos postos de trabalho e de riqueza gerada. Mas esta transformação cria também preocupações legítimas, entre as quais, a garantia do acesso à informação e às tecnologias da informação, bem como a preservação dos direitos humanos e a liberdade, segurança e privacidade".

Vimos também que, a par do desenvolvimento das tecnologias da informação, proliferam assustadoramente técnicas de uso perverso da liberdade de comunicar para a consecução de acções criminosas que atingem não só os valores da protecção da privacidade e dos dados pessoais, como também os próprios valores fundamentais da vida humana, quando tais acções assumem o carácter de terrorismo.

A prevenção da criminalidade, e particularmente o combate a acções terroristas que atingem indiscriminadamente populações inocentes, acarretam a necessidade de se encontrar um equilíbrio entre o respeito devido ao valor fundamental da privacidade e da protecção dos dados pessoais e o direito igualmente essencial à vida em sociedade que é o da segurança pessoal e dos Estados por via da segurança da informação.

Deve assim ser encontrado um equilíbrio, na sequência do princípio da proporcionalidade, entre as medidas de segurança da informação que visem impedir as acções criminosas e as ameaças que, por aplicação dessas mesmas medidas, possam atingir a privacidade.

Como se sabe, os serviços de informações, bem como os serviços e forças de segurança, utilizam a escuta telefónica e a intercepção de mensagens para investigar, prevenir ou combater actividades ilícitas como o crime organizado ou o terrorismo.

Precisamente para evitar o conhecimento do conteúdo das mensagens, por via da sua intercepção, referimos o uso da criptografia. Mas esta pode, em contrapartida, ser utilizada pelos criminosos para evitar que as autoridades possam tomar conhecimento dos seus propósitos.

Onde se deve situar a fronteira? A utilização de sistemas criptográficos tem sido dificultada por países que querem manter a possibilidade de intercepção e compreensão das comunicações tendo em vista a prevenção e repressão de crimes e a defesa nacional. Esta atitude é contestada por Castells[39] quando diz que é "a ultima tentativa por parte dos governos para manter algum grau de controlo sobre os fluxos de informação" e que é "uma grande ironia histórica que a tentativa de controlar a informação proibindo a distribuição da capacidade de encriptação deixe os Estados – e a sociedade – indefesos perante os ataques efectuados a partir da periferia da rede".

A França, por exemplo, que tinha legislado no sentido de restringir a utilização de criptografia, anunciou em 1999 que os cidadãos poderiam utilizá-la sem restrições. A encriptação das mensagens que circulam no ciberespaço poderia de facto ser facilitada e até incentivada pelos governos se tal não viesse a revelar-se afinal como uma arma para utilização de terroristas e organizações criminosas, problema que entretanto tem vindo a ser resolvido através da utilização de programas de encriptação cuja estrutura é conhecida das autoridades competentes.

Mas não é só a criptografia que se revela como uma arma de dois gumes. As comunicações electrónicas são cada vez mais utilizadas pelos cidadãos na sua vida diária: vimos que também por essa via tanto se pode invadir a privacidade, ao interceptar as comunicações e assim obter informações pessoais, como pode essa intercepção ser indispensável para a prevenção, investigação, detecção de atentados terroristas ou de actos de criminalidade organizada.

É a necessidade de definir um enquadramento jurídico equilibrado que levou a União Europeia a adoptar a Directiva 2002/58/CE, relativa à privacidade e às comunicações electrónicas e, em seguimento dos atentados terroristas de Madrid, a preparar uma nova Directiva sobre a matéria (Directiva 2006/24/CE) que, restringindo embora alguns direitos no âmbito da protecção dos dados pessoais e da privacidade, vem criar melhores condições para se utilizarem os dados das comunicações no combate à criminalidade e ao terrorismo. Está, no entanto, sempre presente que tais restrições

39 Castells, Manuel, *A Galáxia Internet – Reflexões sobre Internet, Negócios e Sociedade,* Fundação Calouste Gulbenkian, 2004.

devem ser só as necessárias e adequadas para se atingirem as finalidades referidas com o respeito pelo princípio da proporcionalidade.

A União Europeia está bem consciente da existência de conflito crescente e duradouro entre as múltiplas tentativas dos governos em introduzir novos instrumentos de luta contra o terrorismo, sem prejuízo de ser considerada a necessidade de defender os princípios de protecção de dados, como elemento essencial da liberdade e da democracia[40] e, em consequência dos recentes actos de terrorismo, têm vindo a ser dada primazia à segurança e a aceitar novas medidas de controlo, designadamente introduzindo e ampliando as normas relativas à conservação de dados de tráfego nas comunicações electrónicas, incluindo-se nestas as comunicações pela Internet.

A segurança da informação é, de facto, uma forma de proteger os cidadãos desde que seja conseguido o necessário equilíbrio entre os valores em presença. Assim, por exemplo, está decidida a inserção de elementos biométricos em documentos de identificação e a utilização da videovigilância com regulamentação adequada.

No seguimento desse movimento regulador de equilíbrios, o novo passaporte português (PEP) contém um *chip* com dados biográficos e biométricos do titular contendo 32 dados informativos visando a máxima segurança e a inviabilidade de falsificações.

Como se viu, tanto instrumentos internacionais e comunitários, como a legislação portuguesa, têm revelado preocupação pelo respeito dos princípios de protecção da vida privada e dos dados pessoais mas, cada vez mais, em resultado das crescentes actividades terroristas, com restrições suplementares que derivam da necessidade de, numa sociedade democrática, privilegiar a protecção da segurança do Estado, da defesa, da segurança pública, da prevenção, investigação e repressão das infracções penais e de interesses económicos e financeiros importantes do Estado.

Na sequência do atentado terrorista do 11 de Setembro em Nova Iorque, o Conselho da União Europeia estabeleceu um acordo com o governo dos EUA para lhe permitir o acesso aos dados recolhidos juntos dos viajantes das transportadoras aéreas (PNR). O Parlamento Europeu considerou este acordo ilegal porque a directiva de protecção de dados, instrumento invocado, não se aplica a questões de defesa do Estado e segurança. O Grupo do Artigo 29[041] acompanhou o Parlamento Europeu, dando um

40 8º Relatório anual do Grupo de Trabalho do Artigo 29ª, Comissão Europeia.

41 Grupo consultivo previsto no art. 29.º da Directiva n.º 95/46/CE, composto por representantes das autoridades nacionais de protecção de dados, que funciona junto da Comissão Europeia.

parecer negativo ao fornecimento deste tipo de dados que considerou desproporcionado.[42] O Tribunal de Justiça veio a confirmar este entendimento.

5. Conclusões

1.º – A informação tem uma relevante importância para o desenvolvimento e manutenção de uma sociedade livre e democrática. A afirmação da liberdade de informar e de ser informado está bem acentuada nos n.os 1 e 2 do art. 37.º da Constituição da República, ao afirmar que todos têm o direito de exprimir e divulgar livremente o seu pensamento pela palavra, pela imagem ou por qualquer outro meio, bem como o direito de informar, de se informar e de ser informados, sem impedimentos nem discriminações, e que o exercício destes direitos não pode ser impedido ou limitado por qualquer tipo ou forma de censura.

2.º – Para que a liberdade de informação se possa exprimir, sem peias, censuras ou intromissões indevidas, é indispensável que os sistemas de informação possam reunir as características necessárias a garantir a *segurança da informação*, isto é, Confidencialidade, Integridade, e Disponibilidade da informação.

3.º – Cedo a segurança da informação foi posta em causa por acções criminosas que vão desde o acesso indevido à informação, quebrando a característica da confidencialidade, até à alteração do seu conteúdo, pondo em cheque a sua integridade: assim, tem sido possível o uso indevido de dados pessoais, o roubo de identidades, a burla e a falsidade informáticas, a espionagem industrial e a própria sabotagem, tudo para causar prejuízo ou obter benefícios económicos ou de outra natureza, designadamente na intercepção de segredos militares pondo em causa a segurança nacional.

A encriptação de mensagens, como forma de assegurar a confidencialidade e a integridade das mensagens transmitidas, foi um remédio encontrado, embora inicialmente os Estados tenham reservado o uso da criptografia apenas para mensagens militares por receio de ela ser utilizada para a transmissão de mensagens entre criminosos com o objectivo de preparação em segredo e ocultação da autoria das suas actividades delituosas: entretanto a pressão generalizada no sentido de garantir a segurança da

42 Grupo do Artigo 29º, Opinion 4/2003 – Transfer of Passengers' Data.

informação nas actividades civis levaram a que fossem levantadas as dificuldades para uso corrente da criptografia e das assinaturas electrónicas, com a reserva todavia de os programas de encriptação serem conhecidos das autoridades competentes para eficaz combate ao seu uso pela criminalidade organizada.

4.º – Por sua vez, o direito à privacidade e à protecção dos dados pessoais são valores reconhecidos em todo o mundo civilizado e objecto de múltiplas recomendações e instrumentos jurídicos internacionais e comunitários. A Constituição da República Portuguesa foi pioneira na defesa de tais valores, como está bem reflectido no artigo 26.º, quanto à defesa da privacidade, e no art. 35.º, quanto à protecção dos dados pessoais.

Assim, dispõe o n.º 1 do art. 26.º que a todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação.

Por seu lado, o art. 35.º consagra os princípios fundamentais da protecção de dados pessoais, prevendo especialmente que todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei e proibindo o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.

5.º – Para salvaguarda da privacidade e da protecção de dados pessoais, a segurança da informação é um valor indispensável. E nesse sentido, no seguimento aliás de tratados internacionais, como a Convenção 108 do Conselho da Europa, e de instrumentos jurídicos comunitários, designadamente a citada directiva 95/46/CE, a Lei n.º 67/98, de 26 de Outubro, determina, no seu art. 14.º, que o responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito.

Para protecção de dados pessoais de maior sensibilidade, o art. 15.º exige medidas de segurança mais severas, bem como o controlo da inserção, utilização, acesso e transmissão desses dados. Determina ainda que os sistemas de tratamento da informação garantam a separação lógica entre os dados referentes à saúde e à vida sexual, incluindo os genéticos, dos restantes dados pessoais.

6.º – Esta estrutura de protecção da privacidade e dos dados pessoais foi todavia posta em causa, sobretudo após os ataques terroristas do 11 de Setembro em Nova Iorque, seguidos de ataques similares em Madrid e Londres. Estes atentados, bem como outras acções reveladoras da existência de criminalidade organizada e violenta, revelaram a necessidade imperiosa de conciliar a segurança da informação com a salvaguarda da intimidade da vida privada e dos dados pessoais.

O combate ao terrorismo e às demais acções de criminalidade organizada exigem que seja possível às autoridades competentes, em casos especificamente previstos na lei, pôr em causa, não só a segurança da informação como a privacidade, particularmente através da intercepção de qualquer forma de comunicação e da vigilância, por meios electrónicos e consequentemente à revelia e no desconhecimento dos vigiados, de comportamentos e de actividades suspeitos.

Há assim um difícil equilíbrio a definir, por um lado, entre a utilização de meios destinados a garantir a segurança dos Estados e das populações e, por outro, a salvaguarda dos valores fundamentais do respeito pela liberdade de informação, pela privacidade e pela protecção dos dados pessoas: é o respeito escrupuloso pelo princípio da proporcionalidade que poderá ser a chave do problema.

7.º – Há um longo caminho a percorrer pelos Estados e pelas suas organizações para, em conjugação, poderem consciencializar, por um lado, as autoridades que orientam o combate ou combatem o terrorismo e a criminalidade organizada para a necessidade de, no desenvolvimento das suas actividades, obedecerem ao princípio da proporcionalidade e consequentemente terem presente a necessidade de salvaguarda de direitos fundamentais; e, por outro lado, os cidadãos em geral, quer da extensão dos seus direitos fundamentais, designadamente no domínio da privacidade, quer para a cautela a ter na utilização e divulgação dos dados pessoais, quer ainda para a compreensão a ter para que, em certas circunstâncias e para sua própria protecção, tenha de haver restrições ao exercício daqueles direitos fundamentais.

É esta uma tarefa de grande fôlego que pode ser levada a cabo através de acções massivas de divulgação, junto das populações e pelos meios adequados da comunicação social, dos seus direitos fundamentais e da eventual necessidade de restrições, e junto das autoridades competentes – políticas, militares, judiciárias e de polícia –, através de acções selectivamente dirigidas, dos direitos fundamentais dos cidadãos e da consideração que deve ser conferida ao princípio da proporcionalidade.