II. DOUTRINA INTERNACIONAL

II.1. GLOBALIZAÇÃO, CIRCULAÇÃO DE PESSOAS E BENS E PRIVACIDADE[38]

CATARINA SARMENTO E CASTRO

SUMÁRIO. I. INTRODUÇÃO. II. INFORMAÇÃO E INFORMAÇÃO PESSOAL. II.1. INFORMAÇÃO E INFORMAÇÃO PESSOAL. III. OS LIMITES GERAIS À UTILIZAÇÃO DA INFORMAÇÃO PESSOAL. IV. ALGUNS EXEMPLOS – A IDENTIFICAÇÃO POR RADIOFREQUÊNCIA (IDRF); OS DADOS BIOMÉTRICOS DOS TRABALHADORES; A VIDEOVIGILÂNCIA, AS MENSAGENS DE CORREIO NÃO SOLICITADO (SPAM); OS FLUXOS DE DADOS PARA OUTROS PAÍSES. IV. 1. A IDENTIFICAÇÃO POR RADIOFREQUÊNCIA (IDRF) – A MICRO VIGILÂNCIA. IV. 2. OS DADOS BIOMÉTRICOS DOS TRABALHADORES. IV.3. A VIDEOVIGILÂNCIA. IV.4. BREVE NOTA SOBRE A TRANSFERÊNCIA DE DADOS PESSOAIS PARA OUTROS PAÍSES. IV.5. SPAM OU *JUNK MAIL*– AS COMUNICAÇÕES ELECTRÓNICAS NÃO SOLICITADAS. V. CONCLUSÕES. REFERÊNCIAS BIBILOGRÁFICAS.

RESUMO

A globalização da economia impulsiona a circulação de pessoas e bens, assim como a troca de informações. Dados sobre produtos, sobre trabalhadores, e sobre consumidores estão em constante movimento. As novas tecnologias tornaram possível seguir o rasto de um produto no qual haja sido colocado um *microchip*; localizar uma frota de camiões; ou que um empregador possa aceder aos dados dos seus trabalhadores do outro lado do Oceano. Através do presente trabalho pretende-se estudar estas e outras implicações das novas tecnologias e da globalização na privacidade de cada um de nós, e o que cabe às empresas a operar no espaço europeu, designadamente em Portugal, fazer para respeitar as regras europeias e portuguesas de protecção de dados pessoais.

Palavras-chave: privacidade; protecção de dados pessoais; globalização.

---

[38] NOTA: O presente texto «Globalização, circulação de pessoas e bens e privacidade» corresponde, com pequenas alterações, à 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.

ABSTRACT

Economic globalization increases the movement of people and goods, and information share. Data on products, workers and consumers are permanently on the move. New technologies have allowed the tracking of a product with microchip sensors; have allowed to know the whereabouts of a truck fleet; have allowed an employer to have access to its employee's personal data across the Sea. Through the present work we intend to study these and some other implications of new technologies and globalization on everyone's privacy, and what should private companies working on European ground, namely in Portugal, do, to comply with European and Portuguese national rules on data protection.
Word-key: privacy, data protection; globalization.

I. INTRODUÇÃO

A globalização da economia e dos mercados pressupõe e impulsiona a circulação de pessoas e bens, assim como a troca de informações, no espaço europeu, e fora dele. Circulam, nomeadamente, informações sobre produtos, sobre trabalhadores, e sobre consumidores.

As novas tecnologias permitiram, por exemplo, acelerar a busca, mas também a troca de informações, diversificar e aumentar a quantidade de informações armazenadas. Elas tornaram possível, designadamente, seguir o rasto de um produto no qual haja sido colocado um *microchip*, localizar uma frota de camiões de distribuição, ou que um empregador possa aceder aos dados dos seus trabalhadores em qualquer ponto do país ou em qualquer continente.

Que implicações tiveram o avanço das novas tecnologias e a globalização na privacidade de cada um de nós? O que cabe a cada empresa fazer para respeitar as regras europeias e portuguesas de protecção de dados pessoais? Estas são algumas das questões que nos propomos abordar neste texto.

II.1. INFORMAÇÃO E INFORMAÇÃO PESSOAL

Indiscutivelmente, ter informação é ter poder. Este lugar comum, que poderia ser aplicado em áreas tão diversas como, a título meramente exemplificativo, a da política, da

governação, da justiça ou até do desporto, também faz sentido quando utilizado no universo da gestão das empresas. Quem detém informação e, nomeadamente, informação pessoal, pode com maior segurança tomar opções estratégicas e adoptar soluções de planeamento. Consequentemente, a informação é um bem cobiçado, o que fez com que o legislador europeu procurasse regulamentar a sua utilização, designadamente no caso das informações respeitantes a pessoas.

Os pioneiros na defesa da privacidade como um bem digno da protecção do direito foram dois advogados norte-americanos de *Boston – Warren* e *Brandeis* – que escreveram um artigo jurídico, na *Harvard Law Review*, em 1890, sustentando a existência de um «right to be let alone», um direito a «ser deixado em paz»[39]. Na verdade, *Warren* estava, segundo alguns estudiosos, particularmente cansado da constante curiosidade da imprensa em torno da vida social da sua família, das suas festas, em geral, e do casamento da sua filha em especial.

Desde o escrito de *Warren* e *Brandeis,* a privacidade foi sendo progressivamente reconhecida e protegida enquanto direito fundamental[40].

No final do Século XIX, início do Século XX, a privacidade era fundamentalmente ameaçada pelo crescimento da imprensa escrita, associada à imagem fotográfica, mas o nascimento, a 14 de Fevereiro de 1946, do *Electronic Numerical Integrator and Computer* (ENIAC) – computador que pesava 30 toneladas, tinha 33 metros de comprimento e 3,3

---

[39] WARREN, Samuel/BRANDEIS, Louis. *The right to privacy*. **Harvard Law Review**, Vol. IV, n.º 5, 15 Dezembro 1890.

[40] Referências no direito português sobre o direito à privacidade em geral, ou sobre o direito à autodeterminação informativa, em especial, podem ser encontradas, por exemplo em: ASCENSÃO, José de Oliveira. *Estudos sobre Direito da Internet e da Sociedade da Informação*. Coimbra: Almedina, 2001; CARVALHO, Orlando de. *Teoria Geral do Direito Civil.* Coimbra: Centelha, 1981, p. 89 ss.; *Idem*. *Teoria Geral da Relação Jurídica. Sumários*. Coimbra: 1970, p. 36 ss.; *Idem*. *Direitos de Personalidade* (Apontamentos de aulas), Polic., Coimbra, p. 2 e 3.; *Idem*. *Para uma teoria da pessoa humana (reflexões para uma desmistificação necessária)*. **O homem e o tempo – Liber amicorum para Miguel Baptista Pereira**. Porto: Fundação Eng. António de Almeida, 1999, p. 527 ss.; *Idem*. *Os Direitos do Homem no Direito civil Português*. Coimbra: Vértice*,* 1973, p. 29; CASTRO, Catarina Sarmento. *Privacidade, informática e dados pessoais*. Coimbra: Coimbra Editora, 2004; MARQUES, Garcia/MARTINS, Lourenço. *Direito da Informática*. Coimbra: Almedina, 2000; PINTO, Carlos Alberto da Mota. *Teoria Geral do Direito Civil*. 3.ª Edição, Coimbra: Coimbra Editora, 1989, p. 207 ss.; PINTO, Paulo da Mota, *A limitação voluntária do direito à reserva sobre a intimidade da vida privada*. **Estudos em Homenagem a Cunha Rodrigues**. Vol. II, Coimbra: Coimbra Editora, 2001, p. 527 ss.; *Idem*. *O direito ao livre desenvolvimento da personalidade*. **Portugal-Brasil Ano 2000**. Coimbra: Coimbra Editora, 1999, p. 149 ss; *Idem*. *A protecção da vida privada e a Constituição*. **Boletim da Faculdade de Direito da Universidade de Coimbra**. Coimbra: Vol. LXXVI, 2000, p. 153 ss.; SOUSA, Rabindranath Capelo de. *O direito geral de personalidade*. Coimbra: Coimbra Editora, 1995, p. 320 ss..

metros de altura – tudo mudou. Há mesmo quem, no limite, sustente que foi a informática a verdadeira responsável pela necessidade de se delimitar de uma esfera da vida privada[41].

De facto, os novos tempos de poderosas tecnologias informáticas - em que os descendentes do ENIAC se multiplicaram e vulgarizaram, se tornaram *user-friendly* e hoje em sofisticadas versões cabem no bolso de um casaco - ditariam que se viesse a autonomizar a protecção do que se veio a chamar, por influência alemã, «direito à autodeterminação informativa»[42].

Este deve ser entendido como o direito do indivíduo à protecção contra a utilização dos seus dados pessoais, bem como o direito de cada um determinar por si a utilização e divulgação dos dados que lhe respeitam[43].

O direito à autodeterminação informativa é um direito dirigido à defesa de novas facetas da personalidade, agora ainda mais expostas em consequência da vulgarização da informática. Esta moderna ameaça à privacidade - e contudo de inegável utilidade para a economia e para a qualidade de vida do cidadão em geral - permite a utilização das informações pessoais em operações cada vez mais céleres, em interconexões e associações cada vez mais complexas, podendo as informações ser objecto de pesquisa cada vez mais rápida, sendo tudo isto associado a uma cada vez maior capacidade de armazenamento de informação, e a uma utilização por cada vez mais numerosos titulares dos meios de controlo.

Por isso, este direito deixou de ser apenas um direito de reserva face a grandes bases de dados estatais, na sua maioria estáticas, para passar a ser também a um direito de reserva perante os diversos utilizadores de mecanismos de tratamento de informação, que hoje são também privados como cada um de nós, e que acedem a informação em constante movimento.

Este direito, consagrado como parte de um mais amplo direito à privacidade em diversos instrumentos de Direito Europeu e Internacional[44], e pioneiramente protegido no

---

[41] GALLOUEDEC-GENUYS F.. *La vie privée: une création informatique*. **Les enjeux culturels de l'informatisation**, F. Gallouedec-Genuys (dir.) et P. Lemoine (dir.), La Documentation Française, Paris, 1980.

[42] É a jurisprudência alemã que emite a primeira decisão fazendo expressa referência a este *Recht auf informationelle Selbstbstimmung*. Foi a decisão do Tribunal Constitucional (*Bundesverfassungsgerichts*) de 15 de Dezembro de 1983 (*BVerfGE* 65).

[43] Para maiores desenvolvimentos pode consultar-se o nosso: *Informática, privacidade e protecção de dados pessoais*. Coimbra: Almedina, 2004.

texto da Constituição Portuguesa como um específico «direito à autodeterminação informativa» - a Constituição Portuguesa, logo em 1976, consagrou este direito referido aos «registos mecanográficos», sendo depois seguida por outros textos constitucionais europeus e não europeus[45] – veio em Portugal a receber concretização legal, sendo actualmente protegido pela Lei da Protecção de Dados Pessoais, de 1998, que transpôs a Directiva Europeia na matéria (95/46/CE).

A Directiva Europeia relativa à protecção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (95/46/CE, de 24 de Outubro) pretendeu impulsionar a circulação de informações procurando conciliar este direito com o direito de cada um sobre a sua própria informação. A sua transposição, obrigatória, harmonizou a legislação dos Estados-membros da União Europeia assim conferindo um nível de protecção comum a todos eles, permitindo que a circulação das informações pessoais se faça dentro do espaço Europeu sem especiais constrangimentos.

O tratamento da informação a que de forma breve daremos a nossa atenção é o que se refere a informações *pessoais*, isto é, como refere a lei, a informações de qualquer natureza e

---

[44] Veja-se, por exemplo, o art. 12.º da *Declaração Universal dos Direitos do Homem*: «Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei», e em texto semelhante o art. 17.º do *Pacto Internacional relativo aos direitos civis e políticos*; também o art. 8.º da *Convenção Europeia dos Direitos do Homem* (Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais) impõe, igualmente, que «qualquer pessoa tem o direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência». Outros instrumentos protegem directamente o direito à autodeterminação informativa: é o caso da *Convenção 108 do Conselho da Europa* (Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal), que é um dos instrumentos fundamentais de protecção de dados pessoais, e do art. 8.º da *Carta dos Direitos Fundamentais da União Europeia*, relativo à protecção de dados pessoais, no qual se estabelece «Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito».

[45] O tratamento deste direito noutras Constituições Europeias e nas Constituições dos países Ibero-americanos pode ser encontrada no texto que apresentámos na VIII Congresso Ibero-Americano de Direito Constitucional, realizado em Sevilha, em 2003, *O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança no pós 11 de Setembro*, **Estudos de Homenagem ao Conselheiro José Manuel Cardoso da Costa**. Vol. II, Coimbra: Coimbra Editora, 2005. p. 65 e ss. Em especial sobre o art. 35.º da Constituição Portuguesa veja-se, por todos: CANOTILHO, José Joaquim Gomes/MOREIRA, Vital. *Constituição da República Portuguesa Anotada*. Coimbra: Coimbra Editora, 3. ª Edição, 1993, p. 214 ss.; MARQUES, A. Garcia. *Legislar sobre protecção de dados pessoais em Portugal (do art. 35.º da Constituição, à Lei n.º 10/91, de 29 de Abril*. **Legislação**, n.º 8, p. 37 ss..

independentemente do seu suporte, relativas a pessoas *singulares*, identificadas ou identificáveis[46].

São exemplos de informações pessoais, de acordo com esta definição estabelecida na Directiva Europeia e, na sua sequência, na Lei da Protecção de Dados Pessoais portuguesa, os dados tratados pelas empresas relativos aos seus trabalhadores, como, naturalmente, o nome e outros dados de identificação, dados relativos à actividade profissional, a assiduidade, os dados de saúde tratados pelos serviços de segurança, higiene e saúde e no trabalho, a sua impressão digital utilizada para controlo de assiduidade, mas também os dados de clientes destas empresas que sejam pessoas singulares, como os produtos encomendados, a forma de pagamento, ou os dados sobre perfis de consumidores quando estes sejam identificáveis, os respectivos contactos, *etc*., *etc*.

O regime garantístico estabelecido no diploma geral da protecção de dados pessoais em Portugal não contempla as informações que respeitem a pessoas colectivas, mas apenas as respeitantes a pessoas singulares, muito embora a Directiva não o vedasse e tenha sido outra a opção de alguns Estados-membros da União Europeia. Já no âmbito das comunicações electrónicas, a protecção estende-se às pessoas colectivas: assim, por exemplo, a recente Directiva Europeia 2006/24/CE - que terá de merecer transposição na legislação de cada um dos Estados-membros - referente à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações, e que procedeu à alteração da Directiva Europeia 2002/58/CE, prevê expressamente a sua aplicação aos dados de tráfego e localização relativos a pessoas singulares ou colectivas. Note-se, ainda, que a Comissão Nacional de Protecção de Dados – autoridade administrativa independente que em Portugal zela pelo respeito da legislação da matéria - tem considerado que as informações respeitantes a empresários em nome individual, ainda que ligadas à sua actividade profissional, estão abrangidas pelo regime da protecção de dados pessoais.

Por outro lado, na doutrina portuguesa há quem venha defendendo, designadamente à luz do disposto no n.º 2 do art. 12.º da Constituição da República Portuguesa, que consagra uma das vertentes do princípio da universalidade estabelecendo que "as pessoas colectivas

---

[46] Escrevemos mais desenvolvidamente sobre o regime de protecção de dados pessoais no nosso: *Informática, privacidade e protecção de dados pessoais*. Coimbra: Almedina, 2004.

gozam dos direitos e estão sujeitas aos deveres compatíveis com a sua natureza", que permite às pessoas colectivas a atribuição de direitos compatíveis com a sua natureza, o que seria o caso do direito à autodeterminação informativa.

Apesar de não ser esse o objectivo desta exposição, parece importante lembrar ainda que o *uso de informações não pessoais* (por exemplo dados relativos a empresas), embora fora das limitações impostas para o uso de informações pessoais, não pode, ainda assim, considerar-se totalmente livre. Basta pensarmos nas regras jurídicas que proíbem a utilização e divulgação, nomeadamente por parte da Administração Pública, de informações que possam respeitar a segredos comerciais ou industriais. Exemplo disso mesmo encontramos, nomeadamente, na legislação portuguesa que regula os poderes da Autoridade Nacional da Concorrência[47].

Na Lei portuguesa não são abrangidas pelo especial regime de protecção as informações tratadas por pessoas singulares no exercício de actividades exclusivamente pessoais ou domésticas.

Por ter sido alvo de importante decisão jurisprudencial merece aqui especial destaque a exclusão da protecção relativamente à informação tratada apenas para fins pessoais e domésticos. O Supremo Tribunal Administrativo português, em Acórdão de 5 de Junho de 1997, entendeu que o controlo temporal das entradas e saídas dos trabalhadores, incluindo o controlo dos acessos às casas de banho, efectuado pela entidade empregadora mediante o uso de um cartão magnético, para efeitos de processamento de remunerações mas também disciplinares, não poderia considerar-se um «uso pessoal e doméstico» da informação, pois na prática isso esvaziaria a sujeição das empresas às regras da protecção de dados pessoais. Noutro Acórdão o mesmo Tribunal concretizou que «com a expressão "uso pessoal e doméstico" pretendeu o legislador significar a não aplicação da legislação da protecção de dados aos ficheiros de dados pessoais que, pela sua própria natureza se destinem "a uso por pessoa individual ou no âmbito do domicílio familiar (no sentido restrito ao domicílio familiar"»[48]. Na sequência desta decisão, a actual Lei da Protecção de Dados portuguesa,

---

[47] A Lei n.º 10/2003, de 18 de Janeiro, aprovou a Lei de Organização e Funcionamento; a Lei n.º 18/2003, de 11 de Junho, aprovou a Lei da concorrência.

[48] Acórdão de 19 de Junho. Ambos os Acórdãos foram decididos à luz do disposto naquela que era então a Lei da Protecção de Dados – a Lei n.º 10/91, que na *alínea a)* do n.º 2 do art. 3.º, exceptuava da aplicação do regime nela previsto os tratamentos que tivessem por objecto exclusivo informações destinadas ao uso pessoal e doméstico.

aprovada em 1998, veio reforçar a ideia de que este uso «pessoal e doméstico» se refere apenas a tratamentos realizados por pessoas singulares (art.4.º).

Exemplo de informação não pessoal será a que é fornecida pelo *microchip* emissor de sinais de radiofrequência, quando este esteja apenas associado a um produto para seguir o seu rasto dentro de um armazém, ou entre armazéns, não lhe sendo associado qualquer cliente individual. Todavia, se esse *microchip* permitir associar ao produto, por exemplo, um consumidor final que utilizou o seu cartão de cliente para o adquirir, tornar-se-á informação pessoal, sujeita às regras gerais.

III. OS LIMITES GERAIS À UTILIZAÇÃO DA INFORMAÇÃO PESSOAL

A utilização de informações pessoais – isto é, o tratamento dos dados pessoais, como a recolha, registo, organização, conservação, adaptação, alteração, consulta, comunicação, bloqueio, apagamento, *etc* – está em Portugal sujeita a limites globalmente definidos na Lei da Protecção de Dados Pessoais (a Lei n.º 67/98, de 26 de Outubro), que transpôs a correspondente Directiva Europeia.

O regime legal português é caracterizado pela inexistência de prerrogativas especiais quanto à utilização da informação por parte das entidades públicas: na verdade, Administração Pública e privados estão sujeitos às mesmas regras de protecção de dados pessoais, devendo respeitar os mesmos princípios de tratamento, ficando sujeitos às mesmas obrigações, e devendo igual respeito aos direitos dos titulares dos dados pessoais.

A Legislação da protecção de dados consagra alguns direitos do titular dos dados, a que correspondem deveres do responsável pelos tratamentos:

- O Direito à curiosidade (saber se o responsável tem dados)
- O Direito de informação (saber o que tem) – art. 10.º
- O Direito de acesso (comunicação das informações para conhecê-las) – art. 11.º
- O Direito ao esquecimento (prazo) – art. 5.º, 1, *e)*
- O Direito de rectificação e actualização – art. 5.º, 1, *d)*
- O Direito de oposição – art. 12.º
- O Direito a não ficar sujeito a decisão individual automatizada – 13.º

- O Direito ao não tratamento de dados sensíveis – 35.º CRP
- O Direito ao apagamento ou bloqueio dos dados – art. 11.º, 1, *d)*

Uma das entidades com papel mais relevante nesta matéria é a já mencionada Comissão Nacional de Protecção de Dados (CNPD), perante a qual todo e qualquer recolha e tratamento de dados pessoais realizado em Portugal deve ser notificado (a Lei prevê excepções), para que esta sobre ele se pronuncie.

Esta autoridade administrativa independente tem *poderes de inspecção* tão amplos que lhe permite verificar a utilização indevida de dados pessoais nos computadores de qualquer instituição ou empresa, até naquelas em que o segredo se impõe de maneira mais acentuada, como um banco, ou a Polícia Judiciária.

Pode também aplicar *sanções administrativas* pelo incumprimento das normas jurídicas de protecção de dados pessoais. As coimas variam um mínimo de 249,40 € e um máximo de 2493,99 €, no caso de violação cometida por pessoas singulares, e entre 1 496,39 € e 14 963,94 €, tratando-se de infracção cometida por pessoa colectivas.

É aos tribunais judiciais que cabe a aplicação de ***sanções penais*** pela violação das normas de protecção de dados pessoais, punindo com pena de prisão ou multa, seja por incumprimento dos deveres perante a CNPD, ou violação de sigilo profissional de quem trabalhe com dados pessoais, ou acesso indevido a dados pessoais – por exemplo, violando regras técnicas de segurança (até um ou até 2 anos de prisão ou multa até 120 ou 240 dias).

No caso português, a ausência de notificação à CNPD do tratamento de dados pessoais – como o uso de câmaras de videovigilância, uso de aparelhos biométricos de controlo de entradas e saídas, constituição de ficheiros com dados relativos aos trabalhadores de uma empresa, ou aos seus clientes que seja pessoas singulares (ainda que a maioria do ficheiro pudesse, por exemplo, conter informações sobre pessoas colectivas) - é um dos fundamentos de aplicação de coimas por parte da CNPD. Apesar da nalguns casos ter tido lugar a impugnação judicial da coima aplicada pela Comissão, a jurisprudência tem vindo em larguíssima medida a dar razão à CNPD[49].

Embora sendo ainda fraca a tradição dos tribunais portugueses na aplicação da legislação em matéria de protecção de dados pessoais, estes já algumas vezes decidiram ser

---

[49] Exemplos vários podem ser encontrados em: <http://www.cnpd.pt/bin/legis/juris/jurisprudencia.htm>, acedida em Maio de 2006.

nula a prova obtida com base em tratamentos de dados não legalizados (o que inclui nos tratamentos de videovigilância, as imagens captadas) ou em acessos ilegítimos a dados pessoais (por exemplo, o Tribunal Constitucional decidiu que um operador não pode fornecer a um tribunal, no âmbito de um processo laboral, os dados de comunicação do trabalhador respeitantes a sua casa[50]).

IV. ALGUNS EXEMPLOS – A IDENTIFICAÇÃO POR RADIOFREQUÊNCIA (IDRF); OS DADOS BIOMÉTRICOS DOS TRABALHADORES; A VIDEOVIGILÂNCIA, AS MENSAGENS DE CORREIO NÃO SOLICITADO (SPAM); OS FLUXOS DE DADOS PARA OUTROS PAÍSES

IV. 1. A IDENTIFICAÇÃO POR RADIOFREQUÊNCIA (IDRF) – A MICRO VIGILÂNCIA

A identificação por radiofrequência é uma técnica em expansão em que se faz uso de um *microchip* colocado, por exemplo, num bem de consumo, que mediante a micro-antena que tem incorporada transmite as informações, por exemplo de identificação ou localização, nele armazenadas a um leitor. O identificador único associado ao *microchip* permite ao leitor reconhecer aquele objecto, distinguindo-o de outro. Na maioria dos casos este *microchip* está pensado para funcionar sem necessitar de qualquer fonte de energia.

A solução técnica de recurso à radiofrequência é hoje correntemente utilizada em vários países, incluindo Portugal, para funcionalidades tão básicas como a do reconhecimento dos passes dos transportes públicos em algumas cidades, em mecanismos de controlo de tempo e de percurso de atletas em maratonas, em aparelhos de reconhecimento em portagens e parques de estacionamento, em postos de abastecimento de combustíveis, em pulseiras electrónicas utilizadas em situações de prisão domiciliária. Outras aplicações que são anunciadas consistem em permitir a imediata identificação de um doente crónico que fique inconsciente e de lhe associar de modo célere a sua ficha clínica, ou de evitar a troca ou rapto

---

[50] Acórdão n.º 241/2002: o Tribunal Constitucional julgou inconstitucional o art. 51.º, n.º 3, *alínea b)*, do CPC, quando interpretado «no sentido de que, em processo laboral, podem ser pedidas, por despacho judicial, aos operadores de telecomunicações informações relativas aos dados de tráfego e à facturação detalhada de linha telefónica instalada na morada de uma parte, sem que enferme de nulidade a prova obtida com utilização dos documentos que veiculam aquelas informações, por infracção ao disposto no artigo 26º nº 1 e 34º. nºs 1 e 4 da Constituição».

de bebés nas maternidades. Num futuro próximo, os passaportes e documentos de identificação serão dotados deste tipo de mecanismo.

Conhece-se também a existência de aplicações que actualmente fazem uso de *microchips* emissores de radiofrequência do tamanho de um grão de arroz sob a pele humana[51].

Com o tempo, de mecanismo pensado para seguir o rasto de bens, a identificação por radiofrequência passou a servir para seguir pessoas, permitindo a elaboração de perfis de consumo, ou de padrões de deslocação, por exemplo, podendo, num futuro, permitir conhecer o paradeiro de todos os nossos bens. Do ponto de vista da privacidade este mecanismo suscita ainda preocupações especiais em virtude da sua utilização poder passar despercebida – quer porque os *microchips* podem ser microscópicos, quer porque os leitores podem ser accionados remotamente sem que o seu «portador» se aperceba, visto que, ao contrário dos códigos de barras, não se torna absolutamente necessário aproximá-los do sensor que os detecta. Isto torna imperioso o controlo do uso das informações derivadas deste mecanismo, designadamente dos desvios da finalidade destes tratamentos de dados, bem como das suas condições de segurança.

Nos processos industriais, as aplicações mais vulgares limitam-se à utilização das informações para gestão de *stocks* ou meros fins de inventário, sem que ao produto sejam associados dados relativos a pessoas. Contudo, não deve estar longe a despensa electrónica que nos avise que acabamos de fazer sair do armário a última embalagem de papa infantil, e que nos pergunte se queremos juntá-la à lista de compras do nosso supermercado electrónico – ou, indo mais longe, que essa mesma despensa, chegado o nosso *stock* pessoal a determinado nível, verifique a nossa disponibilidade financeira e, de acordo com as nossas instruções, proceda automaticamente à encomenda das compras da semana. A identificação por radiofrequência em breve destronará os códigos de barras (também pela muito maior quantidade de informação que pode suportar), aumentando a nossa qualidade de vida, mas permitindo potencial e virtualmente, conhecer tudo aquilo que venhamos a adquirir.

Alguns princípios básicos a ter em conta na utilização desta tecnologia são o princípio da finalidade e da proporcionalidade, que devem ditar que seja respeitada a finalidade da

---

[51] Veja-se a divulgação feita, por exemplo em: <http://www.verichipcorp.com>, consultada Maio de 2006.

implantação do *microchip* num determinado bem – por exemplo apenas para gestão de *stocks* dentro de uma fábrica –, não devendo este ser incorporado no produto em si, mas apenas na embalagem de modo a que seja destruído pelo consumidor que a ele acede.

Pelo conflito entre a sua utilidade e as potenciais ameaças à privacidade que poderá gerar, a Comissão Europeia, em Março de 2006, iniciou uma consulta acerca da utilização desta técnica.

IV. 2. OS DADOS BIOMÉTRICOS DOS TRABALHADORES

Outro acesso debate tem sido travado em torno do uso de dados biométricos. O combate ao terrorismo trouxe para a ordem do dia a necessidade da utilização de dados biométricos – de que o exemplo mais comum é a impressão digital – em documentos de identificação como passaportes e bilhetes de identidade.

Estes dados permitem a *identificação* ou a *autenticação* de pessoas, por serem, em via de regra, *universais* – existindo em todas as pessoas -, *únicos* – são diferentes de indivíduo para indivíduo -, *permanentes* – são estáveis para cada pessoa, não variando no tempo -, *acessíveis* e *quantificáveis*.

Mas a utilização destes dados ultrapassa as necessidades de segurança e investigação criminal e vai sendo cada vez mais frequente o uso de aparelhos biométricos para controlo da assiduidade dos trabalhadores, e consequente processamento de remunerações.

Em Portugal, a CNPD tem vindo a aceitar o uso destes mecanismos para controlo de entradas e saídas de funcionários com recurso, designadamente, à impressão digital, ao contorno da mão ou à leitura da íris, considerando que a simples recolha e armazenamento deste dado biométrico, em si mesma, não tem reflexos na integridade física do trabalhador, e que também não põe em causa, por si só, a sua privacidade[52].

O uso de dados biométricos fica sujeito a autorização da CNPD que apreciará as suas condições em concreto.

Note-se que por serem dados biométricos tratados para fins meramente pessoais ou domésticos, não estão abrangidos pela Lei de Protecção de Dados Pessoais o uso da impressão digital para por um computador pessoal ou um automóvel a funcionar.

---

[52] Veja-se, por exemplo, a Autorização n.º 511/2004, disponível em www.cnpd.pt.

IV.3. A VIDEOVIGILÂNCIA

O uso de câmaras de videovigilância vulgarizou-se de tal modo que nos cruzamos com elas no condomínio onde vivemos, na estrada que percorremos, no parque de estacionamento, no estabelecimento que frequentamos para tomar o pequeno-almoço e comprar o jornal, e no nosso local de trabalho…

A Lei portuguesa, na linha da Directiva Europeia, também protege a informação pessoal que seja recolhida sob a forma de imagens, pelo que a utilização de câmaras de videovigilância deve obedecer às regras estabelecidas (a *alínea a)* do art. 3.º inclui na noção de dados pessoais o som e a imagem; o art. 4.º, n.º 4, inclui expressamente a videovigilância no âmbito de aplicação do diploma).

Assim, por exemplo, quando uma empresa contrata uma outra empresa para prestação de serviços de segurança privada, e ainda que esta esteja legalizada para a prestação de tais serviços junto do Ministério da Administração Interna, a empresa contratante deve comunicar o uso de câmaras à CNPD para essa finalidade, pedindo autorização a esta Comissão[53].

O uso de câmaras de videovigilância no local de trabalho foi já, em Portugal, objecto de decisões jurisprudenciais que devem orientar o comportamento das empresas neste domínio. Recentemente, o Supremo Tribunal de Justiça ordenou a uma empresa de produtos farmacêuticos que retirasse câmaras de vídeo de um armazém onde haviam sido instaladas com a finalidade declarada de protecção de pessoas e bens, em especial, para evitar o desvio de medicamentos[54]. O Tribunal argumentou que o empregador não poderia sujeitar «os seus trabalhadores a uma permanente medida de polícia, transformando-os indefinidamente em suspeitos da prática de ilícitos criminais, com clara violação dos seus direitos de personalidade». A vigilância que sujeite a actividade laboral a contínua e permanente observação, por utilização de câmaras direccionadas aos trabalhadores no seu local de trabalho não foi considerada admissível.

---

[53] O que pode fazer através do preenchimento do formulário disponível na página da Internet da CNPD: <www.cnpd.pt>.

[54] A decisão, de 20 de Fevereiro de 2006, encontra-se disponível em: <http://www.cnpd.pt/bin/legis/juris/decisoes/Sindicato.pdf>, acedida em 20 de Maio de 2006.

Em Portugal, o uso de câmaras de videovigilância tem de ser comunicado à CNPD, para efeitos de autorização. Esta vem admitindo como sua finalidade a garantia da segurança de pessoas e bens, sendo o principal objectivo da vigilância a utilização das imagens como prova de infracções criminais praticadas. É importante reforçar que em Portugal a falta de legalização do uso de câmaras junto da CNPD impede a utilização da prova, que tem sido considerada ilegal pelos tribunais.

A Comissão portuguesa não tem aceite o uso de câmaras para efeitos de vigilância do desempenho profissional do trabalhador, na sequência do art. 20.º do Código do Trabalho relativo a «meios de vigilância a distância no local de trabalho». Por segurança devem aqui entender-se não apenas a segurança no sentido de prevenção e combate a delitos contra a pessoas e património, mas também a segurança/saúde/integridade física do trabalhador face à especial perigosidade da tarefa desempenhada (como no caso do trabalho em minas, centrais nucleares), ou dos materiais manuseados (como produtos químicos perigosos).

Para além da necessidade do respeito pela finalidade a que se destina a instalação das câmaras (princípio da finalidade), assume particular importância neste ponto a garantia do direito de informação de todos aqueles que lhes ficam sujeitos.

IV.4. BREVE NOTA SOBRE A TRANSFERÊNCIA DE DADOS PESSOAIS PARA OUTROS PAÍSES

A globalização da economia trouxe consigo, já o referimos, a circulação de pessoas, designadamente trabalhadores, e dos dados pessoais que lhes respeitam. Procurando permitir a livre circulação das informações pessoais, a Directiva Europeia 95/46/CE estabeleceu um regime garantístico base, a transpor para todos os Estados-membros. Apesar da liberdade de circulação de informação, a lei portuguesa prevê que a comunicação de dados a Estados-membros deva ser notificada à CNPD. Já a circulação de informações pessoais para outros Estados fora da União Europeia fica sujeita a regras especiais.

As condições do fluxo de dados, que deve ser previamente autorizado pela autoridade de protecção de dados do Estado-membro em causa, dependerão do nível de protecção garantido pelo país que pretende receber os dados (no caso português, veja-se o art. 20.º da Lei da Protecção de Dados).

Até hoje a Comissão Europeia apenas considerou que ofereciam um nível de protecção idêntico ao Europeu em matéria de dados pessoais, a Suiça, o Canadá, a Argentina, a Ilha de Man e o Guernsey[55].

Não fazem parte deste grupo, por exemplo, o Brasil, a China ou os Estados Unidos da América, muito embora neste último caso a Europa tenha negociado com os Estados Unidos o que ficou conhecido por Acordo *Safe Harbor*, onde se encontram descritos os requisitos a que devem obedecer as empresas e organizações norte-americanas que pretendam receber dados pessoais provenientes da Europa, que devem proceder à sua auto certificação junto do respectivo *Department of Commerce*, comprometendo-se a respeitar esses requisitos, sob pena de aplicação de sanções.

O facto de o país de destino das informações não ter sido considerado como oferecendo um nível de protecção semelhante ao europeu, não impede que o fluxo de dados possa ser autorizado pela autoridade de protecção dados: este pode ficar sujeito ao consentimento informado do trabalhador, cliente, *etc*, que é o fundamento mais invocado para tal transmissão de dados, ou ter por fundamento a prossecução dum interesse público importante, ou a protecção de interesses vitais do titular dos dados. Também se admite que a autoridade de protecção de dados possa autorizar o fluxo se os dados em causa constarem de registo público, ou quando entre os dois Estados seja celebrado um acordo com base nas cláusulas contratuais tipo aprovadas pela Comissão Europeia. Estas, *grosso modo*, admitem que um terceiro – o titular dos dados – que não é parte no compromisso, possa beneficiar dele, fazendo-o valer caso sofra danos, e define as obrigações de ambas as partes, e as garantias para o titular dos dados[56].

IV.5. SPAM OU *JUNK MAIL*– AS COMUNICAÇÕES ELECTRÓNICAS NÃO SOLICITADAS

Os números em torno das mensagens electrónicas não solicitadas são impressionantes.

---

[55] Também considerou a Hungria, hoje Estado-membro. Os fluxos podem igualmente ter lugar para a Noruega, Liechtenstein e Islândia, países que também integram o Espaço Económico Europeu.

[56] Decisão da Comissão n.º 2001/497/CE, de 15 Junho de 2001, publicada no JOCE L 181/19,de 4 de Julho de 2001, sobre cláusulas contratuais gerais para transferência de dados pessoais para países terceiros.

Num estudo de 2001, a União Europeia estimou ser de 10 biliões de euros/ano o custo do envio de SPAM para os seus destinatários[57]. Neste ano, o volume de *junk mail* representava cerca de 7 % das comunicações electrónicas. Números provisórios para 2004 estimavam que cerca de 50% do tráfego fosse SPAM.

Numa outra perspectiva, a americana *Computer Mail Services*, que vende *software* anti-SPAM, disponibiliza na sua página um pequeno simulador para o cálculo do custo do SPAM numa empresa: num dos exemplos aí fornecidos, uma empresa com 500 trabalhadores que em média trabalhem por ano 230 dias, que recebam 5 mensagens de SPAM por dia, demorando 10 segundos a ler, a identificá-la como SPAM e a destruir cada uma dessas mensagens, e se em média esses trabalhadores receberem 25 dólares por hora, o custo para a empresa seria de cerca de 40.000 dólares por ano.

Claro que este mesmo exemplo demonstra que o SPAM em si, aliás, como os vírus informáticos, criou ele próprio uma nova oportunidade de negócio – a daqueles que criam *software* para o combater.

Preocupados com o SPAM, o Parlamento Europeu e o Conselho da União Europeia aprovaram uma Directiva Europeia (2000/31/CE) que impõe regras para o envio de mensagens comerciais não solicitadas por correio electrónico, por SMS (*Short Message Service*) ou MMS (*Multimedia Messaging Service*)[58]: ao contrário do que sucede com a generalidade das mensagens de *marketing*, em que vigora um sistema de *opt-out*, significando que o destinatário da mensagem deve tomar a iniciativa de pedir para sair da *mailing list* utilizada para a operação de marketing, no caso das mensagens comerciais não solicitadas enviadas por via electrónica passa a vigorar um sistema de *opt-in*: o destinatário terá previamente de aceitar receber tais mensagens[59]. Ainda assim, a Directiva Europeia e a Lei

---

[57] Fala-se hoje também já de SPIM: mensagens instantâneas (IM) não solicitadas.

[58] Os Estados Unidos da América também aprovaram a CAN-SPAM Act (*Controlling the Assault of Non-Solicited Pornography and Marketing Act*), sobre ela pode ler-se: REINALDO FILHO, Demócrito, *O CAN-SPAM Act - Em vigor a Lei Federal dos EUA que combate o SPAM*, **Revista de Direito Electrónico**, a 2, nº 05, p. 109, Disponível em <http://www.ibde.org.br/revista/index_arquivos/rede5.pdf>, acedido em 30 de Maio de 2006.

[59] Este regime consta, em Portugal, do art. 22.º, do Decreto-Lei n.º 7/2004, de 7 de Janeiro, relativo ao comércio electrónico. Sobre o SPAM põe ler-se, na doutrina portuguesa: LEITÃO, Luís Menezes. A distribuição de mensagens de correio electrónico indesejadas (SPAM). **Direito da Sociedade da Informação**, Coimbra: Coimbra Editora, Vol. V, 2004, p. 191 e ss.; CASTRO, Catarina Sarmento e. *Protecção de Dados Pessoais na Internet*. **Sub Judice – Justiça e Sociedade**. Coimbra: DocJuris, 2006 (no prelo).

portuguesa admitem que possam ser enviadas mensagens comerciais por via electrónica por um fornecedor de produtos ou serviços, e a propósito destes, aos clientes com quem celebrou anteriormente transacções, se ao cliente tiver sido explicitamente oferecida a possibilidade de o recusar por ocasião da transacção realizada, se lhe forem dados meios de a todo momento recusar a sua futura recepção. Esta imposição da solução de *opt-in*, será, muito provavelmente, uma das disposições mais desrespeitadas em matéria de protecção de dados pessoais.

V. CONCLUSÕES

Estes foram apenas alguns casos que em matéria de protecção de dados pessoais nos pareceram mais relevantes para o dia a dia das empresas, designadamente das empresas que, neste sector, enfrentam os desafios e recolhem as vantagens da globalização, mas que também ficam sujeitas às limitações que na sua sequência a lei impõe.

Para os mais desprevenidos, o exposto neste texto poderá ter parecido uma exacerbada defesa da privacidade.

Não foi, contudo, objectivo desta exposição fazer a todo custo prevalecer a privacidade dos cidadãos sobre a necessidade – para a economia em geral e para as empresas em particular - de circulação de informação, designadamente, de informações que permitem identificar pessoas. Começámos até por afirmar que nas soluções encontradas, o legislador teve de ponderar os bens da privacidade e da liberdade de circulação de informação: foi, afinal, esse o objectivo da Directiva Comunitária que pretendeu salvaguardar a necessidade de circulação de informação.

A informática, e os tratamentos de dados pessoais que permite, é uma ferramenta extraordinária, cuja utilização tem uma mais valia incalculável para fins vários, e também, naturalmente, para fins de natureza económica. O mal que daí possa resultar, não está na tecnologia, pode estar no uso ilegal que dela se faça (por violação dos princípios da finalidade do tratamento das informações, ou dos direitos de informação, acesso e rectificação, por exemplo).

Também não quisemos com tudo isto afirmar que são sobretudo as empresas privadas as maiores ameaças à privacidade: nesta matéria, também o Estado é fortemente prevaricador. E a ameaça que um Estado pode constituir quando faça um uso errado das informações de que dispõe é bem maior do que a de qualquer privado. Basta lembrar um exemplo histórico àqueles para quem a sua própria privacidade não é uma causa, nem mesmo uma preocupação séria: apenas com o auxílio de uma tecnologia hoje muitíssimo rudimentar – uns cartões perfurados inventados por *Hollerith* -, o nacional socialismo pode, durante a II Guerra Mundial, em relativamente pouco tempo, realizar um recenseamento da população judaica e, mais tarde, localizar com precisão judeus e respectivos bens[60].

Ou para dar um exemplo já do novo milénio, segundo um Relatório da União Europeia, o *Echelon* – sistema de vigilância das comunicações posto em prática por 5 serviços secretos: os Estados Unidos da América, o Reino Unido, o Canadá, a Austrália e a Nova Zelândia - intercepta 3 milhões de comunicações por dia com base em palavras-chave, vigiando, por exemplo, as nossas mensagens de correio electrónico, os telefonemas, ou os *downloads* que fazemos de ficheiros da Internet…

A máquina começou por ser inventada para fazer (XIX), mais tarde veio ajudar a pensar (XX), e hoje já consegue sentir – por exemplo, a presença de pessoas ou de bens. Se ela existe para auxílio do Homem, deve o seu uso respeitar a Declaração Universal dos Direitos do Homem (1948), a Convenção Europeia dos Direitos do Homem (1950), e a mais recente Carta dos Direitos Fundamentais da União Europeia (2000), que entre outros direitos consagram o direito à privacidade, isto é, um «direito a ser deixado em paz».

O desafio está em encontrar o melhor equilíbrio entre este «right to be let alone», e a necessidade da circulação da informação imposta pelo mercado.

REFERÊNCIAS BIBILOGRÁFICAS.

ASCENSÃO, José de Oliveira. *Estudos sobre Direito da Internet e da Sociedade da Informação*. Coimbra: Almedina, 2001

CANOTILHO, José Joaquim Gomes/MOREIRA, Vital. *Constituição da República Portuguesa Anotada*. Coimbra: Coimbra Editora, 3. ª Edição, 1993

[60] Foram utilizados os cartões perfurados criados por *Herman Hollerith*, americano que criara o sistema para o recenseamento da população americana em 1890.

CARVALHO, Orlando de. *Teoria Geral do Direito Civil.* Coimbra: Centelha, 1981;

_____*Teoria Geral da Relação Jurídica. Sumários*. Coimbra: 1970

_____*Direitos de Personalidade* (Apontamentos de aulas), Polic., Coimbra

CASTRO, Catarina Sarmento. *Privacidade, informática e dados pessoais*. Coimbra: Coimbra Editora, 2004

_____. *Protecção de Dados Pessoais na Internet*. Sub Judice – Justiça e Sociedade. Coimbra: DocJuris, 2006 (no prelo).

GALLOUEDEC-GENUYS F.. *La vie privée: une création informatique*. Les enjeux culturels de l'informatisation, F. Gallouedec-Genuys (dir.) et P. Lemoine (dir.), La Documentation Française, Paris, 1980

PINTO, Carlos Alberto da Mota. *Teoria Geral do Direito Civil*. 3.ª Edição, Coimbra: Coimbra Editora, 1989

PINTO, Paulo da Mota, *A limitação voluntária do direito à reserva sobre a intimidade da vida privada*. Estudos em Homenagem a Cunha Rodrigues. Vol. II, Coimbra: Coimbra Editora, 2001

_____. *O direito ao livre desenvolvimento da personalidade*. Portugal-Brasil Ano 2000. Coimbra: Coimbra Editora, 1999

_____. *A protecção da vida privada e a Constituição*. Boletim da Faculdade de Direito da Universidade de Coimbra. Coimbra: Vol. LXXVI, 2000

SOUSA, Rabindranath Capelo de. *O direito geral de personalidade*. Coimbra: Coimbra Editora, 1995

LEITÃO, Luís Menezes. A distribuição de mensagens de correio electrónico indesejadas (SPAM). Direito da Sociedade da Informação, Coimbra: Coimbra Editora, Vol. V, 2004, p. 191

MARQUES, A. Garcia. *Legislar sobre protecção de dados pessoais em Portugal (do art. 35.º da Constituição, à Lei n.º 10/91, de 29 de Abril*. Legislação, n.º 8

REINALDO FILHO, Demócrito, *O CAN-SPAM Act - Em vigor a Lei Federal dos EUA que combate o SPAM*, Revista de Direito Electrónico, a 2, nº 05, p. 109, Disponível em <http://www.ibde.org.br/revista/index_arquivos/rede5.pdf>, acedido em 30 de Maio de 2006

WARREN, Samuel/BRANDEIS, Louis. *The right to privacy*. Harvard Law Review, Vol. IV, n.º 5, 15 Dezembro 1890