que não impliquem uma restrição inaceitável do direito ao sigilo (cfr., no sentido da desproporcionalidade de um prazo de 38 dias, cfr. Ac. n.º 528/03). O Ac. n.º 347/01 é especialmente importante nesta matéria, uma vez que Tribunal entendeu, na linha dos acórdãos anteriores, inconstitucional que o juiz ordenasse novos períodos de escuta antes do controlo do conteúdo das escutas anteriormente realizadas (cfr. ainda Ac. n.º 379/04).

Já no domínio da nova versão do Código de Processo Penal, no Ac. n.º 293/08, o TC foi chamado a pronunciar-se sobre a conformidade com a Constituição da interpretação do artigo 188.º, n.º 6, alínea *a*), que permita ao juiz de instrução ordenar a destruição dos suportes técnicos e relatórios manifestamente estranhos ao processo, que digam respeito a conversações em que intervenham pessoas referidas no n.º 4 do artigo 187.º, sem que o arguido deles tenha conhecimento e se possa pronunciar sobre a sua relevância. Na parte da fundamentação com interesse para o artigo 34.º, n.º 4, o Tribunal, depois de entender que o não conhecimento por parte do arguido das referidas escutas não viola as suas garantias de defesa, afirma que "a destruição de suportes técnicos e relatórios manifestamente estranhos ao processo [...] tem por base a proteção a proteção do direito ao sigilo das telecomunicações". Este aresto, em aplicação do princípio da proporcionalidade, conclui que esperar que o arguido tivesse conhecimento das referidas escutas e relatórios "comportaria uma desnecessária e inaceitável compressão daqueles direitos constitucionalmente consagrados" (referindo-se ao n.º 4 do artigo 34.º e ao n.º 1 do artigo 26.º).

No Ac. n.º 241/02 julgou inconstitucional a interpretação do artigo 519.º, n.º 3, alínea *b*), do Código de Processo Civil quando, em processo laboral, a sua interpretação conduz à valoração de documento que contenham dados relativos a tráfego de comunicações de faturação detalhada, ainda que recolhidos com autorização judicial, por violação dos artigo 26, n.º 1, e 34.º, n.ºs 1 e 4. O Tribunal entendeu que "tal como num processo em que o resguardo da dignidade do arguido, com proscrição de meios de prova obtidos com violação de direitos fundamentais, há de sempre condicionar a averiguação da verdade material – e isto mesmo estando em causa a ofensa de bens essenciais à vida em sociedade – também num outro, em que se dirime um litígio de interesses privados, não se justifica sanção menos grave para a prova alcançada com idêntica violação". Acrescente-se ainda que o artigo 34.º, n.º 4, admite apenas que as escutas sejam determinadas por exigências penais, o que levanta a questão de saber se escutas obtidas para esses fins poderão ser utilizadas como prova em processo de outra natureza, questão à qual o Tribunal não responde. A limitação constitucional da quebra de sigilo das comunicações nos termos da lei processual penal parece implicar também que a prova recolhida só possa ser usada nesse tipo de processo, não podendo as escutas ser *exportadas* para outro tipo de processos. Apenas no caso da de dedução de pedido cível apenso ao processo penal parece ser de admitir *cum grano salis* o aproveitamento de escutas, visto que, muitas vezes, são estas que indiciam e provam os factos imputados ao arguido que sustentam esse pedido.

XIX – A **prova ilicitamente obtida através da intromissão no domicílio ou da violação das comunicações privadas** é nula nos termos do disposto no n.º 8 do artigo 32.º Esta nulidade significa uma proibição de *utilização* e *valoração* do material probatório ilicitamente recolhido (para mais desenvolvimentos, cfr. a anotação ao artigo 32, n.º 8, deste *Comentário*).

GERMANO MARQUES DA SILVA | FERNANDO SÁ

Artigo 35.º
Utilização da informática

1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam nos termos da lei.

2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.

3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.

5. É proibida a atribuição de um número nacional único aos cidadãos.

6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

Origem do texto: A redação deste artigo sofreu grandes alterações desde a sua inclusão no texto constitucional justificadas pela natureza da matéria a regular, e pela necessidade de adaptar o conteúdo da regulamentação às normas e diretivas comunitárias que foram entrando em vigor neste domínio (esta necessidade fez-se particularmente sentir em relação à Diretiva n.º 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares face ao tratamento de dados pessoais e à livre circulação desses dados).

Inicialmente, o texto deste artigo dividia-se em três números. O n.º 1 do artigo 35.º começou por consagrar o direito de todo o cidadão de tomar conhecimento do conteúdo de registos mecanográficos a seu respeito, de se inteirar do fim a que se destinassem essas informações, e de exigir a retificação e a atualização dos dados constantes desses registos. O n.º 2 deste artigo proibia o uso da informática para o tratamento de dados referentes a convicções políticas, fé religiosa ou vida privada, salvo quando se tratasse do processamento de dados não identificáveis para fins estatísticos, e o n.º 3 proibia a atribuição de um número nacional único aos cidadãos.

Com a revisão de 1982 foi substituída a expressão "registos mecanográficos" – utilizada até aí pelo n.º 1 deste artigo – por "registos informáticos", e alargou-se substancialmente o âmbito de aplicação do n.º 2 (que entretanto passara a n.º 3, pelo aparecimento de um novo n.º 2, que vem proibir o acesso por terceiros a ficheiros com dados pessoais e a respetiva interconexão). O novo n.º 3 do artigo 35.º, vem então alargar a proibição do tratamento informático de dados aos elementos relativos às convicções filosóficas e à filiação partidária ou sindical do cidadão. Introduz-se um n.º 4, que remete para a lei a tarefa de definir o conceito de dados pessoais para efeitos de registo informático, e converte-se o anterior n.º 3, que não sofre quaisquer alterações, em n.º 5 do artigo 35.º revisto.

Em 1989 procede-se a uma nova alteração da redação deste artigo em ordem a permitir o fluxo transfronteiriço de dados pessoais, que era proibido na redação anterior, salvo nos casos previstos na lei, o que não se considerava compatível com a Convenção sobre Proteção de Dados Pessoais do Conselho da Europa. O n.º 1 é modificado, introduzindo-se como limite ao direito de acesso aos dados pessoais constantes de registos informáticos o segredo de Estado e o segredo de justiça. Os n.ºs 2 e 3 mantêm-se inalterados. Alargam-se as competências legais previstas pelo n.º 4, passando a ser tarefa do legislador a definição do conceito de bases e bancos de dados e respetivas condições de acesso, constituição e utilização por entidades públicas e privadas.

O atual n.º 1 do artigo 35.º (1997) deixou de referir-se ao segredo de Estado e de justiça como as únicas hipóteses de restrição do direito de acesso e de informação do cidadão relativamente aos dados informáticos que lhe dizem respeito, para substituir essa enumeração, casuística e in-

completa, por uma remissão genérica para os "termos da lei" (lei que refere expressamente muitos outros fundamentos de restrição legítima). O n.º 2 (que corresponde genericamente ao anterior n.º 4), prevê a proteção dos dados pessoais através de uma entidade administrativa independente (CNPD). O n.º 3 alarga uma vez mais a tutela concedida aos dados pessoais, passando a proibição do uso da informática a abranger dados relativos à origem étnica das pessoas. Por outro lado, o legislador passa a incluir o "consentimento expresso" do titular e a "autorização legal com garantias de não discriminação" entre as causas de justificação para o uso informático de elementos ditos "sensíveis", a par da possibilidade já prevista do seu processamento como dados estatísticos não individualmente identificáveis. O atual n.º 4 (anterior n.º 2) proíbe de forma lapidar o acesso a dados pessoais de terceiros salvo em casos excecionais previstos na lei. Mantém-se a redação do anterior n.º 5. O n.º 6 passa a garantir a todos os cidadãos o livre acesso às redes informáticas de uso público. Acrescentou-se ainda um n.º 7 a este artigo que estabelece expressamente que a tutela que é conferida às informações processadas informaticamente se estende aos dados pessoais constantes de ficheiros manuais.

Trabalhos preparatórios: DAC, n.º 38, de 28/8/1975, págs. 1058 e segs.

DAR, 2.ª legislatura, 2.ª sessão legislativa, 2.ª série, 2.º suplemento ao n.º 6, pág. 70(57); 2.º suplemento ao n.º 80, págs. 1508(29)-1508(30); suplemento ao n.º 98, págs. 1878(12) e 1878(13); suplemento ao n.º 124, págs. 2230(1) e segs.; 1.ª série, n.ºs 101, 103 e 115, de 11 e 16/6/1982 e 8/7/1982, págs. 4186, 4239 e 4778 e segs.

DAR, 5.ª legislatura, 2.ª sessão legislativa, 2.ª série, n.º 11-RC, págs. 311 e segs.; n.º 13-RC, págs. 361 e segs.; 3.ª sessão legislativa, n.º 72-RC, págs. 2162 e segs., e 79-RC, págs. 2357 e segs.; 1.ª série, n.º 68, de 21/4/1989, págs. 3295 e segs.

DAR, 7.ª legislatura, 2.ª sessão legislativa, 2.ª série, n.º 21-RC, págs. 573 e segs., e n.º 78-RC, págs. 2286 e segs.; e 1.ª série, 2.ª sessão legislativa, n.º 95, de 16/7/1997, págs. 3412 e segs.

Direito Comparado: Constituições angolana, artigo 60.º; brasileira, artigo 5.º-LXXII e LXXVII; cabo-verdiana, artigos 44.º e 45.º; espanhola, artigo 18.º, n.º 4; moçambicana, artigo 71.º; timorense, artigo 38.º

Doutrina: José António Barreiros, *Informática, Liberdades e Privacidade (artigo 35.º)*, in AA.VV., *Estudos sobre a Constituição*, Vol. I, Lisboa, 1977; Cavaleiro de Ferreira, *Curso de Processo Penal*, Vol. III, Lisboa, 1981; Bacelar de Gouveia, *Os Direitos Fundamentais à protecção dos dados pessoais informatizados*, ROA, Ano 51, n.º 3, dezembro de 1991, págs. 699 e segs.; Alberto Martins, *Protecção de Dados Pessoais Informatizados na Constituição da República Portuguesa*, Colóquio Informática e Tribunais: Bases de Dados Administrativas e Jurídicas, org. pelo Gabinete Diretor da Informatização Judiciária, Lisboa, 1991, págs. 425 e segs.; Agostinho Eiras, *Segredo de Justiça e Controlo de Dados Pessoais Informatizados*, Coimbra, 1992; José A. S. Garcia Marques, *Legislar sobre protecção de dados pessoais em Portugal (do artigo 35.º da Constituição à Lei n.º 10/91, de 29 de abril)*, Legislação. Cadernos de Ciência de Legislação, n.º 8, 1993, págs. 37 e segs.; Alberto Martins, *O Direito à Protecção dos Dados Pessoais Informatizados*, Novos Direitos dos Cidadãos, Lisboa, 1994, págs. 27 e segs.; Manuel Lopes Rocha, *Do Direito da Informática ao Direito da Informática em Portugal*, in AA.VV., *Direito da Informática. Legislação e Deontologia*, Lisboa, 1994; Rabindranath Capelo de Sousa, *O Direito Geral de Personalidade*, Coimbra, 1995; José F. de Faria Costa, *O Direito Penal, a Informática e a Reserva da Vida Privada*, in AA.VV., *Comunicação e Defesa do Consumidor*, Instituto Jurídico da Comunicação da Faculdade de Direito da Universidade de Coimbra, 1996, págs. 303 e segs.; José N. da Cunha Rodrigues, *Informática e Reserva da Vida Privada*, in AA.VV., *Comunicação e Defesa do Consumidor*, Instituto Jurídico da Comunicação da Faculdade de Direito da Universidade de Coimbra, 1996, págs. 287 e segs.; Helena Isabel Moniz, *Notas sobre a protecção de dados pessoais perante a informática – o caso especial dos dados pessoais relativos à saúde*, RPCC, Ano 7, abril-junho de 1997, págs. 231 e segs.; Damião da Cunha, *Comentário Conimbricense ao Código Penal, Parte Especial*, Tomo I, anotação ao artigo 193.º, Coimbra, 1999; José de Oliveira Ascensão, *E Agora? Pesquisa do Futuro Próximo*, in AA.VV., *Sociedade da Informação. Estudos Jurídicos. Seminário organizado pela Associação Portuguesa de Direito Intelectual*, Coimbra, 1999, págs. 9 e segs.; Germano Marques da Silva, *Curso de Processo Penal*, Vol. III, 3.ª edição revista e atualizada, Lisboa, 2000; Paulo da Mota Pinto, *A protecção da vida privada e a Constituição*, Boletim da Faculdade de Direito de Coimbra, Vol. LXXVI, 2000, págs. 153 e segs.; AA.VV., *Estudos sobre Direito da Internet e da Sociedade da Informação*, Coimbra, 2001, págs 45 e segs.; Vieira de Andrade, *Os Direitos Fundamentais na Constituição Portuguesa de 1976*, 2.ª ed., Coimbra, 2001; José Renato Gonçalves, *Acesso à Informação das Entidades Públicas*, Coimbra, 2002; Seabra Lopes, *A Proteção da Privacidade e dos Dados Pessoais na Sociedade da Informação: Tendências e Desafios numa Sociedade em Transição*, in *Estudos dedicados ao Prof. Doutor Mário Júlio de Almeida Costa*, Lisboa, 2002, págs. 779 e segs.; Rui Medeiros, *O Estado de Direitos Fundamentais Português: Alcance, Limites e Desafios*, Anuário Português de Direito Constitucional, Vol. 2.º, Lisboa, 2002, págs. 23 e segs.; Amadeu Guerra, *A Lei de Protecção de Dados Pessoais*, Direito da Sociedade da Informação, 2.º Vol., Coimbra, 1999-2003, págs. 145 e segs.; José A. S. Garcia Marques, *A criminalidade informática no quadro da proteção de dados pessoais*, Polícia e Justiça, Coimbra Editora, III Série, n.º 1, jan.-jun. de 2003, págs. 7 e segs.; José A. S. Garcia Marques, *Do tratamento de dados pessoais sensíveis (comentário)*, Cadernos de Justiça Administrativa, Braga, n.º 39, maio-jun. de 2003, págs. 44 e segs.; Maria Eduarda Gonçalves, *Direito da Informação – Novos Direitos e Formas de Regulação na Sociedade da Informação*, Coimbra, 2003; Pedro Pais de Vasconcelos, *Protecção de Dados Pessoais e Direito à Privacidade*, Direito da Sociedade da Informação, 1.º Vol., Coimbra, 1999-2003, págs. 241 e segs.; José A. S. Garcia Marques/Lourenço Martins, *Cyberlaw em Portugal – O Direito das Tecnologias da Informação e da Comunicação*, Editora Centro Atlântico, 2004; Catarina Sarmento e Castro, *Direito da informática, privacidade e dados pessoais*, Coimbra, 2005; José A. S. Garcia Marques/Lourenço Martins, *Direito da Informática*, 2.ª ed., Coimbra, 2006; AA.VV., *Sociedade da informação. O Percurso Português. Dez Anos de Sociedade da Informação. Análise e Perspetivas*, Lisboa, 2007; Ana Vaz, *Segurança da Informação, Proteção da Privacidade e dos Dados Pessoais*, Nação e Defesa, Lisboa, n.º 117, verão de 2007, págs. 35 e segs.; Gomes Canotilho/Vital Moreira, *Constituição da República Portuguesa Anotada*, 5.ª ed., Coimbra, 2007; José Magalhães, *Dicionário da Revisão Constitucional*, Lisboa, Editorial Notícias, 1999 (Publicações Europa-América, 2008); Jorge Miranda, *Manual de Direito Constitucional, Direitos Fundamentais*, Vol. IV, 4.ª ed., Coimbra, 2009.

Jurisprudência: ParCC n.º 3/81; AcTC n.ºs 182/89 (inconstitucionalidade por omissão/informática), 135/90 (quotizações sindicais), 458/93 (segredo de Estado como restrição ao direito de acesso dos cidadãos aos dados constantes de ficheiros ou registos informáticos a seu respeito), 355/97 (informática/registos oncológicos), 255/02 (equipamentos eletrónicos e de vigilância), 256/02 (estatuto legal do defensor do contribuinte), 362/02 (higiene, segurança e saúde no trabalho/exames médicos), 368/02 (banco de dados sobre o estado de saúde dos trabalhadores), 207/03 (videovigilância nas salas de jogos), 306/03 (tratamento de dados sobre o estado de saúde dos trabalhadores), 555/07 (afixação de elementos relativos á identificação civil e estatuto profissional dos trabalhadores), 230/08 (dados constantes dos mapas de quadros de pessoal), 213/08 (valoração de provas documentais/base de dados/VIA VERDE).

I

I – Não existe consenso absoluto quanto ao **modelo constitucional a seguir como forma de assegurar as faculdades individuais que integram o conteúdo essencial do direito à proteção dos dados pessoais perante o uso das novas tecnologias e, em particular, da informática** (é interessante aqui a posição do direito norte americano, cuja Constituição não reconhece expressamente um "*right of privacy*", e onde não existe uma definição constitucional do conceito, mas onde ele vale incontestado a partir da IV Emenda Constitucional, entendendo-se que o seu teor literal abrange conteúdos vários como a tutela do domicilio, a propriedade privada, e a liberdade da pessoa em geral, que vão sendo concretizados por via jurisprudencial). Além da natureza fortemente "instável" do objeto de regulamentação que torna precária a intervenção constitucional neste domínio, as opiniões e as legislações dividem-se entre a necessidade de garantir um direito fundamental autónomo, e a consideração do direito à proteção dos dados pessoais como parte integrante do âmbito de tutela de outro direito fundamental.

De entre os países que entenderam ser de optar pela consagração expressa do direito à proteção dos dados pessoais, contam-se Portugal, a Suécia, a Eslovénia, a

Hungria e a Polónia (já não reconhecem de forma específica esse direito, mas contém disposições sobre a matéria, designadamente sob a forma de imposições legiferantes, as Constituições espanhola, holandesa e finlandesa).

Enveredaram pelo caminho oposto, considerando que a proteção dos dados pessoais não deve ter autonomia em relação à tutela que é concedida à intimidade da vida privada ou ao livre desenvolvimento da personalidade e à dignidade humana, a maior parte dos textos constitucionais dos países da União Europeia, sendo este o caso, por exemplo, da Itália e da Alemanha.

Todavia, e apesar das diferenças que intercedem entre os vários Estados-membros da União Europeia nas formas de reconhecimento deste direito, o conteúdo e limites da sua proteção são tendencialmente coincidentes em todos eles, uma vez que todos subscreveram a Convenção (108) do Conselho da Europa sobre a Proteção de Dados, estando obrigados a transpor para as ordens jurídicas internas o estabelecido pela Diretiva n.º 95/46/CE sobre Proteção de Dados Pessoais.

II – Concretamente, o **direito constitucional alemão** não consagra um direito autónomo de tutela dos dados pessoais, tendo ele sido construído jurisprudencialmente como "direito à autodeterminação informativa", a partir da consideração conjunta do direito geral de personalidade previsto pelo artigo 2.1. da Constituição (GG) e do princípio da dignidade humana consagrado pelo artigo 1.1. do mesmo texto fundamental. O direito previsto pelo artigo 2.1. da GG como um direito ao livre desenvolvimento da pessoa em todas as esferas da sua vida pessoal, integra duas dimensões ou vertentes: uma delas, refere-se especificamente à liberdade de movimentos do sujeito, o que para aqui não é relevante; e a outra, diz respeito ao desenvolvimento da personalidade de cada pessoa nos vários domínios da vida social, abrangendo aspetos ou direitos tão distintos como o direito à imagem, à palavra, à honra, ao casamento e a constituir família e, também, o direito à autodeterminação informativa. Uma vez que a partir do tratamento informatizado de dados pessoais é possível construir uma determinada imagem ou perfil da pessoa, e uma vez que o uso desses elementos pode condicionar ou restringir fortemente a sua liberdade, deve fazer parte dos direitos fundamentais de cada um a possibilidade de controlar e de decidir por si quando, e em que condições, se usarão, ou se tornarão públicas, informações que lhe digam respeito.

Numa decisão jurisprudencial que marcou a construção do direito à autodeterminação informativa nos moldes que acabámos de descrever (*Volkszählungs-Urteil BVerfGE* 65, 1, págs. 42 e segs.), o Tribunal Constitucional alemão considerou que integrava o conteúdo do direito geral de personalidade previsto pelo artigo 2.1. da GG, o direito à "proteção do indivíduo contra a recolha, armazenamento, utilização e transmissão dos seus dados pessoais sem restrições", conferindo, de igual modo, a cada cidadão, a possibilidade de decidir sobre o abandono e a utilização dos seus dados pessoais. A lei tem regulamentado a tutela do cidadão face à administração neste domínio, através da *Bundes-DatenschutzG* e da *Landes-DatenschutzG*, mas segundo SCHMALZ (*Grundrechte, AjS, Schriftenreihe, Juni 1984*, anotação ao artigo 2.1., §§ 480 e segs.) esta regulamentação é todavia imprecisa e pouco clara, pelo que se impõe uma interpretação conforme à Constituição mediante a utilização da *Volkszählungs-Urteils*.

Apesar desta decisão do Tribunal Constitucional alemão no sentido de ter a tutela dos dados pessoais contra abusos da informática como parte integrante de um direito de autodeterminação informativa, há ainda quem entenda na doutrina deste país que o conteúdo desse direito corresponde antes ao âmbito de tutela do direito à imagem que cada um pode querer ter perante os outros e perante a sociedade em geral, quem aceite a sua caracterização como um direito de autodeterminação informativo pertencente todavia ao domínio dos direitos de comunicação enquanto liberdade de

pensamento, de imprensa e de ciência, e quem sustente até que está em causa um verdadeiro direito de natureza real, um direito de propriedade da pessoa sobre os dados de natureza informática que lhe digam respeito. Acerca de todas estas posições, veja-se em detalhe, ARENAS RAMIRO, *El Derecho Fundamental à La Protección de Datos Personales en Europa*, págs. 389 e segs.

III – Também a **Itália** não dispõe de uma previsão constitucional específica neste domínio. Assim, encontram-se autores que tentam uma aproximação ao conceito genérico de *privacy*, usado pelos tribunais norte americanos, como expressão de um direito à reserva da vida privada entendido em moldes amplos, e autores que defendem a existência de um direito de natureza específica, que denominam de direito à liberdade informática, mas cuja fundamentação e enquadramento constitucionais são controvertidos. Acerca do estado da discussão desta questão em Itália, veja-se, MARIA MERCEDES SERRANO PEREZ, *El Derecho Fundamental a la Protección de Datos. Derecho Español y Comparado*, Civitas Ediciones, Madrid, 2003, págs. 35 e segs.

IV – Em **Espanha**, o fundamento material, quer do direito à intimidade pessoal, quer do direito à proteção dos dados pessoais, é o artigo 18.º da Constituição, que consagra, em primeiro lugar, o direito à honra, à intimidade pessoal e familiar, e à própria imagem, sendo dos três direitos aí previstos, o direito à intimidade da vida privada aquele que de mais perto se deixa relacionar com o direito à proteção dos dados pessoais. O n.º 2 deste artigo tutela a inviolabilidade do domicílio, e o n.º 3, protege o direito ao segredo das comunicações. É o n.º 4 do artigo 18.º que contém um mandato ao legislador no sentido de regular o uso da informática com autonomia em relação aos direitos previstos nos outros números deste artigo, e o Tribunal Constitucional tem afirmado claramente que a justificação constitucional deste número se encontra no direito fundamental à proteção dos dados pessoais que não resulta expressamente do texto constitucional, mas que tem um conteúdo distinto do direito à intimidade pessoal reconhecido pelo n.º 1 da mesma disposição.

II

V – O artigo 35.º da Constituição portuguesa atual consagra um **direito à autodeterminação informativa** que tem por finalidade evitar intromissões abusivas na vida privada das pessoas através da recolha e tratamento de dados pessoais informatizados, muito embora a sua materialidade vá para além da tutela da esfera íntima de vida de cada um (contra, entendendo que o direito à tutela dos dados pessoais funciona como garantia do direito à reserva sobre a intimidade da vida privada consagrado no artigo 26.º, pela proibição que aí se encontra consagrada relativamente à recolha e utilização de elementos referentes à vida privada, e porque os elementos de informação que pertencem à vida privada das pessoas podem deixar-se rodear de diferentes níveis de sensibilidade, MOTA PINTO, *A protecção da vida privada*, págs. 526 e segs.; diferentemente, não parecendo restringir o conteúdo deste direito a um princípio ou lógica de privacidade, HELENA MONIZ, *Notas sobre a protecção de dados pessoais*, pág. 245, e GOMES CANOTILHO, *Constituição da República Portuguesa anotada*, artigo 35.º, II, pág. 551, relacionando-o de uma forma mais ampla com o princípio da dignidade da pessoa humana, do desenvolvimento da personalidade e da integridade pessoal). Na verdade, tudo depende da abrangência que se estiver disposto a reconhecer à intimidade da vida privada da pessoa, embora nos pareça que o direito de autodeterminação informativa que aqui se encontra consagrado não se refere apenas a factos pertencentes a essa esfera íntima ou particular de vida (mais próxima dessa esfera íntima de vida estarão os

chamados dados de natureza sensível) mas abrange todos os poderes e faculdades que permitem garantir que a pessoa não é usada como fonte de informação para terceiros contra a sua vontade, podendo além disso controlar a informação que é fornecida e os termos e abrangência em que ela é tratada.

VI – São **dados informáticos** (cfr., sobre o conceito de dados aqui usado, definido como "representação convencional de informação, sob a forma analógica ou digital, possibilitadora do seu tratamento automático", GOMES CANOTILHO/VITAL MOREIRA, *Constituição*, I, pág. 550) de **natureza pessoal** os elementos que, de acordo com a formulação particularmente ampla do n.º 1 do artigo 35.º, "dizem respeito ao cidadão". Trata-se de um conceito muito abrangente de dados pessoais que também é utilizado pela Lei de Proteção dos Dados Pessoais. Segundo o artigo 3.º deste diploma, integra a noção de dados pessoais, "qualquer informação, de qualquer natureza, e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social". Cabem assim neste conceito de dados pessoais, dados ou elementos informativos da mais variada natureza (sinais ou elementos de natureza não convencional ou convencional, como é o caso do nome da pessoa, dados de natureza biométrica, de que fazem parte a identificação da retina, das impressões digitais, e da geometria da mão, fotografias, entre tantos outros) que possibilitem a identificação da pessoa a vários níveis, ou sob vários aspetos (referentes à sua solvabilidade, saúde, costumes, personalidade).

VII – Neste contexto, têm vindo a assumir particular importância os **dados de natureza genética** que são dados considerados sensíveis e que, como tal, merecem tratamento autónomo (artigo 35.º, n.º 3), **e os dados biométricos** que permitem reforçar a segurança do acesso a determinados locais, e permitir que ele fica restringido a certas pessoas, apresentando a identificação com base nestes elementos vantagens inegáveis em relação ao uso de outros meios de identificação, já que não existe em relação a eles a possibilidade de extravio ou de apropriação ilícita, ou a necessidade de recordar números, senhas ou códigos de acesso (sendo proibida a reversão do número ou imagem numérica em que se consubstanciam no elemento físico a partir do qual foram obtidos). A obtenção e uso destes dados está sujeito ao regime geral da Lei n.º 67/98, de 26 de outubro, colocando em geral as mesmas questões de informação, confiança, e proporcionalidade na recolha que se colocam em relação aos restantes dados pessoais, tendo entendido a CPDP (orientação sobre os princípios aplicáveis ao tratamento de dados biométricos para controle de acessos e assiduidade, de 26 de fevereiro de 2004) que a sua colheita não envolve necessariamente uma violação da integridade física, da privacidade, ou da intimidade das pessoas (são formas de proceder socialmente adequadas e inócuas sob o ponto de vista destes bens jurídicos, podendo existir, quando muito, uma violação do direito à autodeterminação informativa onde não sejam cumpridos os requisitos exigidos por lei para a colheita, uso e manutenção dos dados).

VIII – De acordo com a lei, **os dados pessoais devem referir-se a pessoa singular identificada ou identificável**. A natureza pessoal dos dados condiciona a sua proteção por parte da ordem jurídica, pelo que parecem ficar excluídos do âmbito de tutela desta disposição os elementos de informação que permitem identificar pessoas coletivas (em consonância com o âmbito de aplicação subjetivo da Diretiva n.º 95/46/CE que

deixa claro que: "... as regras relativas à proteção das pessoas jurídicas em relação ao tratamento de dados que lhes digam respeito não são objeto da presente Diretiva). Em Espanha, a questão coloca-se em moldes paralelos. A doutrina maioritária mostra-se a favor do reconhecimento deste direito em relação às pessoas coletivas, mas esta não tem sido a posição do Tribunal Constitucional desse país, que não só entende que está em causa um direito que supõe um substrato pessoal e físico de que a pessoa coletiva não dispõe, como considera que essa interpretação não é possível face aos termos em que a lei de proteção de dados está formulada e que refere expressamente, tal como a nossa, os direitos da pessoa física (veja-se, entre outros, MÓNICA RAMIRO, *El Derecho Fundamental a la Protección*, *ob. cit.*, pág. 459). Entre nós, entendem GOMES CANOTILHO e VITAL MOREIRA (*Constituição*, I, pág. 558) que o princípio interpretativo que permite conceder às pessoas coletivas os direitos e deveres compatíveis com a sua natureza (consultar ainda anotação ao artigo 12.º) só pode funcionar nos casos previstos pelo n.º 1 desta disposição, uma vez que aí não se refere expressamente a natureza pessoal dos dados, falando-se apenas de "dados informatizados".

IX – Por outro lado, **o âmbito de tutela constitucional não se refere apenas aos elementos capazes de identificar diretamente o cidadão, mas também aos elementos que o permitam fazer por via indireta, tornando-o identificável**. Neste sentido, são interessantes as decisões do Tribunal Constitucional espanhol (STC 20/1992, de 14 de fevereiro) relativamente à publicação de uma noticia num jornal de Palma de Mallorca onde se dava conta que dois arquitetos da cidade estavam infetados com o vírus da SIDA, e onde, apesar de não se proceder à identificação dos nomes, se usavam as iniciais das pessoas em causa como meio de referência, tendo o tribunal entendido que houve uma identificação indireta, mas apesar de tudo inequívoca, de determinadas pessoas como infetadas pelo vírus, ou a decisão do TEDH (25 de fevereiro de 1995) onde se valorou a divulgação no âmbito de um processo judicial, e sem consentimento do demandante, do seu historial clínico, incluindo o resultado de uma análise de HIV positivo, tendo-se considerado que uma tal forma de proceder violava as garantias fundamentais da pessoa no domínio da tutela de dados pessoais, e a decisão do Tribunal de Estrasburgo que condenou a difusão de imagens através de circuitos de videoconferência onde o demandante surgia atravessando a rua de faca na mão depois de tentar cortar as veias. A cara do demandante encontrava-se oculta, mas essa ocultação foi tida como inadequada, porque o penteado e o bigode o tornavam reconhecível a todos os que o conhecessem.

X – Quando se pergunta do conteúdo efetivo deste direito, e das faculdades ou poderes que integra, tem que se começar por ter presente a realidade que se pretende regular, e **os riscos que o uso desenfreado dos meios informáticos na manipulação da informação pessoal envolve para os direitos e liberdades individuais**. O alargamento das possibilidades de recolha e de armazenamento de dados relativos ao cidadão individual por parte de entidades privadas e poderes públicos, e a facilidade e a velocidade de acesso e de cruzamento de todos esses dados, tornam mesmo justificado o receio da construção de um *Big Brother* no mais puro sentido *orwelliano* (designadamente onde está em causa a concentração de informação pelo Estado). É que, não só existe o risco de uma recolha injustificada de dados suscetível de constituir por si só uma intromissão ilegítima na vida privada das pessoas e uma compressão das suas liberdades (não tanto pela sua natureza, como pela desnecessidade ou natureza infundada dessa recolha), como o uso e divulgação sem limites desses dados pode gerar desigualdades de tratamento e riscos de exclusão. Tendo também que se ponderar e prevenir o perigo, que foi acautelado autonomamente pelo n.º 5 desta disposição,

de se conseguir obter, através da articulação de sistemas informativos e elementos de informação constantes de vários ficheiros, uma imagem completa da pessoa capaz de identificar todos os seus movimentos, os seus bens, as suas doenças, as suas crenças, em suma, todos os espaços mais recônditos da sua vida privada e pessoal.

XI – O direito que é consagrado no artigo 35.º é, em primeiro lugar, **um direito de defesa e um direito de liberdade com um conteúdo negativo** *(Abwehrrecht)* na medida em que permite ao indivíduo decidir quem, quando, e em que condições, poderá usar, ou tornar pública, informação que lhe diz respeito, o que significa a possibilidade de não revelar dados de natureza pessoal, ou de recusar o tratamento dessa informação em certas circunstâncias. Está em causa a tutela da reserva sobre factos cujo conhecimento por terceiros deve depender da decisão do seu titular, independentemente de respeitarem ao núcleo mais estrito da sua vida privada ou de serem inócuos sob esse ponto de vista, e independentemente mesmo de poderem ser muito bem valorados pela opinião pública (De Cupis dava, a propósito, o exemplo da figura pública que faz sacrifícios para manter um filho num colégio particular, ou que pratica atos de benemerência), e que fica garantida através de uma omissão ou de um *non facere* (pode-se falar de uma *proibição de ingerência* do Estado relativamente a dados informativos que pertencem originariamente ao cidadão).

XII – Mas o mesmo direito faz-se necessariamente acompanhar por faculdades de decisão e de atuação relativamente aos dados pessoais, do poder de supervisionar essa informação, prevenindo e corrigindo lesões da liberdade individual, o que constitui inequivocamente uma dimensão positiva deste direito (Agostinho Eiras, *Segredo de Justiça e Controlo de Dados Pessoais Informatizados*). São estas **faculdades e poderes de natureza positiva** que o legislador constitucional consagrou expressamente, e que, de uma forma sucinta, se reconduzem ao direito de acesso e de retificação e cancelamento dos dados, ao direito ao sigilo sobre eles, ao direito de não tratamento de certos dados, e à proibição da criação de um número único de cidadão capaz de permitir o acesso e a manipulação de toda a informação sobre uma determinada pessoa através de um só número de identificação, que constituem os direitos fundamentais em matéria de defesa contra o tratamento informatizado de dados pessoais (fala-se mesmo em relação a eles de um verdadeiro *Habeas Data* ao constituírem garantia de uma liberdade de natureza fundamental dos tempos modernos), muito embora possam sofrer limitações de conteúdo em determinadas situações, e sob determinados pressupostos (expressão artística ou literária, finalidades estatísticas, segurança do Estado, entre outras).

XIII – Antes de nos referirmos com mais detalhe ao conteúdo destes direitos, cabe ainda dizer que **o exercício da liberdade consagrada neste artigo supõe uma prestação normativa por parte do Estado, vincula-o a tomar medidas legislativas para a realização plena da autodeterminação da pessoa em face do uso da informática, autodeterminação que vale plenamente quer perante entidades públicas, quer perante entidades privadas com força económica e social equiparável** (o que se designa por eficácia horizontal, ou *Drittwirkung*, dos direitos fundamentais cfr., sobre esta temática, anotação ao artigo 18.º).

XIV – O artigo 35.º contém assim uma **imposição legiferante** ao estabelecer expressamente que a tutela dos cidadãos relativamente à utilização da informática e o conteúdo dos seus direitos será definida pela "lei e nos termos da lei". É à lei, mais precisamente à Lei n.º 67/98, de 26 de outubro, que veio assegurar a transposição da Diretiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de

1995, sobre dados pessoais, que cabe a definição das condições de legitimidade para a recolha e tratamento de dados e os fundamentos para a limitação do direito de acesso e de informação do cidadão relativamente aos seus dados pessoais, o esclarecimento sobre as atribuições e competências da "entidade administrativa independente" a que se refere o n.º 2, do artigo 35.º, em suma, toda a regulamentação dos mecanismos através dos quais se torna possível o exercício da liberdade informacional constitucionalmente consagrada, muito embora a relação entre a lei e o texto do artigo 35.º da Constituição não seja totalmente pacífica dados os termos bastantes detalhados em que a Constituição regulou este direito (Bacelar de Gouveia, *Os Direitos Fundamentais*, págs. 714 e segs.; referindo, noutro sentido, a falta de densificação da disciplina legislativa em relação a certos pontos ou aspetos, como, por exemplo, onde se trata da definição do conceito de dados pessoais, Gomes Canotilho/Vital Moreira, *Constituição*, I, pág. 553).

XV – A Diretiva n.º 95/46 do Parlamento Europeu e do Conselho de 24 de outubro de 1995, surgiu pela necessidade de garantir a harmonização das legislações nacionais dos Estados-membros em relação à tutela dos direitos fundamentais no âmbito do tratamento de dados de natureza pessoal como forma de evitar que pelo desencontro legislativo dos vários países se inviabilizasse ou impedisse a plena integração económica europeia. A livre circulação de mercadorias, pessoas, serviços e capitais implica também a **livre circulação de dados**, quer por exigência do sector económico privado quer da cooperação administrativa científica e técnica entre países, e foi com este objetivo unificador que entrou em vigor a Diretiva n.º 95/46 cujo artigo 25.º contém uma série de princípios-base sobre a transferência de dados no quadro da UE. Assim, a cedência dos dados terá que estar de acordo com o direito nacional do Estado cedente, e só pode ser realizada quando o país que os recebe assegure um nível de garantia suficiente em relação a eles, sendo de atender nesta decisão à natureza dos dados que estão em causa, à finalidade e duração do tratamento previsto, ao país de origem e país de destino, ao direito vigente no país de destino e às medidas de segurança aí adotadas. No entanto, o artigo 26.º da mesma Diretiva estabelece uma série de restrições à regra geral prevista por este artigo 25.º Mesmo que o país de destino dos dados não lhes garanta proteção adequada, a cedência pode ter lugar sempre que esse país respeite de forma suficiente a vida privada e os direitos e liberdades fundamentais da pessoa, sempre que o titular dos dados tenha dado consentimento, quando exista um interesse vital do interessado, e numa série de outras situações que não parecem ter todavia um grau suficiente de determinabilidade jurídica tendo em conta a importância dos interesses em causa (Lucrecio Rebollo Delgado, *Derechos Fundamentales y Protección de Datos*, Madrid, 2004, págs. 137 e segs.; veja-se também sobre a evolução da legislação comunitária sobre a proteção de dados, Maria del Cármen Guerrero Picó, *El Impacto del Internet en el Derecho Fundamental a la Protección de Datos de carácter Personal*, Navarra, 2006).

XVI – Esta Diretiva, como a Lei de Proteção dos Dados Pessoais que a transpôs, concretizando o imperativo constitucional do artigo 35.º, n.º 2, condicionam a legitimidade da recolha dos dados pessoais à finalidade para a qual têm lugar, exigindo que se trate de uma finalidade previamente determinada, explicita e constitucionalmente legítima, não podendo estes dados vir a ser tratados num momento posterior de forma incompatível com essa finalidade [artigo 5.º, alínea *b*), da Lei]. O **conceito de "finalidade incompatível"** que é aqui utilizado não tem, todavia, um significado muito claro, pelo que, usando um argumento *a contrario*, poder-se-ia entender que os dados só não poderiam ser usados para finalidades incompatíveis, avessas, ou de todo em todo contrárias aquela para a qual tivessem sido inicialmente obtidos. No entanto, é duvidoso se esta interpretação é a mais razoável, ou se não se poderá atribuir a este

critério um sentido mais amplo através da associação dos conceitos e dos conteúdos previstos pela Diretiva n.º 46/1995, de 24 de outubro, e pela Lei de Proteção de Dados Pessoais. Esta não é a posição seguida em Espanha, por exemplo, por ISABEL CECILIA VASQUEZ, *Protección de Datos: Cuestiones Constitucionales y Administrativas (el derecho a saber y la obligación de calar)*, Pamplona, 2007, pág. 327, que considera que existe "compatibilidade" com o fim da recolha sempre que os dados são usados para fins históricos, estatísticos ou científicos, ou para garantir o exercício das funções próprias da Administração Pública no âmbito das suas competências. Entre nós, e uma vez que a nossa Lei exige que a colheita dos dados se deixe relacionar com uma finalidade explicita e determinada, fazendo depender a incompatibilidade do seu uso com essa finalidade especifica, não nos parece que a interpretação a dar ao conceito de "incompatível" possa ser tão permissiva, muito embora no que se refere ao uso dos dados para finalidades estatísticas, históricas e de investigação científica, essa conclusão se deixe legitimar pelo disposto no artigo 10.º, n.º 5, relativamente ao afastamento do direito à informação do titular dos dados.

XVII – **A recolha de dados deve servir uma finalidade constitucionalmente legítima, deve ser idónea ao cumprimento dessa finalidade, deve ser necessária, no sentido de que não deve existir medida mais moderada capaz de atingir a mesma finalidade com menor sacrifício, e deve ainda ser proporcional**, decorrendo dela mais benefícios e vantagens do que prejuízos para outros bens ou valores em conflito (proporcionalidade em sentido estrito). Resulta ainda da necessária vinculação dos dados informáticos a uma finalidade explícita e definida, a *proibição de armazenamento de dados*, uma vez que esse armazenamento significa que deixou de existir uma finalidade clara ou específica, pese embora se possa admitir o depósito de informação mediante autorização da CNPD estando em causa o cumprimento de objetivos de natureza estatística (em todo o caso, e essa será uma das razões que permite que o tratamento estatístico de dados mereça um tratamento diferenciado a vários níveis, trata-se sempre da utilização de dados de forma anónima e não individualizada).

XVIII – **O princípio do consentimento ou da autodeterminação** é a pedra angular sobre a qual se estrutura o tratamento dos dados pessoais [artigos 3.º, alínea *h*), e 6.º da Lei n.º 67/98, de 26 de outubro, e artigo 7.º, alínea *a*), da Diretiva n.º 95/46/CE, de 24 de outubro de 1995]. Certo que não é a vontade do titular dos dados que define o nível de proteção a que eles ficam sujeitos, dependendo a proteção outorgada a cada tipo ou categoria de dados da vontade do legislador (atenda-se ao n.º 3 do artigo 35.º da Constituição, e à regulamentação específica a que são sujeitos os dados referentes à saúde dos cidadãos e dados genéticos, Lei n.º 12/2005, de 26 de janeiro) mas existe uma relação necessária entre o consentimento e a licitude da recolha e tratamento dos dados que apenas poderá ser afastada ou derrogada nos casos particulares previstos na lei [há, no entanto, quem entenda que o consentimento não constitui o critério principal da legitimidade da recolha de dados, sendo antes uma condição dessa recolha, de valor equivalente ou equiparado ao das restantes circunstâncias, previstas pelo artigo 6.º, alíneas *a*), *b*), *c*), *d*) e *e*), da Lei de Proteção dos Dados Pessoais, e pelo artigo 7.º, alínea *b*), da Diretiva e que, de uma forma geral, se referem à prossecução de interesses legítimos, missão de interesse público, defesa de interesses vitais do titular dos dados não estando ele em condições de prestar o seu consentimento, e cumprimento de uma obrigação legal].

XIX – É reconhecido aos cidadãos o **direito de acesso** aos dados e registos informáticos que lhes dizem respeito, que a partir da Revisão Constitucional de 1997 (artigo

35.º, n.º 6) passou a estender-se à rede informática de natureza pública (para uma definição de rede informática confira-se o artigo 2.º da Lei n.º 109/91, de 17 de agosto, sobre *Criminalidade Informática*) regulado nos termos do artigo 11.º da Lei n.º 67/98, de acordo com as exigências impostas pelo artigo 12.º da Diretiva n.º 95/46/CE.

Além do direito de acesso, o titular dos dados tem o **direito de retificação, bloqueio ou apagamento** de dados [artigo 11.º, n.º 1, alínea *d*), da Lei, e artigo 12.º da Diretiva] e **o direito de atualização** de todos os elementos de informação que lhe dizem respeito.

Todos estes direitos supõem a existência de um **direito a ser informado** sobre a obtenção dos dados e sobre a "finalidade" a que se destinam, devendo o responsável pelo tratamento dos dados ou o seu representante informar a pessoa de quem recebe os dados da sua identidade, da finalidade ou objetivo pretendidos e dos destinatários dos dados.

XX – Relativamente às restrições ao direito de acesso e de informação dos cidadãos sobre os seus dados pessoais, elas foram reguladas em pormenor pela Diretiva n.º 95/46/CE e pela Lei de Proteção de Dados Pessoais, contando-se entre as causas mais relevantes de limitação destes direitos a **segurança do Estado** (tenha-se em conta o disposto no artigo 137.º, n.º 2, do Código de Processo Penal que estabelece que "o segredo de Estado a que se refere o presente artigo abrange, nomeadamente, os factos cuja revelação, ainda que não constitua crime, possa causar dano à segurança, interna e externa, do Estado português, ou à defesa da ordem constitucional) e a **prevenção ou investigação criminal.** Admite-se também que o dever de informação cesse onde o seu cumprimento envolva um esforço excessivo ou desproporcionado, estando em causa o uso dos dados para finalidades estatísticas, históricas ou de investigação científica (artigo 10.º da Lei).

XXI – Importa fazer neste contexto uma referência ao **Acordo de *Schengen* de 14 de junho de 1985**. A livre circulação de pessoas e a abolição de fronteiras dentro do espaço europeu veio criar uma série de exigências em termos de segurança que redobraram de intensidade a partir do ataque terrorista do 11 de setembro. O Acordo de *Schengen* (complementado pela sua Convenção de aplicação de 19 de junho de 1990) que Portugal subscreveu em 1991, teve por objetivo fazer acompanhar essa abertura de fronteiras e a livre circulação de pessoas no espaço interno europeu de um sistema de segurança capaz de controlar o cruzamento das fronteiras, de dar resposta aos pedidos de asilo, e de concretizar a cooperação policial e judicial penal, instituindo também um sistema de informação comum: o Sistema de informação *Shengen* (SIS). Este sistema de informação *Schengen* (SIS) que se destina a assegurar o intercâmbio de dados relativos à identidade das pessoas e a objetos procurados é composto de duas partes: uma unidade nacional em cada um dos Estados-membros (N-SIS), e um sistema central ao qual se encontram ligadas as unidades informativas nacionais (C-SIS). Esta rede informática é completada por uma outra rede (SISNET) que é um suplemento de informação solicitado à entrada nacional e que integra elementos sobre a imigração.

XXII – O **sistema de redes informáticas *Shengen*** congrega informação relativa a pessoas procuradas para detenção para efeitos de extradição, a pessoas desaparecidas, a pessoas cuja presença e circulação é proibida no espaço *Schengen*, entre outra, apenas sendo permitido o registo de certos dados, que nunca poderão ser os dados de natureza sensível previstos pelo artigo 6.º da Convenção n.º 108 do Conselho da Europa, estando o seu tratamento e transmissão sujeitos a princípios estritos de confidencialidade, de exatidão, atualidade, licitude, limitação temporal e adequação ao fim prosseguido. A Convenção de aplicação *Schengen* também criou a autoridade

de Controlo Comum *Schengen* (ACCS) que está encarregada de verificar se o sistema informativo *Schengen* cumpre as regras aplicáveis ao uso de dados pessoais, muito embora as suas competências sejam bastante limitadas. Não se prescindiu todavia, em toda esta matéria, de uma regulamentação mais concreta e detalhada por parte dos Estados-membros (veja-se, entre nós, a Lei n.º 2/94, de 19 de fevereiro, que cria o centro de dados que serve o Sistema *Schengen*), muito embora nem mesmo em relação a estes dados se tenha excluído por completo os direitos de acesso e de informação do seu titular, devendo, no entanto, esse acesso ter lugar através da autoridade nacional de controlo (CNPD), que quando entenda (artigo 11.º da Lei de Proteção dos Dados Pessoais) que a sua comunicação pode prejudicar a segurança do Estado (conferir de igual modo o artigo 23.º da Lei de Proteção de Dados Pessoais que confere ao CNPD funções de representação e fiscalização no âmbito do sistema *Schengen* e *Europol*), ou estando em causa a necessidade de prevenir e punir a prática de crimes, designadamente de formas particularmente violentas de crime organizado e terrorismo, pode recusá-lo.

XXIII – No contexto da análise do quadro legal da cooperação entre os Estados-membros no domínio da luta contra o terrorismo, a criminalidade transfronteiras e a imigração ilegal, assume um papel muito importante o **Tratado de *Prümm***, que foi assinado em 27 de maio de 2005 em *Prümm* na Alemanha entre vários Estados-membros. Este Tratado regula o intercâmbio de informações sobre ADN, impressões digitais, registo de veículos e dados pessoais e não pessoais no âmbito da cooperação transfronteiriça entre as Partes Contratantes, revelando a transposição do seu regime para o quadro jurídico da UE bastantes semelhanças com o que se passou a este nível com o "acervo de *Schengen*". O seu objetivo consiste na intensificação das trocas de informações entre autoridades e será alcançado pela comparação entre um determinado perfil de ADN e os perfis registados em bases automatizadas existentes nos Estados-membros, através de pontos de contacto nacionais. Toda esta matéria é regulada entre nós pela Lei de Proteção dos Dados Pessoais, designadamente pelos seus artigos 8.º, 9.º, 10.º, n.º 5, e 11.º, n.º 4, e pelo artigo 7.º, uma vez que se trata de dados de natureza sensível, e por sua vez pela Lei n.º 12/2005, de 26 de janeiro, sobre Informação Genética Pessoal e Informação de Saúde. Sobre a criação da base de dados de perfis de ADN para fins de investigação civil e criminal, requisitos de legitimidade da recolha de amostras, marcadores de ADN admitidos para efeitos de análise da amostra, ficheiros que integram a base de dados de perfis de ADN, tratamento e conservação da informação recolhida em ficheiro informático, direitos das pessoas envolvidas, fiscalização da base de dados, veja-se a Lei n.º 5/2008, de 12 de fevereiro [em particular, no que diz respeito ao exercício dos direitos de informação e acesso, confiram-se os artigos 9.º e 17.º, n.º 3, alínea *b*)].

XXIV – Toca-se também aqui a difícil problemática do **segredo de justiça**, regulado nos artigos 86.º e segs., do Código de Processo Penal e cujo regime sofreu uma alteração substancial com a entrada em vigor da Lei n.º 48/2007, de 29 de agosto. Esta modificação legislativa que já foi designada como uma verdadeira *revolutio* do processo penal (Paulo Pinto de Albuquerque, *Comentário do Código de Processo Penal*, 2.ª ed., Lisboa, 2008, anotação ao artigo 86.º, n.º 2, pág. 239) veio inverter a regra vigente em matéria de publicidade no processo penal português, cuja fase de investigação deixou de ser, por princípio, secreta, para passar a ser abrangida pela regra inversa da publicidade interna e externa. Assim, enquanto no momento anterior à entrada em vigor da lei de revisão do CPP, o segredo de justiça apenas cessava a partir da decisão instrutória ou do requerimento para abertura de instrução, ou, não tendo lugar um e outro, a partir do momento em que a instrução deixava de poder ser requerida, no momento

atual, quer o inquérito, quer a instrução são fundamentalmente públicos, incluindo a publicidade externa a possibilidade da assistência do público aos atos processuais praticados no decurso dessas fases. No entanto, nem por isso deixa de interessar a referência aqui a dados ou elementos abrangidos pelo segredo, porque ele não deixou de existir por completo, continuando a valer, nos termos do artigo 86.º, n.º 7, relativamente aos elementos que dizem respeito à reserva da vida privada das pessoas que não constituam meios de prova, devendo o juiz especificar quais são, ordenando, se for caso disso, a sua destruição ou entrega à pessoa a quem dizem respeito, e sempre que, por determinação do Ministério Público (artigo 86.º, n.º 3), ou a requerimento do arguido, ou do assistente, ouvido o Ministério Público, e no interesse daqueles, o juiz de instrução decida pela sua manutenção relativamente aos elementos que constam do processo. Deixando de lado a intrincada questão de saber se a amplitude com que o legislador consagra atualmente a publicidade interna e externa do processo é constitucional, ao desequilibrar a balança entre a liberdade informacional e o interesse no regular e eficaz desenvolvimento da investigação que constitui o fundamento do próprio inquérito (aceitando abertamente a inconstitucionalidade, Paulo Pinto de Albuquerque, *Comentário*, anotação ao artigo 86.º, n.º 5, pág. 240; pronunciando-se a favor da existência de segredo na fase de investigação, sujeito todavia a prazos limitados de duração, Germano Marques da Silva, *Curso de Processo Penal*, III, Lisboa, 2009, pág. 105) parte-se da aceitação de que podem existir dados de natureza pessoal cobertos pelo segredo de justiça, pelo que não podem ser exercidos em relação a eles os direitos de informação e de acesso previstos em geral pela Constituição e pela lei.

XXV – Neste caso, e uma vez que a decisão sobre a existência do segredo dependerá sempre da ponderação das circunstâncias do caso concreto por parte do Ministério Público (validada pelo juiz de instrução), ou por parte do juiz de instrução, não estando já em causa numa proibição geral e abstrata de publicidade, parecerá que quaisquer limitações que daí advenham para o direito de acesso e de informação acerca dos dados pessoais constantes do processo para o seu titular, terão sido já devidamente pesadas, não existindo grande justificação para as considerar desadequadas ou contrárias à lei. No entanto, **não sendo de aceitar que o segredo de justiça valha sempre como sinónimo de proibição abstrata e absoluta de conhecimento de toda a informação constante do processo**, caso, por exemplo, o titular dos dados queira saber posteriormente à decisão sobre a restrição da publicidade se está bem identificado no processo, não parece haver razões suficientes para lhe negar o acesso a esses dados, uma vez que não resulte daí qualquer prejuízo para a investigação e para a realização da justiça penal. Tudo ficando dependente, em suma, da valoração do caso concreto, da natureza da informação a que o titular dos dados pretende ter acesso, do tipo de processo em causa, e do prejuízo que o exercício desses direitos pode envolver para a efetivação da justiça.

III

XXVI – O artigo 35.º, n.º 3, da Constituição conferiu autonomia aos chamados "*dados sensíveis*", a que por sua vez se refere o artigo 7.º da Lei de Proteção de Dados Pessoais e o artigo 8.º da Diretiva n.º 95/46/CE, de 24 de outubro de 1995. São considerados **dados sensíveis** os elementos de informação cujo tratamento informático além de poder contender com a privacidade do seu titular, pode dar origem a tratamentos desiguais ou discriminatórios, pelo que, em princípio, o seu tratamento é proibido. No entanto, e em nome de um interesse público importante, podem justificar-se derrogações a essa proibição, em domínios como a segurança social e a saúde pública

(para garantir a qualidade e a rentabilidade dos serviços prestados, e em ordem a regularizar e a controlar os pedidos de prestações; em relação à informação genética pessoal e informação de saúde, incluindo os dados de informação médica, atente-se ao regime estabelecido pela Lei n.º 12/2005, de 26 de janeiro) desde que se garanta que não haverá lugar a discriminação com base nesses dados (e que serão cumpridas as medidas de segurança previstas pelo artigo 15.º da Lei de Proteção de Dados) e que a recolha se encontra estritamente vinculada (mais ainda do que a dos dados ditos "normais") ao cumprimento de finalidades determinadas por parte da entidade que procede à recolha. A ponderação de interesses que aqui se faz poderá permitir a recolha destes dados estando ainda em causa finalidades de investigação científica e de estatística pública, o exercício de atividades de índole eleitoral que podem justificar a recolha de dados sobre a opinião pública das pessoas, a consecução de finalidades de natureza constitucional por parte de associações religiosas oficialmente reconhecidas, entre outras. A Lei impõe ainda que a recolha e o tratamento informático destes dados seja precedida de disposição legal ou autorização prévia pela CNPD, a não ser que o titular do interesse tenha prestado o seu consentimento expresso nos termos previstos pelo artigo 3.º De acordo com esta disposição, é considerado consentimento "qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados pessoais sejam objeto de tratamento".

XXVII – Também **são dados de natureza sensível os dados relativos ao comportamento criminal do cidadão**. De acordo com o artigo 8.º da Lei de Proteção de Dados *(suspeitas de atividades ilícitas, infrações penais e contraordenações)* apenas é permitida a criação e manutenção de registos centrais relativos a pessoas suspeitas de atividades ilícitas, infrações penais, contraordenações e decisões que apliquem penas, medidas de segurança, coimas e sanções acessórias por parte de serviços públicos com competência específica prevista na respetiva lei de organização e funcionamento, observando normas procedimentais e de proteção de dados previstas em diploma legal, com prévio parecer da CNPD (os responsáveis pelo tratamento destes dados devem observar medidas especiais de segurança nos termos do artigo 15.º da mesma Lei, enumerando este artigo uma série de mecanismos de controlo que em certos casos podem ser dispensados pela CNPD, onde a natureza das entidades responsáveis pelo tratamento, e o tipo das instalações em que é efetuado o tratamento dos dados o permita, e garantindo sempre o respeito pelos direitos, liberdades e garantias dos titulares dos dados.). Esta matéria encontra-se regulamentada pela Lei n.º 57/98, de 18 de agosto, que define quais os elementos que podem constar do registo criminal dos cidadãos e que decisões estão sujeitas a ele, quem é o responsável pela base de dados de identificação criminal e a quem cabe garantir os direitos de informação, retificação e acesso em relação a ele, e quem pode aceder a essa informação e em que termos. Também são dados de informação sensível referentes ao comportamento criminal do cidadão, os dados que resultam da análise de amostras de material biológico obtido em processo-crime, a pedido do arguido, ou ordenada oficiosamente ou a requerimento, por despacho do juiz a partir da constituição de arguido, ao abrigo do disposto no artigo 172.º do CPP (artigo 8.º, n.º 1, da Lei n.º 5/2008, de 12 de fevereiro), ordenadas mediante despacho do juiz de julgamento, e após trânsito em julgado, em condenado por crime doloso com pena concreta de prisão igual ou superior a 3 anos, ainda que tenha sido substituída (artigo 8.º, n.º 2), ou em arguido declarado inimputável a quem tenha sido aplicada medida de segurança nos termos do artigo 91.º do Código Penal, não tendo havido recolha de amostra segundo o n.º 1 deste artigo 8.º (artigo 8.º, n.º 3). Os perfis de ADN obtidos a partir da análise das amostras colhidas nos termos dos n.os 2 e 3 do artigo 8.º [artigo 15.º, n.º 1, alínea *e*)] são eliminados na mesma data em

que se venha a proceder ao cancelamento definitivo das respetivas decisões no registo criminal [artigo 26.º, n.º 1, alínea *f*)].

IV

XXVIII – De acordo com o artigo 35.º, n.º 4, da Constituição **é proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais**.

O acesso ilícito a dados pessoais determina a responsabilidade civil do infrator a efetivar nos termos gerais (artigos 34.º da Lei da Proteção de Dados Pessoais e artigos 483.º e segs. do CC) e pode ainda originar a responsabilidade penal do agente de acordo com o artigo 44.º da *Lei de Proteção dos Dados Pessoais*, em todos os casos de acesso não autorizado a dados pessoais que tenham sido objeto de tratamento informático lícito (prisão até um ano ou multa até 120 dias), e nos termos do artigo 193.º do Código Penal (cujo conteúdo de regulamentação foi deliberadamente reduzido pela Revisão de 1995 em ordem a evitar a sua sobreposição em relação aos crimes previstos nesta matéria pela *Lei da Proteção de Dados Pessoais*) onde esteja em causa o conhecimento de dados absolutamente insuscetíveis de registo informático, por isso mesmo, ilicitamente tratados, uma vez que este tipo legal incrimina o *tratamento e utilização* não autorizados de dados referentes ao núcleo irredutível da vida privada da pessoa. Como afirma Damião da Cunha, *Comentário Conimbricense do Código Penal, Parte Especial*, Tomo I, artigo 193.º, § 9, este tipo legal pode ter-se por preenchido onde a conduta do agente se dirige ao "acesso a um ficheiro automatizado cujo conteúdo é constituído por dados individualmente identificáveis respeitantes a determinados *items* absolutamente proibidos".

Pode colocar-se ainda a hipótese de um concurso entre a conduta prevista e punida pelo artigo 43.º da Lei de Proteção de Dados Pessoais *(Não cumprimento de obrigações relativas a proteção de dados)*, mais concretamente a omissão do pedido de tratamento de dados, e o artigo 193.º do Código Penal, uma vez que a partir da omissão dos deveres aí previstos, o tratamento dos dados passa a ser absolutamente ilícito, e a preencher a factualidade típica desta incriminação.

Também se pode colocar a hipótese de um concurso com eventuais crimes informáticos constantes da Lei n.º 109/91, de 17 de agosto, sobre criminalidade informática, que prevê e pune, no seu artigo 7.º, o acesso ilegítimo a um sistema ou rede informática. Todavia, a punição é aqui sempre colocada na dependência da intenção do agente de alcançar para si ou para terceiro benefício ilegítimo.

XXIX – Há que **distinguir o acesso por parte do "terceiro", das situações de comunicação ilegítima dos dados a "terceiro"**, que pode determinar a responsabilidade civil e criminal da entidade que procede ao tratamento dos dados. Os responsáveis pelo tratamento dos dados pessoais e as pessoas que no exercício das suas funções tomam conhecimento desses dados estão sujeitos a sigilo profissional, que permanece mesmo para além do termo das suas funções. De acordo com o artigo 47.º da Lei de Tutela dos Dados Pessoais, a violação desse sigilo, e a revelação de dados pessoais a terceiro, sem justa causa e sem consentimento do titular dos dados, constitui um ilícito criminal punível com pena de prisão ou multa, e suscetível de agravação nos termos do n.º 2, se se tratar de funcionário público ou equiparado, se tiver atuado com a intenção de obter um benefício ilegítimo, ou se puser em perigo a reputação, a honra e consideração ou a intimidade da vida privada de outrem.

XXX – A este propósito é interessante conferir o parecer que foi pedido à Comissão Nacional de Proteção de Dados (ParCC n.º 22/2001) relativo à **legitimidade da**

comunicação a terceiros de dados de natureza pessoal constantes da base de dados do recenseamento eleitoral, e que procede à articulação entre a proibição de acesso aos dados pessoais de terceiros e o princípio da finalidade a que também se refere o artigo 35.º da Constituição. Sobre este ponto, acabou por se considerar legítima a comunicação dos dados feita pelo STAPE a forças e serviços de segurança, organismos da Administração Pública e da Administração Local, sempre que demonstrassem existir uma autorização ou obrigação legal de comunicação, mas já onde fosse feita em relação a entidades/pessoas privadas (singulares ou coletivas), ou a outras entidades de natureza não administrativa, que apenas poderiam ter acesso à referida informação através de autorização excecional por parte da CNPD (admite-se aqui, a título pontual, o desvio da finalidade inicial).

XXXI – Há ainda que referir a possibilidade de **responsabilidade contraordenacional** prevista pelos artigos 35.º e segs. da Lei de Tutela dos Dados Pessoais, em todos os casos em que as pessoas ou entidades responsáveis pelo tratamento dos dados omitam obrigações de notificação à CNPD, prestem falsas informações, ou quando, depois de notificadas pela CNPD, mantenham as redes abertas a responsáveis por tratamento de dados pessoais que não cumpram os requisitos legais.

V

XXXII – Não poderíamos terminar esta anotação ao artigo 35.º, sem referir o seu n.º 5, que proíbe a **atribuição aos cidadãos de um número único capaz de concentrar toda a informação sobre a pessoa**, e que chegou a estar previsto na Lei n.º 2/73, regulada pelo Decreto-Lei n.º 555/73 de 26 de outubro (revogada, pelo menos na parte relativa a esta matéria, pela entrada em vigor da Constituição). A proibição da concessão de um número único ao cidadão capaz de constituir meio exclusivo de relacionamento com a Administração Pública constituiu uma novidade da Constituição de 1976, que foi sendo mantida ao longo das várias revisões constitucionais, muito embora se tenha reaberto a discussão em torno desta norma e da garantia que permite, a propósito da introdução do cartão de cidadão que reúne os três números determinantes da relação do cidadão com o Estado: o número fiscal de contribuinte, o número do bilhete de identidade e o número da segurança social. O cartão do cidadão cumpre com a norma constitucional uma vez que se trata de números distintos, e não existe interconexão dos dados disponíveis, apenas sendo possível a cada uma das entidades aceder à informação que lhe diz respeito, mas há quem considere que a manutenção de todos estes níveis de informação envolve custos injustificados para o Estado, e a diminuição da qualidade dos dados, pelo que haveria que abandonar a garantia prevista pelo n.º 5 do artigo 35.º da Constituição, procedendo à sua revisão e admitindo a junção de todos estes dados num só número. Parece-nos, no entanto, que a introdução do número único significa a possibilidade incontestada e legítima de construir uma imagem completa da pessoa pelo Estado, que conjugada com a possibilidade de localização espacial que já permitem as operadoras móveis, o uso da Via Verde, as redes de Internet, e do sistema SIBS, leva a temer a reprodução do mundo de ORWELL e a total perda da privacidade e de algumas liberdades básicas do cidadão, pelo que entendemos que esta garantia deve ser mantida (a este propósito, parece-nos particularmente relevante o direito do cidadão, consagrado no artigo 13.º da Lei n.º 86/98, de 26 de outubro, de não ficar sujeito a decisões jurídica e pessoalmente relevantes tomadas exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspetos da sua personalidade, designadamente a sua capacidade profissional, o seu crédito, a confiança de que é merecedor ou o seu comportamento)

XXXIII – Confira-se ainda, e a este propósito, o Decreto-Lei n.º 266/91, de 6 de agosto, sobre o **número fiscal**, que estatui que ele se destina ao uso exclusivo do tratamento de informação em matéria fiscal, respeitando absolutamente no que se refere às pessoas físicas, as normas constitucionais que proíbem a atribuição de um número nacional único. Para garantir o imperativo constitucional, evita-se a transcrição do número do bilhete de identidade para o suporte magnético que contém os dados fiscais, e, nos casos de homonímia prevê-se o recurso à consulta manual, o que torna fisicamente impraticável o cruzamento através de meios informáticos de informação com outros ficheiros que tenham como chave de identificação o número do bilhete de identidade do cidadão.

MARIA PAULA RIBEIRO DE FARIA