

## PARECER Nº 37/ 2006

O senhor Presidente da Comissão de Assuntos Constitucionais - Direitos, Liberdades e Garantias - da Assembleia da República solicitou à Comissão Nacional de Protecção de Dados (CNPD), requerendo a maior brevidade possível, a emissão de um parecer sobre a Proposta de Lei que cria o cartão do cidadão e rege a sua emissão e utilização.

Nos termos da alínea a) do nº 1 do artigo 23º da Lei de Protecção de Dados (Lei 67/98, de 26 de Outubro, designada apenas por LPD), a CNPD é competente para emitir o parecer solicitado.

A CNPD, cabe lembrar, integrou uma comissão inter-ministerial e inter-institucional criada para análise e estudo da criação e introdução do cartão do cidadão, quer do ponto de vista técnico, quer do ponto de vista jurídico, pedindo-se-lhe, em ambiente informal de trabalho, o seu contributo no que toca à protecção da privacidade e dos dados pessoais dos cidadãos, comissão que procedeu a duas reuniões preliminares e introdutórias. O passo seguinte a essas reuniões foi o pedido à CNPD, em 21 de Agosto, por Sua Excelência o Ministro da Administração Interna, para emissão de parecer sobre o projecto de proposta de lei relativo à mesma matéria, parecer que foi elaborado e emitido (Parecer nº 29/2006, de 6 de Setembro de 2006), não obstante, conforme se afirmou, a falta de informação suficiente para que a CNPD pudesse analisar as complexas questões técnicas e jurídicas levantadas por essa intenção legislativa.

A brevidade pedida pelo Senhor Presidente da Comissão de Assuntos Constitucionais foi totalmente atendida pela CNPD, apesar de ter estado condicionada pela superação de faltas de informação e por esclarecimentos necessários que a CNPD pediu lhe fossem prestados.

Cabe, então, emitir o parecer solicitado.

### I - Introdução

A criação do cartão do cidadão, com as características daquele que se visa criar com o projecto do diploma ora em estudo (reunindo, num único suporte documental, as informações de identificação pessoal e outras, relativas a quatro sectores que abarcam as quatro grandes áreas do sector público administrativo com as quais os cidadãos se relacionam, a saber, a identificação

civil, fiscal, de segurança social e de saúde), toca os fundamentos primeiros do Estado de Direito (democrático) - a dignidade da pessoa humana e a liberdade e autonomia dos cidadãos.

A dignidade da pessoa humana não é a dignidade de um ser ideal e abstracto, é a dignidade da pessoa concreta.<sup>1[1]</sup> *“O conceito de dignidade da pessoa humana obriga a uma densificação valorativa que tenha em conta o seu amplo sentido normativo-constitucional”.*<sup>2[2]</sup> É essa dignidade da pessoa humana que justifica a existência de garantias contra a obtenção e utilização abusivas de informações relativas às pessoas e às famílias, como aquela que se estabelece no artigo 35º da Constituição da República Portuguesa (CRP).<sup>3[3]</sup>

Diremos, então, que talvez não haja um direito à dignidade, mas antes é a dignidade humana a base de todo o direito. E a dignidade da pessoa evoca uma realidade intrínseca, específica de seres dotados de razão e de liberdade.<sup>4[4]</sup>

A liberdade é, pelo menos na inspiração republicana, não apenas a ausência de intrusão ou interferência, é também a ausência de dominação; liberdade é a disposição por parte dos indivíduos dos recursos e meios instrumentalmente necessários para concretizar os seus próprios planos de vida, o seu auto-governo e a sua auto-realização.<sup>5[5] 6[6]</sup>

Por isso, existe uma corrente que entende que os direitos fundamentais (ou os direitos humanos, no plano internacional) proclamados nas diversas Declarações e Cartas são basicamente direitos ligados à liberdade.<sup>7[7]</sup>

O Estado de Direito (democrático), a democracia ocidental é o regime da História que conferiu aos homens maior grau de liberdade política.<sup>8[8]</sup>

A democracia não é apenas um conjunto de garantias institucionais e procedimentais; ela é também *“a luta dos «sujeitos» na sua cultura e na sua liberdade, contra a lógica dominadora dos sistemas”*. O que é característico da *“sociedade moderna é que esta afirmação de liberdade se exprime sobretudo pela «resistência» à autoridade crescente do poder social sobre a*

---

<sup>1[1]</sup> Jorge Miranda, Rui Medeiros, “Constituição Portuguesa Anotada”, Tomo I, Coimbra Editora, Coimbra, 2005, pag. 53.

<sup>2[2]</sup> J. J. Gomes Canotilho e Vital Moreira, “Constituição da República Portuguesa Anotada”, 1º Volume, Coimbra Editora, Coimbra, 1984, pag. 70.

<sup>3[3]</sup> Jorge Miranda, Rui Medeiros, *ob. cit.*, pag. 54.

<sup>4[4]</sup> Salvador Vergés Ramirez, “Derechos y Libertades Hoy. Evolución y Progreso”, San Pablo, Madrid, 2000, pag. 10.

<sup>5[5]</sup> Félix Ovejero, José Luís Martí e Roberto Gargarella, “Nuevas Ideas Republicanas. Autogobierno y Libertad”, Paidós, Barcelona, 2003, pag. 21.

<sup>6[6]</sup> Para uma noção do indivíduo enquanto processo de construção no qual se cruzam circuitos de informações, em que a liberdade ganha valor de condição *sine qua non* da própria existência autónoma do sujeito, Ulrich Beck e Elisabeth Beck-Gernstein, “La Individualización - El Individualismo Institucionalizado y sus Consecuencias sociales y políticas”, Paidós, Barcelona, 2003.

<sup>7[7]</sup> Trazemos a título de exemplo Xabier Etxebarria Mauleon, na sua obra “Imaginário y Derechos Humanos desde Paul Ricoeur”, Instituto Diocesano de Teología y Pastoral Bilbao, Bilbao, 1995.

<sup>8[8]</sup> Maurice Duverger em diálogo com Olaf Palme, “A Crise da Sociedade Contemporânea”, Edições 70, Lisboa, pag. 120.

*personalidade e a cultura". "O poder do povo significa a capacidade de o maior número viver livremente, quer dizer, de construir a sua vida individual associando aquilo que se é e aquilo que se quer ser, resistindo ao poder em nome, ao mesmo tempo, da liberdade e da fidelidade a uma herança cultural."*

*" O regime democrático é a forma de vida política que dá maior liberdade ao maior número, que protege e reconhece a maior diversidade possível"<sup>9[9]</sup>*

Na relação da liberdade com a democracia, no contexto do Estado de Direito (democrático e social), foi realçado o perigo de, por cima dos cidadãos absorvidos no seu bem-estar, o Estado-Providência assumir a sua veste de Estado-Tutelar, que se encarrega de assegurar a felicidade dos cidadãos e velar pelo seu destino.

Um dos mecanismos de salvaguardar a liberdade, quer na perspectiva liberal de não sujeição dos cidadãos a interferências, quer na perspectiva republicana da ausência de *"dominação"*, consiste, precisa e respectivamente, na protecção da privacidade dos cidadãos e na protecção dos seus dados pessoais. Esta, a protecção dos dados pessoais dos cidadãos, funciona como um direito (fundamental) instrumental da protecção da privacidade, mas constitui simultaneamente um direito fundamental autónomo à autodeterminação informativa dos cidadãos.<sup>10[10] 11[11]</sup>

A CRP inaugurou o regime democrático constitucional com a consagração expressa no nº 3 do artigo 35º, dedicado à utilização da informática no que toca aos dados pessoais, da proibição da atribuição de um número nacional único aos cidadãos. Essa proibição mantém-se intacta até hoje.

A matéria do presente projecto, aqui em apreço, prende-se, desde logo, com o regime da protecção da privacidade e dos dados pessoais dos cidadãos e, de modo muito especial e sensível, com esta específica norma do actual nº 5 do artigo 35º da CRP que proíbe a atribuição de um número nacional único.

## II - Breve descrição da evolução histórica do cartão do cidadão

---

<sup>9[9]</sup> Alain Touraine, "O que é a Democracia?", Instituto Piaget, Lisboa, 1996, pag. 22 e 23.

<sup>10[10]</sup> Veja-se, sobre este assunto, Catarina Sarmento e Castro, "Direito da Informática, Privacidade e Dados Pessoais", Almedina, Coimbra, 2005, pag. 24.

<sup>11[11]</sup> Também o direito à privacidade pode aparecer como um direito fundamental instrumental cuja protecção assegura a protecção, num outro momento lógico e temporal, a protecção de outros direitos e liberdades fundamentais: Ricardo Martínez Martínez, "Una Aproximación Crítica a la Autodeterminación Informativa", Thomson Civitas, Madrid, 2004, pag. 28.

A intenção de concentrar a informação de identificação dos cidadãos num só documento é antiga, vindo, na doutrina, pelo menos desde 1936, preconizando-se, nessa altura, a atribuição de um número pessoal permanente e exclusivo.<sup>12[12]</sup>

Em 1972, a Câmara Corporativa explanava sobre as vantagens da atribuição de um número nacional único a cada cidadão, elencando, em suma, a da melhor avaliação das características demográficas para efeitos de planeamentos sectoriais (saúde, educação, segurança social, etc), a do incremento da eficiência da administração pública e a oferta aos cidadãos de maior comodidade nas suas relações com o Estado.

Não existia, para esta Câmara, qualquer risco de despersonalização dos indivíduos.

Estas foram as considerações que a Câmara Corporativa do Estado Novo teceu no parecer que deu à Lei 2/73, de 10 de Fevereiro, que instituiu o registo nacional de identificação baseado na atribuição de um número de identificação constituído por códigos numéricos significativos e uniformes, com carácter exclusivo e invariável, diploma que foi regulamentado pelo Decreto-Lei nº 555/73, de 26 de Outubro.

O Plano de Acção do Ministério da Justiça elaborado em Setembro de 1974, portanto, após a abertura à democracia trazida pela Revolução de 25 de Abril desse ano, ditou a suspensão daqueles dois diplomas legais até *“à definição legislativa das garantias jurídicas do sistema no que se prende às liberdades públicas e à defesa da privacidade, e isto porque tal projecto, com as características actuais, é antidemocrático”*.<sup>13[13]</sup>

A CRP de 1976 introduziu, expressamente no nº 3 do artigo 35º, a proibição da atribuição de um número nacional único aos cidadãos. Apesar de nos sucessivos debates parlamentares dedicados à utilização da informática e ao tratamento de dados pessoais essa norma ser recorrentemente estudada e discutida, essa proibição mantém-se intacta até hoje.

### III - A proibição constitucional da atribuição de um número nacional único

Foi, como se disse, logo na primeira versão do período constitucional que a CRP introduziu a norma proibitiva da atribuição a cada cidadão de um número nacional único. Os antecedentes históricos atrás sumariados ditaram essa proibição. A atribuição a cada cidadão, no Estado

---

<sup>12[12]</sup> Acta da Câmara Corporativa nº 121, disponível em [http://debates.parlamento.pt/r2/acc/shpg\\_acc.asp](http://debates.parlamento.pt/r2/acc/shpg_acc.asp)

<sup>13[13]</sup> Plano de Acção do Ministério da Justiça aprovado em Conselho de Ministros de 20 de Setembro de 1974.

autoritário anterior ao Estado democrático, de um número de identificação exclusivo e invariável, através de códigos numéricos significativos e uniformes, trazia associado o risco de permanente vigilância, de eliminação da autonomia e de perda da liberdade para os indivíduos.

A razão de ser da proibição de atribuição de um número nacional único a cada cidadão não é, porém, datada desse período histórico, da mudança de um regime autocrático para um regime democrático. *“Trata-se da proibição de um facto que merece continuar a ser proibido”*.<sup>14[14]</sup>

Por isso, não apenas a CRP de 1976 consagrou expressamente a proibição de atribuição de um número nacional único a cada cidadão, como essa proibição manteve-se intacta ao longo de todo o período democrático. Apesar das sucessivas alterações ao artigo 35º da CRP, onde a norma se insere, alterações decorrentes, também, da necessidade de adaptar o regime da utilização da informática sobre os dados pessoais à veloz dinâmica tecnológica e aos instrumentos normativos internacionais e comunitários vinculativos do Estado português, aquela proibição manteve-se intocável.

A consagração expressa da proibição de atribuição de um número nacional único a cada cidadão no Capítulo I (Direitos, Liberdades e Garantias Pessoais) do Título II (Direitos, Liberdades e Garantias) da CRP tem, também, uma significância que merece ser referida.

Em primeiro lugar, tendo em conta que todos os direitos fundamentais encerram um bem jurídico ou um valor que visam proteger, temos que a liberdade, ela própria, é o bem jurídico que esta norma do actual nº 5 do artigo 35º da CRP visa proteger.

Em segundo lugar, a consagração expressa, positivada, da proibição de atribuição de um número nacional único, desde 1976 até aos nossos dias, só pode significar a intenção de reforçar aquele direito fundamental material dos cidadãos de não verem a sua liberdade coarctada por meio da sua identificação pelos poderes públicos através de um número exclusivo e inalterável.

Em terceiro lugar, a inserção de uma regra proibitiva num campo - o dos direitos fundamentais - tipicamente ocupado por princípios<sup>15[15]</sup> significa um acréscimo de densificação normativa que, tanto deve introduzir uma maior protecção dos indivíduos face aos poderes públicos, vinculando o legislador no sentido dessa densificação, como deve servir de inspiração ao ordenamento jurídico

---

<sup>14[14]</sup> Diário da Assembleia da República de 12 de Maio de 1988 relativa à sessão de 27 de Abril de 1988, pag. 327, disponível em [http://debates.parlamento.pt/r3/dar\\_s2rc/shpg\\_dars2rc.asp](http://debates.parlamento.pt/r3/dar_s2rc/shpg_dars2rc.asp)

<sup>15[15]</sup> Sobre a distinção entre regras e princípios, designada e especificamente na área dos direitos fundamentais, Luís María Díez-Picazo, “Sistema de Derechos Fundamentales”, Thomson Civitas, Navarra, 2005, pag., 44.

na sua globalidade, criando um ambiente amistoso e respeitador do conteúdo e fim último dessa regra.

A proibição da atribuição de um número nacional único a cada cidadão tem, dentro da elevada precisão da sua fórmula, dois significados distintos mas complementares. Por um lado, proíbe-se a identificação directa dos cidadãos através de um número único e imutável, proibindo-se, assim, a eliminação da personalidade dos indivíduos e da sua dignidade humana, levando a que *“não se pode chapar na testa de um indivíduo que ele é o número 3 milhões”*<sup>16[16]</sup>. Por outro lado, proíbe-se a concentração da (tendencial) globalidade da informação atinente a um cidadão com uma única chave de acesso a essa informação, impedindo-se, também, que aquele mesmo resultado de despersonalização seja alcançado através da junção de toda a informação existente nas bases de dados do Estado e da possibilidade de compor uma imagem completa da pessoa<sup>17[17]</sup>.

Por isso, compreende-se que, sobretudo com a evolução tecnológica no campo da informática e com as crescentes potencialidades de recolha, manuseamento, cruzamento e conservação da informação, a proibição da atribuição de um número único a cada cidadão se tenha mantido expressamente prevista no capítulo dos direitos, liberdades e garantias pessoais da CRP, sendo o sentido dessa norma acrescido com a proibição de chegar ao mesmo resultado, mesmo sem número de identificação único e imutável, através da concentração da informação que permite moldar a totalidade da imagem dos cidadãos.

#### IV - A questão tecnológica e os princípios da prevenção, da precaução e da proporcionalidade

O direito à privacidade, na sua formulação de direito à *“privacy”*, é um direito fundamental fundacional dos direitos fundamentais, protector dos indivíduos face à actuação do Estado e dos poderes públicos.

O direito à protecção dos dados pessoais, enquanto liberdade de dispor sobre as informações pessoais concretizada na preservação da *“sua própria identidade informática”*<sup>18[18]</sup> é um direito fundamental de terceira geração.<sup>19[19]</sup>

Direito fundamental de terceira geração que surge num contexto novo, o da Sociedade da Informação, contexto que tanto pode revestir um papel libertador, como pode assumir um

---

<sup>16[16]</sup> Diário da Assembleia da República de 12 de Maio de 1988 relativa à sessão de 27 de Abril de 1988, pag. 327, disponível em [http://debates.parlamento.pt/r3/dar\\_s2rc/shpg\\_dars2rc.asp](http://debates.parlamento.pt/r3/dar_s2rc/shpg_dars2rc.asp)

<sup>17[17]</sup> Jorge Miranda, Rui Medeiros, *ob. cit.*, pag. 389.

<sup>18[18]</sup> Francisco Fernández Segado, “El régimen jurídico del tratamiento automatizado de los datos de carácter personal en España”, *Ius et Praxis*, Ano 3, nº 1, Talca (Chile), 1997, pag. 343, citado em Catarina Sarmiento e Castro, *ob. cit.*, pag. 28

<sup>19[19]</sup> Catarina Sarmiento e Castro, *ob. cit.*, pag. 28.

ambiente de dominação sobre os indivíduos. « *Si la période actuelle est marquée par de réels progrès de la démocratie constitutionnelle dans le monde, l'évolution liée à un changement technologique reste toujours ouverte* »<sup>20[20] 21[21]</sup>

Na verdade, a generalização da utilização das Tecnologias de Informação e Comunicação (TIC's), o crescente potencial de recolha, conservação e manuseamento da informação através destas tecnologias, a veloz evolução das características e desempenhos dessas tecnologias, estes são, sumariamente, factores que trazem alguma instabilidade ao consenso alcançado no "contrato social" no que respeita aos direitos fundamentais e ao papel do Estado e dos poderes públicos na protecção e promoção dos direitos, liberdades e garantias dos cidadãos.

Os novos desafios trazidos pelos direitos fundamentais de terceira geração apelam para um acompanhamento permanente da evolução daquelas características e daqueles desempenhos das TIC's e para um método partilhado e transparente ("governance") da informação existente e do processo decisório, levando à apreensão real das opções tomadas pelo Estado e pelos poderes públicos por parte dos destinatários e, assim, conduzindo à autêntica aceitação dessas decisões.

A introdução do cartão do cidadão que aqui nos ocupa, por conseguinte, recorrendo a novíssimas tecnologias que operam sobre a informação respeitante aos indivíduos, haverá de resultar de processos de decisão envolventes e participados pela comunidade científica, por forma a merecer o maior consenso possível na comunidade política.

Por outro lado, o processo decisório de introdução do cartão do cidadão haverá de tomar em linha de especial consideração os princípios jurídicos de particular relevo na sociedade de risco em que actualmente nos encontramos (princípios que ganham notoriedade em matéria ambiental, talvez a mais difundida das matérias da sociedade de risco, mas igualmente recomendados e aplicáveis à sociedade da informação): o princípio da prevenção (obstar ao surgimento de perigos e prejuízos que se antevêm como possíveis, ao invés de os reparar) e o

---

<sup>20[20]</sup> Stéphane Callens, "La «Société de L'Information»: Une Société de Surveillance?", em "La «Société de L'Information»: Entre Myths et Réalités", Coordenação de Michel Mathien, Bruylant, Bruxelas, 2005, pag. 295.

<sup>21[21]</sup> Sobre a Sociedade da Informação como uma sociedade de risco para os direitos fundamentais e para as liberdades públicas, pode também ver-se, entre muitos outros: Maria Eduarda Gonçalves, "Risk Society and the governance of innovation in Europe: opening the black box?", em Science and Public Policy, Volume 31, número 6, Dezembro de 2004, Beech Tree Publishing, Guildford (Inglaterra); Maria Eduarda Gonçalves, "Mudança Tecnológica, Conflito Social e Novos Direitos", em Cidadania, Administração Pública e Sociedade, INA, Oeiras; José Rodolfo Hernández-Carrión, "El marco de las TICs como potencial constrictor de espacios y libertades en favor de intereses corporativos y empresariales", em Derecho de la Sociedad de la Información nº 9 (dirigida por Santiago Cavanillas Múgica), "Libertades, Democracia y Gobierno Electrónicos", coordenado por Lorenzo Cotino Hueso, Editorial Comares, Granada, 2006, pag. 115; Ulrich Beck, "Risk Society. Towards a New Modernity", Sage, Londres, 1992.

princípio da precaução (na dúvida, podendo prever-se o surgimento de riscos e perigos efectivos, não prosseguir com a introdução da opção inovadora através das TIC´s).<sup>22[22]</sup> <sup>23[23]</sup>

Por fim, a questão tecnológica, ou seja, a utilização das TIC´s numa área de especial incidência sobre os direitos fundamentais dos cidadãos e alicerces do Estado de Direito - direito à privacidade e à protecção dos dados pessoais, enquanto direitos instrumentais face à protecção e promoção da dignidade da pessoa humana e da liberdade dos indivíduos, tal como a introdução de uma alteração tão profunda na forma e regime de identificação civil e sectorial dos cidadãos,<sup>24[24]</sup> a implicação dessa alteração com uma matéria tão sensível e cara ao regime democrático como é a proibição de um número nacional único a cada cidadão, os riscos incindíveis da utilização de tecnologias de elevado potencial concentracionário da informação (elevado potencial para coligir e processar) de desconhecidas repercussões e imprevisíveis consequências, tudo isto exige um apurado e exaustivo juízo de proporcionalidade.

Assim sendo e desde logo, importa relevar que a concentração da informação respeitante aos cidadãos e a intensificação do processamento dessa informação significa sempre, de *per sí*, não apenas um acréscimo dos riscos e perigos acima indicados, mas, antes disso, uma restrição dos direitos fundamentais à privacidade e à protecção dos dados pessoais ou à autodeterminação informativa. Desta forma, há que averiguar qual o direito fundamental dos cidadãos que se visa proteger e promover com o sacrifício imposto por esta restrição, sendo certo que esta restrição opera sobre os aspectos mais centrais dos núcleos e dos significados destes dois direitos fundamentais. Ora, no juízo de ponderação importa proteger e promover prioritariamente os direitos e liberdades fundamentais que vejam envolvidos nessa tensão os seus aspectos mais centrais do seu núcleo e significado.<sup>25[25]</sup>

Mas requer este juízo de ponderação, antes de tudo, que se reporte à actuação concreta através da qual a expansão/compressão dos direitos fundamentais é efectivamente concretizada, havendo, então, de aferir os proveitos concretos que essa tensão traz para os direitos fundamentais expandidos e quais os custos e sacrifícios que traz para os direitos fundamentais comprimidos.

---

<sup>22[22]</sup> Sobre os alcances destes princípios em matéria ambiental, totalmente transponíveis para a matéria das TIC´s na sociedade da informação aqui tratada, pode ver-se Maria Alexandra de Sousa Aragão, "O Princípio do Poluidor Pagador", *Studia Iurídica 23*, Coimbra Editora, Coimbra, 1997.

<sup>23[23]</sup> Iguais princípios recomendou a CNPD fossem observados no caso da adopção de meios electrónicos de votação em eleições políticas: Deliberação da CNPD sobre "Privacidade dos Eleitores no Voto Electrónico", pag. 17, disponível em [www.cnpd.pt/bin/orientacoes/Delib\\_voto\\_electronico.pdf](http://www.cnpd.pt/bin/orientacoes/Delib_voto_electronico.pdf).

<sup>24[24]</sup> A especial perigosidade para a democracia e para as liberdades dos indivíduos do relacionamento do registo centralizado de identificação civil com registos sectoriais, com o risco do "*controlo administrativo*" dos cidadãos, foi já aflorado por José António Barreiros, "Informática, Liberdades e Privacidade", em "Estudos sobre a Constituição - 1º Volume", Livraria Petrony, Lisboa, 1997, pag. 119 e ss.

<sup>25[25]</sup> Luíz Maria Díez-Picazo, *ob. cit.*, pag. 107 e ss.



Ora, a proposta aqui em estudo não traz consigo qualquer estudo que avalie o risco para a privacidade e para a protecção dos dados pessoais da introdução do cartão do cidadão, não traz qualquer estudo sobre os riscos e perigos efectivos para a segurança e fiabilidade do sistema de informação adoptado para tão grande mudança e concentração de informação, nem traz nenhum estudo que avalie o impacto positivo - o proveito para a segurança dos documentos de identificação, o proveito para o desempenho da Administração Pública e o proveito para os cidadãos - pretendidos com a introdução do cartão do cidadão.

Sem a prognose e análise exaustiva dos riscos e perigos decorrentes da introdução do cartão do cidadão nos termos e pelas vias propostas pela intenção legislativa e sem a prognose e análise do impacto positivo decorrente da introdução do cartão do cidadão, a viabilidade do indispensável juízo de proporcionalidade fica seriamente comprometida.

Neste domínio, os princípios da prevenção, da precaução e da proporcionalidade estão interligados. A ponderação à luz do princípio da proporcionalidade - ponderação da adequação, necessidade (indispensabilidade) e proibição do excesso - requer a prévia formulação dos princípios da prevenção e da precaução e o levantamento das questões que estes dois princípios suscitam nomeadamente através de exaustivos estudos de risco, por um lado, e de impacto, por outro, relativos à introdução do cartão do cidadão.<sup>26[26]</sup> <sup>27[27]</sup>

Passamos, de seguida, após estas considerações gerais e de enquadramento da Proposta de Lei em análise no Direito, ao estudo das normas concretas da Proposta com implicações na protecção

---

<sup>26[26]</sup> Um pouco mais à frente neste parecer voltaremos a esta questão, mas pode ser importante concretizar, já neste capítulo, o que entendemos por riscos concretos da introdução do cartão do cidadão. Por exemplo, o sistema de informação encontra-se sujeito a “ataques” informáticos e o próprio cartão é passível de clonagem. A avaliação dos riscos importaria a adopção de uma “bateria” de testes “cegos” de tentativas de clonagem e “*hacking*” do cartão levados a efeito pela comunidade científica de reconhecida capacidade e competência técnicas. Por outro lado e a título meramente exemplificativo dos perigos de concentração da informação, temos de lembrarmo-nos que a informação - dados pessoais - existente nas bases de dados da Administração Pública nem sempre merece as melhores garantias de segurança e criteriosa utilização. A CNPD apontou isso mesmo no relatório da inspecção que efectuou a diversos hospitais sobre o registo de dados pessoais de saúde, sua segurança e condições de utilização, expressando as mais graves preocupações sobre o tratamento de dados pessoais de saúde nas unidades que visitou - verdadeiramente representativas do tecido nacional de unidades de saúde, concluindo por um generalizado incumprimento da lei, pelas deficientes condições de segurança e pela falta de privacidade e de protecção dos dados pessoais dos utentes (Relatório da CNPD disponível em [www.cnpd.pt/bin/relatorios/outros/outros.htm](http://www.cnpd.pt/bin/relatorios/outros/outros.htm)). Mas, ainda e para melhor ilustração, as notícias vindas a público sobre o manuseamento indevido, com alteração abusiva da informação substantiva existente, da base de dados do Registo Individual do Condutor da Direcção-Geral de Viação, revela a fragilidade dos sistemas de informação que por vezes se verifica. Na matéria aqui em apreço, como é a do cartão do cidadão que concentra informação de identificação civil com informação sectorial - desde logo, informação respeitante ao Sistema Nacional de Saúde - estas preocupações e realidades não podem deixar de, em primeiro lugar, ser equacionadas e, em segundo lugar, ponderadas de forma fundamentada, antes de serem tomadas profundas e irreversíveis decisões.

Ver, *infra*, nota de rodapé 29.

<sup>27[27]</sup> Sabemos que as decisões político-legislativas não devem ser tomadas com base nas patologias e desvios aos padrões normais de boa-fé, zelo e diligência. No entanto, no que toca à insuficiência e deficiência de regras de segurança da informação dos sistemas informáticos e à utilização abusiva e indevida dos dados pessoais, quer no seio da Administração Pública, quer no âmbito de entidades privadas, a proliferação e frequência dessas patologias e desses desvios devem integrar o elenco de factores de ponderação no juízo de proporcionalidade, à luz dos princípios da prevenção e da precaução.

Ver, *infra*, nota de rodapé 29.

da privacidade e dos dados pessoais, à luz, obviamente, daquelas considerações e daquele enquadramento.

Antes, porém, em termos resumidos e simplificados, passamos a uma breve explicação do funcionamento do Cartão do Cidadão.

#### V - Sumária explicação do funcionamento do cartão do cidadão

O cartão do cidadão que a presente Proposta visa introduzir é composto por uma parte visível e por uma outra parte apenas acessível por meios electrónicos, através do *chip*.

Para os cidadãos portugueses, o cartão do cidadão é, não apenas documento de identificação, mas complementarmente documento de viagem.

A parte visível tem os dados e as informações listados no artigo 7º nº 1 e 3 da Proposta. Nela estão expostos os quatro números de identificação referidos no artigo 16º da Proposta, além de outros dados.

A parte apenas acessível por meios electrónicos contém os dados, as informações e as aplicações constantes do artigo 8º da Proposta. Para aceder à informação nela existente, é necessário introduzir o cartão do cidadão num sistema informático que suporte a utilização do *smartcard* (*chip*).

A existência de uma parte invisível, com informação apenas acessível com recurso a meios electrónicos, permite:

- Efectuar a *identificação forte on-line* do cidadão em serviços electrónicos baseados em mecanismos "*challenge-response*", bem como a sua *autenticação forte* noutros canais, como seja o telefónico, através de *autenticação por geração de token* - Autenticação multicanal baseada em *One-Time-Passwords*;
- Assinar documentos electrónicos com valor legal;
- Armazenar a informação visível no cartão;
- Armazenar dados biométricos (fotografia e *templates* de impressões digitais);
- Armazenar informação adicional que o cidadão pretenda colocar no *chip*, para seu uso pessoal;
- Identificar univocamente o cartão e o *chip* através de dados relativos à sua emissão.

Nesse sistema, o cartão do cidadão entra em interacção com aplicações desenvolvidas por todas as entidades - públicas e privadas - aderentes ao sistema, sendo certo que todos os organismos e

serviços da Administração Pública e outras entidades do Estado terão esta funcionalidade disponível.

O acesso à informação do cartão é definido por níveis diferenciados estabelecidos pelos certificados e pela inserção prévia do código de identificação pessoal (PIN), salvo as excepções previstas no nº 4 do artigo 13º e nº 5 do artigo 14º.

Todas as operações de assinatura digital/autenticação são realizadas no *chip* pelo que é obrigatória a introdução do cartão no leitor seguida da digitação do PIN respectivo.

A compartimentação do acesso à informação é controlada pelos PINs existentes e que têm as seguintes finalidades:

- PIN de acesso a dados (morada) - PIN1;
- PIN para autenticação *on-line* e por mecanismo EMV-CAP - PIN2;
- PIN para criação de assinatura digital qualificada - PIN3;

As entidades privadas aderentes ao protocolo de utilização do cartão do cidadão só acedem à área pública do cartão mediante o desenvolvimento das respectivas aplicações de *“middleware”* (aplicações informáticas de comunicação com os dados do cartão). *“O “middleware” irá disponibilizar funcionalidades para a autorização de execução de serviços às entidades que manifestem e justifiquem o interesse em o fazer. Estas entidades terão de ser responsáveis pela implementação da aplicação.”*<sup>28[28]</sup>

Deste modo assegura-se a interacção do Cartão de Cidadão com as referidas aplicações apenas para a realização de operações de identificação do titular (autenticação electrónica) e para as operações de uso de assinatura electrónica qualificada.

Através de uma outra aplicação gráfica igualmente disponibilizada, o cidadão titular do Cartão terá também a possibilidade de consultar os dados nele gravados, incluindo os respectivos certificados. Esta aplicação permitirá igualmente ao cidadão inserir informações na pasta pública existente no cartão do cidadão, bem como alterar qualquer um dos três PINs já referidos.

O processo para aceder ao dado fotografia é igual ao seguido para o acesso aos restantes dados contidos no cartão.

---

<sup>28[28]</sup> Esclarecimentos prestados à CNPD, a pedido desta, pela UMIC - Unidade para a Missão Inovação e Conhecimento.

Em relação às impressões digitais, a verificação da correspondência (*matching*) de impressões digitais do cidadão com os *templates* (ou imagens) de impressões digitais armazenados no cartão, é realizada através de mecanismos *match-on-card*. O *matching* de impressões digitais será utilizado apenas como mecanismo de verificação/autenticação da identidade do cidadão, e não como solução de controlo de acessos a dados ou a funcionalidades do Cartão de Cidadão.

Através da *Framework* de Serviços Comuns (FSC) são realizadas, electronicamente, as operações de interacção, autenticação, autorização e de segurança com os sistemas de informação da Administração Pública.

Um dos componentes integrados na FSC designa-se de *toolkit* e consiste numa *interface* para a integração dos serviços dos organismos, entidades externas e do Sistema Ciclo de Vida. Entre outras funcionalidades, esta infra-estrutura garante um controlo de acessos distinto para cada Organismo. *“O toolkit de um dado Organismo será instalado e configurado exclusivamente para esse Organismo, pelo que terá um certificado próprio instalado neste processo, sob controlo do Organismo. Este certificado e o próprio toolkit local do Organismo serão administrados sob responsabilidade e controlo do seu detentor - o Organismo.”* <sup>29[29]</sup>

Seguidamente, então, examinaremos o articulado da Proposta, no que às normas atinentes à protecção de dados pessoais diz respeito, introduzindo os comentários e observações que nos parecem ajustadas no lugar próprio de cada preceito do articulado em estudo.

## VI - Análise da Proposta de Lei

### a) Exposição de Motivos

De acordo com a Exposição de Motivos introdutória à Proposta de Lei aqui em apreço (doravante designada simplesmente por Proposta), pretende-se com esta iniciativa legislativa que introduz o cartão do cidadão, em suma, alcançar maior segurança na identificação civil, modernizar, desburocratizar e obter maior eficiência na Administração Pública e harmonizar o sistema de identificação civil de acordo com os países da União Europeia. Por outro lado, a introdução do cartão do cidadão visa conduzir a população nacional até elevados e generalizados níveis de utilização das TIC's, tal como contrariar uma cultura de desconfiança dos cidadãos face à Administração.

---

<sup>29[29]</sup> Ver nota anterior.

Quanto aos padrões de segurança, afirma-se que a Proposta incorpora os patamares delineados no Regulamento (CE) nº 2252/2004, do Conselho, de 13 de Dezembro, aguardando as especificações técnicas por instrumento normativo - portaria.

Este instrumento normativo, aquando da sua emissão, deve ser remetido às CNPD para esta Comissão dar o seu parecer.

No que toca à Exposição de Motivos, a CNPD faz os comentários seguintes:

- i)* Os níveis de segurança da identificação civil dependem muito mais das características do sistema de informação, das regras de manuseamento desse sistema e de utilização da informação e das práticas operacionais efectivamente adoptadas, do que da concentração da informação (que, por si só, aumenta os riscos de insegurança da identificação civil e agrava as consequências para os cidadãos), do tipo de suporte documental do cartão e da tecnologia adoptada.
- ii)* A conformidade dos patamares de segurança com os parâmetros de segurança proclamados em qualquer instrumento não garante a segurança da informação. O Regulamento (CE) nº 2252/2004, do Conselho, de 13 de Dezembro actualiza as normas mínimas para os dispositivos de segurança e dados biométricos dos passaportes e documentos de viagem, tendo em vista a harmonização desses documentos no seio da União Europeia. A segurança da informação nos passaportes e documentos de viagem com circuitos integrados de informação ("*chips*") e dados biométricos tem levantado sérias preocupações quanto à fiabilidade, inviolabilidade, risco de falsificação e de contrafacção. De qualquer modo, o Regulamento (CE) nº 2252/2004, do Conselho, de 13 de Dezembro, refere-se apenas a especificações não secretas, cabendo aos Estados-Membros completar estas com as especificações secretas que entendam adoptar. De qualquer modo, a segurança da informação depende, além das regras proclamadas em instrumentos normativos e regulamentares, do acompanhamento pontual da evolução tecnológica, da antecipação e perseguição das técnicas utilizadas pelos agentes de "ataques informáticos", das regras de operacionalidade, da observância de boas práticas e da efectiva fiscalização.

#### **b) Artigo 2º**

Esta norma define o cartão do cidadão e indica quais os números de identificação que este engloba.

Por enquanto, o cartão do cidadão não tem dispositivo de sistema de Identificação por Rádio Frequência (doravante designado pela sigla RFID), mas esta opção pode ser acolhida no futuro, à semelhança do que acontece com os novos passaportes.

A CNPD alerta que o sistema de RFID nos novos passaportes tem trazido preocupações quanto à fiabilidade, inviolabilidade, risco de falsificação e de contrafacção, pelo que a utilização desta tecnologia deve conhecer prévia e cuidada avaliação.<sup>30[30]</sup>

### c) Artigo 5º

O nº 2 do artigo 5º da Proposta acolheu uma recomendação da CNPD.

No entanto, cabe ainda lembrar que, mesmo nos casos em que o titular consente na reprodução por cópia do cartão do cidadão (ainda que a liberdade desse consentimento, face à necessidade e exigência em determinados casos, seja duvidosa: caso da celebração de contratos e prática de actos bancários, comprovação da identidade por fotocópia do cartão de identificação civil, apenas por mero exemplo), frequentemente o receptor da cópia do cartão do cidadão fica com a posse de mais dados pessoais de identificação do que aqueles que necessita para os seus propósitos. Nestes casos, não deixa de verificar-se que esse receptor dispõe de uma porta de acesso a dados pessoais que não se mostram pertinentes, nem necessários, mostrando-se, aliás, excessivos (ao contrário do disposto na alínea c) do nº 1 do artigo 5º da LPD), potenciando o risco de utilização abusiva.<sup>31[31]</sup>

### d) Artigo 7º

De acordo com os nº 3 e 4 deste artigo 7º, na zona específica destinada à leitura óptica consta o número do documento (alínea h) do nº 4 deste artigo). Tal significa que qualquer entidade que interage com o cartão conhece o número do documento. Tendo em conta que, de acordo com o

---

<sup>30[30]</sup> Ver, quanto à RFID, a Deliberação da CNPD sobre esta matéria, disponível em [www.cnpd.pt/bin/orientacoes/RFID.pdf](http://www.cnpd.pt/bin/orientacoes/RFID.pdf)

<sup>31[31]</sup> A CNPD não pode ser alheia, na apreciação da Proposta, a realidade tal como ela se apresenta, mormente perante a actividade desta Comissão. A configuração do tecido institucional, público e privado e empresarial, de sectores de diversa e díspar natureza surge, com crescente frequência e amplitude, com uma proximidade deveras apertada. Para ilustrar este retrato, vejam-se as relações de Grupo tantas vezes existente entre entidades de sectores de actividade tão diversa como sejam o bancário, financeiro e creditício, segurador, imobiliário, hospitalar, laboral, comercial. A recolha por parte de uma entidade de dados pessoais de identificação sectorial que nada têm a ver com a actividade dessa entidade “abre a porta” e propicia o acesso indevido a dados pessoais. A CNPD alerta que são frequentes os casos de utilização abusiva e de falta de regras de segurança da informação, nomeadamente no sector da saúde e noutros sectores da Administração Pública.

Ver, *infra*, nota de rodapé 29.

nº 2 do artigo 41º do Projecto, é gerada uma base de dados com o número do documento e nome do titular durante o prazo de validade do cartão, com finalidade de controlar a existência de cartões válidos e cancelados e que, de acordo com o nº 2 do artigo 31º, o pedido de cancelamento pode ser feito por telefone ou por via electrónica, parece à CNPD que é, não apenas não pertinente, não necessário e excessivo o acesso ao dado pessoal número de documento por parte de qualquer entidade que interaja com o cartão, mas esse acesso comporta riscos graves para o titular.

#### e) Artigo 8º

No artigo 8º indica-se a informação existente no circuito integrado (*chip*).

Quanto à alínea f) do nº 1 deste artigo, relativo às indicações eventuais tipificadas na lei, a CNPD alerta para a necessidade imperiosa de impedir indicações geradoras ou potenciadoras de discriminações inadmissíveis à luz da CRP (artigo 13º) e da LPD (artigos 5º nº 1 alíneas a) e b) e 7º nº 2).

Quanto às informações pessoais arquivadas pelo próprio cidadão, deve a este ser garantido o direito de informação, com verificação do seu cabal esclarecimento, quanto às condições de acesso a essa informação, às regras e procedimentos de segurança da informação aí inserida e quanto aos riscos da inserção de informação no que respeita ao acesso e alterações indevidos efectuados por terceiros.

A CNPD chama a atenção para a maior importância, em especial quanto aos nº 2 e 3 deste artigo 8º, para as concretas e pragmáticas regras de operacionalidade e para a necessidade da eficácia do acompanhamento, avaliação e fiscalização do desempenho das funcionalidades e das regras e procedimentos de segurança da informação.

#### f) Artigo 12º

Nesta norma, também se vê espelhada a chamada de atenção da CNPD para a definição legal e alcance atingido da noção anteriormente proposta de assinatura.

#### g) Artigo 13º

O dado pessoal morada serve para definir o domicílio do cidadão apenas nas relações que este mantém com o Estado. Quanto às outras entidades, observam-se as regras do Código Civil, do Código do Processo Civil e de outros diplomas que, eventualmente, se lhe refiram.

O acesso ao dado pessoal “morada” é livre para as autoridades judiciárias e policiais (nº 3).

Do nº 4 deste artigo 13º deve extrair-se a qualificação dada ao dado pessoal morada, vendo este dado pessoal reforçada a intensidade do seu valor enquanto “porta de entrada” para a intrusão e devassa da privacidade dos cidadãos, impondo-se o consentimento expresso do titular para poder ser acedido. Isto é, nesta proposta fica espelhada a especial sensibilidade do dado pessoal “morada”, no seio dos dados pessoais dos cidadãos, em virtude do especial cuidado que o seu tratamento merece, podendo mesmo revelar-se um dado pessoal sensível quando inserido em tratamentos para determinadas finalidades. Tal levou mesmo o legislador a mantê-lo secreto e a exigir o consentimento expresso - através da introdução do PIN - para o seu acesso.

Ao cidadão deve ser dada a informação da vantagem de atribuição à morada de um código pessoal (PIN) - ver artigo 18º nº 4 - diferente dos outros PIN´s atribuídos às restantes funcionalidades, bem como do maior risco de atribuir o mesmo PIN a todas as funcionalidades e à sua morada.

#### h) Artigo 14º

Importa, de novo, esclarecer se a impressão digital - dado pessoal biométrico constante do *chip* do cartão (alínea e) do nº 1 do artigo 8º) - é registada através de cópia ou através do seu “template” (número ou binário exclusivo obtido após aplicação de algoritmo sobre o dado biométrico que permite o reconhecimento da impressão digital mas não a sua integral reprodução).<sup>32[32]</sup>

---

<sup>32[32]</sup> Ver Deliberação da CNPD sobre a utilização dos dados biométricos para controlo da assiduidade dos trabalhadores, disponível em [www.cnpd.pt/bin/orientacoes/principiosbiometricos.htm](http://www.cnpd.pt/bin/orientacoes/principiosbiometricos.htm), na qual muitas das considerações sobre o tratamento deste tipo de dados devem ser tidas em conta nos tratamentos feitos noutros contextos.



Adverte a CNPD que o acesso de todas as entidades policiais à impressão digital pode significar um procedimento desproporcionado sobre dados pessoais que não se apresentam pertinentes, necessários e não excessivos (alínea c) do nº 1 do artigo 5º da LPD).

A Base de Dados da Identificação Civil, no estado em que a CNPD a conheceu, não se encontrava em condições de registo dos “templates” - das impressões digitais, da imagem facial - nem se encontrava preparada para a comunicação de dados prevista pela Proposta.

Para a CNPD, o “template” da impressão digital, convertível num código cujo método de produção é exclusivo da Base de Dados de Identificação Civil, vigorando, portanto, para todo o país para todos os cidadãos e diferindo de todos os outros métodos de produção de “templates” relativos a dados biométricos, pode funcionar como verdadeiro número único - exclusivo e imutável - de identificação e de acesso à informação existente sobre determinado cidadão.

#### **i) Artigo 15º**

As indicações eventuais existentes no *chip* devem ser pertinentes (adequadas), necessárias e não excessivas face à finalidade que visam prosseguir (alínea c) do nº 1 do artigo 5º da LPD), bem como devem ser exactos e actualizados (alínea d) do mesmo nº 1 do artigo 5º da LPD) e, ainda, garantir a não discriminação dos cidadãos.

Na opinião da CNPD deve ser garantido ao cidadão o direito de informação sobre a existência e conteúdo destas indicações eventuais, direito que haveria de estar, ainda na opinião da CNPD, previsto nesta Proposta.

#### **j) Artigo 16º**

Este artigo prevê a concentração no cartão do cidadão da informação de identificação civil e sectorial, prevendo a separação lógica dessa informação e proibindo a interconexão ou cruzamento de dados e da informação.

No entanto, a CNPD adverte para o facto de a concentração da informação acarretar, só por si, riscos para a segurança da informação, para a privacidade e protecção de dados pessoais e para outros direitos dos cidadãos. Basta pensar, como mero exemplo, que a apropriação e utilização do cartão, ou a sua clonagem, significam a usurpação global da identidade dos cidadãos. Este

risco é tão mais imediato quanto se crê, no que à tecnologia diz respeito, que com o decurso do tempo tudo é possível conhecer, interferir e recriar.

De qualquer modo, esclarece-se que parece à CNPD que os serviços e organismos sectoriais têm de ter informação recíproca de identificação dos cidadãos, até para poderem confirmar a identidade dos requerentes. A verificação da identidade dos cidadãos por parte dos diversos serviços sectoriais através dos números de identificação civil e dos demais serviços confere maior garantia de certeza e fiabilidade da informação sobre o requerente, mas traz também menores garantias de não concentração (unicidade) do cartão.

Importa, igualmente, à CNPD alertar que os quatro números de identificação existentes no cartão - o número de identificação civil, o número de identificação fiscal, o número de utente dos serviços de saúde e o número de identificação da Segurança Social - todos seguidos e justapostos pode funcionar como um verdadeiro número único (composto por códigos numéricos significativos, imutáveis e exclusivos) quer de identificação nacional do cidadão, quer de chave de acesso à totalidade da informação que permite *“compor uma imagem completa da pessoa”*<sup>33[33]</sup>

Prevê-se que o cartão do cidadão inclua o número de utente do Serviço Nacional de Saúde. No entanto, entende a CNPD que, de acordo com o nº 1 do artigo 2º do Decreto-Lei 198/95, de 29 de Julho, mesmo com a alteração introduzida pelo Decreto-Lei 52/2000, de 7 de Abril, a emissão do cartão de utente do Serviço Nacional de Saúde é facultativa.

Assim sendo, na opinião da CNPD, deve ser facultativa a introdução do número de utente dos serviços de saúde no cartão do cidadão.

No caso de o cidadão não querer a constância do número de identificação de utente junto dos serviços de saúde, deve ser adoptada a solução prevista no nº 2 do artigo 7º da Proposta.

#### **k) Artigo 17º**

Esta norma prevê o número do documento para fiscalizar e impedir o uso de cartões cancelados. No entanto, para além do caso da alínea h) do nº 2 do artigo 36º, a Proposta não prevê outros casos de comunicação, nem prevê os mecanismos de fiscalização sobre esse uso.

---

<sup>33[33]</sup> Jorge Miranda, Rui Medeiros, *ob. cit.*, pag. 389.

Não é atribuída a qualquer entidade a responsabilidade pela atribuição, conservação e, sobretudo, segurança deste número, sendo certo que as operações de emissão, substituição e cancelamento do cartão (artigos 20º e 36º) não incluem, necessariamente, essa responsabilidade.

De acordo com o nº 1 do artigo 39º, o cidadão tem o direito de conhecer o número do documento. No entanto, na opinião da CNPD devia ser proibido o tratamento deste dado pessoal, em todos os casos, mesmo com o consentimento por parte do cidadão, salvo para efeitos de cancelamento do cartão e de controlo do uso de cartão cancelado.

Devia haver a previsão legal expressa da proibição de atribuição do mesmo número do documento cancelado e substituído a outro cartão do mesmo cidadão.

Tendo em conta que o número do documento composto por uma parte numérica significativa (número de identificação civil) e por um número de três caracteres - dois alfanuméricos e um dígito de controlo - permanece exclusivo e imutável durante um prazo alargado de tempo - prazo de validade, segundo o artigo 41º nº 2 da Proposta, neste período de tempo o número de documento, parece à CNPD, pode funcionar como verdadeiro número único, quer de identificação directa do cidadão, quer de acesso à informação global que permite criar a sua imagem completa.

#### **l) Artigo 18º**

Deve ser garantido ao cidadão o direito de informação e aviso sobre as vantagens de atribuição de um PIN diferente para cada funcionalidade e para o dado pessoal "morada", tal como a advertência dos riscos de atribuição de um PIN igual para cada uma destas funcionalidades.

#### **m) Artigo 20º**

A Direcção-Geral dos Registos e Notariado (DGRN) é a entidade responsável pelo tratamento dos dados pessoais, de acordo com esta norma e com o artigo 38º, à frente analisado.

Responsável pelo tratamento, nos termos da alínea d) do artigo 3º da LPD, é a *"pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios de tratamento sejam determinados por disposições legislativas ou regulamentares, o responsável pelo tratamento deve ser indicado na*

*lei de organização e funcionamento ou no estatuto da entidade legal ou estatutariamente competente para tratar os dados pessoais em causa”.*

A CNPD recomenda, então, que fique consignado que, a DGRN, no que toca aos requisitos técnicos, à segurança da informação, à definição dos procedimentos de controlo e fiscalização e à credenciação dos funcionários e agentes, recorra aos melhores conhecimentos técnicos e científicos disponíveis, por consulta “cega” à comunidade académica e científica.

A prossecução das competências pelas entidades referidas na alínea c) do nº 2 do artigo 20º implica a celebração de protocolos ou contratos que, de acordo com o artigo 16º e com a alínea e) do artigo 29º da LPD, devem ser avaliados pela CNPD.

Não está consagrada na lista de competências da DGRN *“proceder à auditoria de procedimentos, monitorização e detecção de incidentes de segurança, repositório de permissões, sincronização temporal e transmissão.”*

Na opinião da CNPD, estas são competências típicas do responsável pelo tratamento dos dados pessoais, sobretudo aquelas que se prendem com as condições e limites desse tratamento - transmissão, com as regras de segurança e padrões de procedimento, bem como com a respectiva fiscalização.

#### **n) Artigo 21º**

No serviço de apoio ao cidadão, deve ser assegurado o direito de informação ao cidadão, nos termos do artigo 10º da LPD, bem como informá-lo da existência e conteúdo das indicações eventuais, das condições de tratamento, regras de segurança e riscos para a privacidade relativos aos dados pessoais introduzidos pelo próprio cidadão e das vantagens de atribuição de PIN´s diferentes a cada funcionalidade e à morada e riscos de atribuição de um só PIN a cada funcionalidade e à morada.

Deve, ainda, na opinião da CNPD, ser prestada a informação aos cidadãos da natureza facultativa da inserção no cartão do cidadão do número de utente dos serviços de saúde, bem como da inexistência de consequências desvantajosas para a fruição desses serviços no caso de optarem pela não inclusão desse número de identificação (alínea c) do nº 1do artigo 10º da LPD)

#### **o) Artigo 23º**

Nesta norma prevê-se que a supervisão caiba à Agência para a Modernização Administrativa, organismo criado junto da Presidência do Conselho de Ministros.

A supervisão é uma função que, na opinião da CNPD, deve ser efectuada por entidades com meios e capacidades técnicos indubitáveis e marcadas por inquestionável independência política e administrativa.

Sobre o controlo da existência de um número único, nos debates parlamentares sobre a criação da CNPD, defendeu-se que devia ser esta autoridade, pela sua natureza independente, pelo seu quadro material de competências e pela sua composição plural, quem acompanhava e fiscalizava a actuação do Estado e dos poderes públicos no que a essa proibição respeitava.<sup>34[34]</sup>

Assim sendo, a Agência para a Modernização Administrativa fiscaliza a emissão, substituição e cancelamento do cartão do cidadão, fiscaliza as operações de personalização no que toca à observância dos requisitos técnicos e de segurança, fiscaliza a actuação dos funcionários e agentes e o respeito pelas regras do Sistema de Certificação Electrónica do Estado na emissão dos certificados para autenticação e certificados qualificados para assinatura electrónica qualificada, operações desenvolvidas no âmbito das competências da DGRN.

A supervisão deve ser efectuada por equipas plurais, arbitrária e aleatoriamente rotativas.

No entanto, esta supervisão deve ser participada por entidades com vocação, meios e capacidade para a acompanhar, no esteio da maior transparência e confiança generalizada no sistema criado para o cartão do cidadão, participação que pode ser desenvolvida pela CNPD, conforme perspectiva defendida no debate parlamentar que criou a CNPD.

#### p) Artigo 25º

Este artigo elenca os dados pessoais recolhidos no momento do pedido de emissão do cartão do cidadão.

A CNPD adverte para a exigência de actuação zelosa e diligente dos funcionários e agentes da DGRN.

Ademais, a CNPD alerta para a necessidade de a DGRN adoptar procedimentos uniformes de recolha dos dados pessoais, nomeadamente, no que diz respeito aos dados biométricos.

---

<sup>34[34]</sup> Ver [http://debates.parlamento.pt/r3/dar\\_s2rc/shpg\\_dars2rc.asp](http://debates.parlamento.pt/r3/dar_s2rc/shpg_dars2rc.asp)

A CNPD reproduz, sobre o “template” da imagem facial, caso venha a ser criado, o que atrás disse sobre os “templates” da impressão digital (ver comentários aos artigos 12º e 14º).

Mais ainda, a CNPD informa que, no seu entendimento, a melhor tecnologia disponível sobre a recolha da imagem facial e a sua transformação em “template”, com aptidão para reconhecimento e verificação com exactidão, ainda se encontra longe de satisfazer padrões aceitáveis de fiabilidade.

**q) Artigo 26º**

Nesta norma dedicada à substituição do cartão do cidadão, a CNPD chama especialmente a atenção para as previsões das alíneas d) e e) do nº 1, casos em que a actuação da DGRN deve ser imediata, sob pena de imprevisíveis prejuízos para os cidadãos.

**r) Artigo 27º**

Quanto à verificação dos dados pessoais tratada nesta norma, novamente se chama a atenção para o especial cuidado requerido pelos dados biométricos. De facto, a fidedignidade destes dados não é absolutamente garantida por nenhuma tecnologia existente e a fiabilidade desses dados dependem, em larga medida, da operação de recolha.

O nº 3 deste artigo haveria, no entendimento da CNPD, de reforçar o dever de confidencialidade sobre toda a informação trocada para comprovar a exactidão ou a titularidade dos elementos de identificação, tal como haveria de prescrever a eliminação imediata dos dados pessoais e dos ficheiros produzido no processo de verificação.

**s) Artigo 29º**

Nesta norma referente aos dados pessoais relativos ao sistema de saúde, repete-se que, de acordo com o nº 1 do artigo 2º do Decreto-Lei 198/95, de 29 de Julho, mesmo com a alteração

introduzida pelo Decreto-Lei 52/2000, de 7 de Abril, a emissão do cartão de utente do Serviço Nacional de Saúde é facultativa.

Assim sendo, na opinião da CNPD, deve ser facultativa a inserção destes dados no cartão do cidadão, devendo este ser informado da natureza facultativa dessa inserção e da inexistência de consequências decorrentes da sua não inserção.

O tratamento de dados pessoais deve ser feito de boa-fé: alínea a) do nº 1 do artigo 5º da LPD.

Aos cidadãos deve ser prestada a informação sobre a elevada sensibilidade da informação a que se acede através do número de utente do Sistema Nacional de Saúde, sobre os riscos de acesso indevido e sobre os potenciais prejuízos daí decorrentes.<sup>35[35]</sup>

#### t) Artigo 31º

Repete a CNPD, neste artigo dedicado à entrega do cartão do cidadão ao indivíduo requerente ou a terceiro que o represente, a obrigação de informar o cidadão da vantagem para a sua privacidade, para a protecção dos seus dados pessoais e para a segurança da informação de atribuir um PIN diferente a cada funcionalidade e à sua morada, bem como do risco de atribuir um PIN igual para todas as funcionalidades e para a sua morada.

#### u) Artigo 33º

A confiança no sistema depende, na óptica da CNPD, da segurança da comunicação e da certeza quanto ao requerimento de cancelamento.

Na opinião da CNPD, devem ser adoptadas medidas especiais de verificação no caso do cancelamento previsto no nº 6 desta norma e deve ser equacionada a possibilidade de cancelamento, provisório ou definitivo, do cartão do cidadão relativo a menor, interdito ou inabilitado por anomalia psíquica, a partir de comunicação proveniente de terceiro diferente do representante legal.

---

<sup>35[35]</sup> Ver, *supra*, notas de rodapé 24 a 26. Ao vertido nestas notas devem acrescer as observações seguintes: geralmente, a vítima da violação da privacidade e do acesso indevido e utilização abusiva dos dados pessoais é uma vítima silenciosa, tantas vezes ignorando que essa violação, esse acesso e essa utilização aconteceram. Tal é frequente no que toca aos dados pessoais de saúde. Por outro lado, a violação da privacidade, o acesso indevido a dados pessoais e a utilização abusiva desses dados geralmente acontecem nos circuitos informais, mas vastos, de circulação da informação, circuitos que escapam aos mecanismos instituídos pelos regimes e perceptíveis, quer às entidades de controlo, quer às de fiscalização.

**v) Artigo 35º**

Esta norma define a finalidade do tratamento dos dados pessoais que, à luz da LPD, é determinada, explícita e legítima. Os dados pessoais não devem ser utilizados para qualquer outra finalidade (artigo 5º, nº 1, alínea b) da LPD).

**w) Artigo 36º**

Os dados pessoais objecto de tratamento, listados nos artigos 7º, 8º e 29º, são pertinentes, necessários e não excessivos face à finalidade do tratamento: alínea c) do nº 1 do artigo 5º da LPD.

Os dados pessoais devem ainda ser exactos e actualizados: alínea d) do nº 1 do artigo 5º da LPD. Os dados pessoais do artigo 29º apenas devem ser tratados se o titular consentir na inserção da sua identificação junto do Serviço Nacional de Saúde no cartão do cidadão, decisão que deve ser precedida da informação cabal sobre a voluntariedade dessa inserção e sobre a inexistência de qualquer consequência da opção tomada pelo mesmo cidadão.

**x) Artigo 37º**

Este artigo, versando sobre a comunicação de dados, repete a comunicação em separado dos dados pessoais respeitantes aos diversos sectores.

Ao nº 4 desta norma devia seguir, na opinião da CNPD, a obrigação de eliminação dos ficheiros produzidos na operação de personalização, imediatamente após a comunicação à Base de Dados de Identificação Civil, ainda que essa obrigação esteja prevista no nº 1 do artigo 41º.

O nº 5 desta norma, repetindo para os dados pessoais de saúde a regra já estabelecida para todos os dados pessoais (nº 1 e 2), mais não reflecte, na perspectiva da CNPD, do que a especial sensibilidade dos dados de saúde, requerendo estas especiais medidas de segurança em virtude da também especial perigosidade e gravidade da sua violação, acesso indevido e utilização abusiva.



**y) Artigo 38º**

Esta norma define o responsável pelo tratamento, dando a CNPD por reproduzidas as considerações atrás tecidas nos comentários ao artigo 20º da Proposta.

**z) Artigo 39º**

Neste preceito dedicado ao direito à informação, prevê-se que o cidadão conheça todos os dados e aspectos relevantes de tratamento desses dados que lhe dizem respeito.

No entanto, se não é prestado o dever de informação aos cidadãos sobre os dados invisíveis, se não se informam os cidadãos sobre onde, como e em que condições podem conhecer os dados pessoais que estão invisíveis no cartão, fica seriamente esvaziado o direito de informação dos cidadãos sobre o tratamento dos dados pessoais que lhe respeitam.

**aa) Artigo 41º**

O nº 1 deste artigo ordena a destruição dos ficheiros criados com a personalização (impressão) do cartão, logo após a confirmação da entrega do cartão ao titular.

O nº 2 prevê a criação de uma base de dados, após a entrega e validação do cartão pelo cidadão, onde constam o nome do cidadão e o número do documento (ver artigo 17º desta Proposta), conservando esses dados pelo período de validade do cartão.

A leitura deste nº 2 do artigo 41º da Proposta, contextualizado pelos artigos 19º, 26º, 33º nº 4, 55º nº 6, 63º nº 2 e pelo artigo 13º da Lei 33/99, de 18 de Maio (Lei de Identificação Civil), aponta para que o prazo de validade do cartão do cidadão seja um prazo de longa duração (5 ou 10 anos).

Parece à CNPD que, pelo menos durante este período de tempo correspondente ao prazo de validade do cartão do cidadão, é criada nesta base um número único, composto por um código numérico significativo e por três caracteres (dois alfanuméricos e um dígito de controlo), número

que é exclusivo e imutável, permitindo a identificação directa do cidadão e permitindo o acesso a informação que permite a composição da imagem completa da pessoa.

**bb) Artigo 42º**

Nesta norma sobre as regras e procedimentos de segurança, a CNPD reconhece o acolhimento dos artigos 14º e 15º da LPD, cabendo especificar que ao responsável pelo tratamento é pedido o cumprimento, não de uma obrigação de meios ou de comportamentos adoptados, mas uma obrigação de resultados alcançados na segurança da informação.

**cc) Artigo 45º**

Nesta norma, já dentro do regime sancionatório, prevê-se, pela combinação do nº 1 do artigo 43º com os nº 1, 2 e 3 do artigo 45º, a possibilidade de punição da tentativa negligente.

A CNPD reflecte e sugere igual reflexão sobre a possibilidade destes casos ocorrerem.

**dd) Artigo 50º**

A epígrafe desta Secção é "Crimes".

No entanto, a referência aos artigos 37º e 38º da LPD, logo no nº 1 do artigo 50º, remete para normas sancionatórias contra-ordenacionais

Assim, a epígrafe da Secção deve passar a incluir os casos das contra-ordenações, na opinião da CNPD.

**ee) Artigo 51º**

Esta norma faz a previsão do tipo de ilícito pela indicação falsa.

Na opinião da CNPD, esse tipo de ilícito haveria de se limitar aos casos de indicação falsa dolosa, com intenção de tirar proveito indevido ou de enganar os serviços de identificação civil.

Parece à CNPD que é excessivo onerar o cidadão com a invocação e demonstração de erro que afaste a sua culpa no fornecimento de informação errada para emissão do cartão do cidadão. De resto, não deve operar-se uma transferência da responsabilidade pela exactidão da informação do responsável pelo tratamento (DGRN) para o cidadão.

Por outro lado, deve ser equacionada a liberdade do cidadão introduzir no seu cartão informação juridicamente relevante e não verdadeira, desde que o faça na parte do *chip* destinada a arquivar informações pessoais.

**ff) Artigo 53º**

No processo de expansão territorial progressiva, deve atender-se, na opinião da CNPD, às considerações vertidas *supra* em “IV - A questão tecnológica e os princípios da prevenção, da precaução e da proporcionalidade”.

## VII - Conclusões

1 - A CNPD enquadra a Proposta nos capítulos I a IV deste parecer, devendo as considerações aí tecidas informar a análise desta Proposta.

2 - A CNPD recomenda a realização de estudos de risco do sistema, testes de segurança e de fiabilidade e análise de impacto das medidas que pretende adoptar, por entidades independentes e dotadas de meios técnicos, humanos e de capacidades de elevado e indiscutível valor.

3 - A CNPD recomenda a observância dos comentários e sugestões feitos em cada artigo da Proposta, no capítulo VI, em que procedeu à análise do articulado.

Este é o parecer da CNPD.

Lisboa, 23 de Outubro de 2006

Eduardo Campos (Relator)

Helena Delgado António

Carlos Campos Lobo

Ana Roque

Luís Barroso

Luís Lingnau da Silveira (Presidente)

---