A PRIVACIDADE DOS ELEITORES NO VOTO ELECTRÓNICO

I – INTRODUÇÃO

A) As Autorizações da CNPD às experiências não vinculativas de voto electrónico presencial e não presencial

Nos actos eleitorais de 13 de Junho para a eleição dos Deputados ao Parlamento Europeu e de 22 de Fevereiro de 2005 para a eleição dos Deputados à Assembleia da República, a UMIC – Unidade de Missão Inovação e Conhecimento – solicitou à Comissão Nacional de Protecção de Dados – CNPD – autorização para proceder ao tratamento de dados pessoais dos eleitores para efeitos de votação electrónica presencial e não presencial – nome e número de eleitor, no primeiro caso e nome, morada e número de eleitor, no segundo.

Esse tratamento, sumariamente, consistia no acesso, através de comunicação pelo STAPE – Serviço Técnico de Apoio ao Processo Eleitoral – aos dados pessoais dos eleitores – nome e número de eleitor – para efeitos de realização da experiência de voto electrónico em algumas assembleias eleitorais, bem como ao acesso e tratamento dos dados pessoais nome, morada e número de eleitor dos cidadãos eleitores residentes no estrangeiro para efeitos da experiência de voto electrónico não presencial.

A CNPD considerou que o pedido da UMIC, porque foi criada na dependência da Presidência do Conselho de Ministros com a função de estudar as formas de aprofundamento da democracia pela utilização das tecnologias de informação (nº 2 e alínea n) do nº 3 da Resolução do Conselho de Ministros nº 135/2002, publicada no D. R. nº 268 de 20 de Novembro de 2002), tendo, aliás e especificamente, como mister actuar de modo a incrementar a participação electrónica e o exercício de votação electrónica presencial (4º Pilar da Resolução de Conselho de Ministros nº 107/2003, que aprovou o Plano de Acção para a Sociedade de Informação), respondia positivamente aos requisitos fixados pelo artigo 16º da Lei 13/99 de 22 de Março para aceder aos dados pessoais mencionados, ou melhor, para que o STAPE pudesse comunicar à UMIC esses mesmos dados para as finalidades indicadas.

Relembrando as Autorizações concedidas pela CNPD, salienta-se que:

a) Experiência de voto electrónico presencial na eleição de 13 de Junho de 2004[1]

A Autorização concedida determinou, entre os elementos comuns a todas as autorizações emitidas pela CNPD ao abrigo do disposto no artigo 30º da LPD – Lei da Protecção de Dados Pessoais, Lei 67/98 de 26 de Outubro – que os dados pessoais fossem conservados pelo prazo máximo de 60 minutos após o encerramento das urnas de voto para a eleição dos euro-deputados.

A CNPD exigiu, no entanto, que *i)* a comunicação dos dados pessoais da BDRE – Base de Dados de Recenseamento Eleitoral – pelas Comissões de Recenseamento à UMIC por meio digital (disquete ou cd/rom) fosse encriptada por palavra-passe, para segurança da comunicação dos dados, *ii)* que essa comunicação acontecesse imediatamente antes da abertura das urnas, procedendo-se à imediata transferência dos dados do suporte digital para o disco dos computadores do processo da votação electrónica e *iii)* que imediatamente após a introdução dos dados no sistema o suporte digital (disquete ou cd/rom) fosse destruído.

Além destas exigências, a CNPD impôs que:

- Fosse feita a monitorização de cópia dos ficheiros com cópia do *log* para disquete, assinada digitalmente, seguida de formatação dos computadores instalados nas Comissões Recenseadoras das freguesias seleccionadas, com observância dos procedimentos que impedissem recuperação dos dados formatados;

- Fossem encriptados os ficheiros temporários entretanto criados e utilizados, desde a instalação dos computadores até à eliminação dos dados e finalização do tratamento;

- Fossem observadas, no quadro do sistema operativo dos computadores utilizados, as mais elementares regras de segurança informática, ou seja, *password* de acesso, *password* de protecção da tela e protecção de BIOS;

- Não ficasse registada a hora do exercício do voto electrónico, bem como a escolha tomada pelo eleitor, a par do registo da hora de apresentação do eleitor junto da mesa de voto, para descarga no caderno eleitoral, pois esses registos permitiam, na óptica da CNPD, com elevado grau de probabilidade e de certeza, conhecer o

[1] Projecto de Autorização e Despacho da CNPD dados no Processo nº 1031/ 2004.

sentido de voto dos eleitores, o que violava o disposto no artigo 2º, nas alíneas a) e c) do artigo 5º e nº 1 e 2 do artigo 7º (uma vez que não existia lei nem consentimento dos titulares). A CNPD proibiu expressamente o tratamento que colocasse em perigo essa ocorrência.

- A CNPD fez impender sobre a UMIC o ónus de demonstrar cabalmente que seriam tomadas todas as cautelas e medidas técnicas suficientes para impedir que tal acontecesse.

- A Autorização concedida pela CNPD ficou dependente da condição dessa demonstração.

b) Experiência de voto electrónico presencial na eleição de 20 de Fevereiro de 2005[2]

Na experiência de votação electrónica presencial nas eleições legislativas de Fevereiro de 2005, o pedido de autorização para tratamento dos dados pessoais "nome" e "número de eleitor" não trouxe qualquer aspecto que o distinguisse do pedido feito para a experiência nas eleições europeias de 13 de Junho anterior, pelo que também a Autorização da CNPD a esse pedido não conteve qualquer diferença face àquela que se descreveu na alínea anterior.

c) Experiência de voto electrónico não presencial na eleição de 20 de Fevereiro de 2005[3]

Na experiência de voto electrónico não presencial, o pedido de autorização de comunicação de dados pessoais da BDRE à UMIC revestiu algumas especificidades, desde logo porque essa comunicação incluiu o dado pessoal "morada" dos eleitores residentes e eleitores fora do território nacional.

Distinguiram-se três momentos. Por um lado, o momento relativo à comunicação de dados a efectuar por parte do STAPE; por outro e em segundo lugar, o processo de

[2] Autorização da CNPD nº 48 /2005
[3] Autorização da CNPD nº 47/2005

atribuição de *passwords* e *usernames*, bem como o envio de *mailings*; por outro ainda e em último lugar, o momento do exercício do voto.

Quanto ao primeiro aspecto, foi necessário aferir, face à Lei do Recenseamento Eleitoral (LRE – Lei 13/99 de 22 de Março) conjugada com a Lei de Protecção de Dados (LPD) se se encontravam reunidos os requisitos que estas prevêem para que a comunicação se possa efectuar.
A resposta foi positiva, com igual fundamentação àquela que presidiu nas experiências anteriormente descritas.

Quanto ao segundo aspecto, importou verificar se estavam cumpridos os requisitos previstos na LPD. Efectivamente, a UMIC pretendeu enviar correspondência a todos os eleitores portugueses residentes no estrangeiro, no sentido de providenciar informação para os sensibilizar a participar nesta experiência, enviando-lhes o(s) código(s), *username* e *password*, de modo a habilitar as pessoas a participar na experiência de voto electrónico. Para efeitos de envio do *mailing* aos eleitores, a UMIC recorreu à empresa CESA – Campos Envelopagem, SA, como subcontratante.
Na primeira carta que a UMIC enviar ao titular dos dados, a CNPD fez impender sobre a UMIC o dever de fornecer todas as informações indicadas no artigo 10º, n.º 1 da LPD. Assim, por uma questão de transparência, haveria de ficar claro para o titular dos dados que o responsável do tratamento era a UMIC, qual a finalidade daquele tratamento e que os dados foram obtidos junto do STAPE.
A CNPD impôs ainda que fosse facultado ao titular dos dados informação sobre a possibilidade de o eleitor "*se opor, em qualquer altura, por razões ponderosas e legítimas relacionadas com a sua situação particular, a que os dados que lhe digam respeito sejam objecto de tratamento, devendo, em caso de oposição justificada, o tratamento efectuado pelo responsável deixar de poder incidir sobre esses dados*" (Cfr. artigo 12º al. a) da LPD). Coube à UMIC indicar o modo como o titular podia exercer esse direito.
Importou ainda analisar a questão relativa às medidas de segurança e de confidencialidade do tratamento. Neste contexto, foram analisados os modelos de contrato entre a UMIC e a empresa de envelopagem CESA e entre aquela e a Novabase.
A CNPD considerou que a UMIC não deixava de ser a responsável pelo tratamento, uma vez que as empresas intervenientes actuaram sempre na qualidade de subcontratantes, ou seja, mediante instruções do responsável pelo tratamento (no n.º 1 do artigo 14º e artigo 16º da LPD). No entanto, o contrato devia conter

especificamente quais as medidas técnicas e organizativas que o responsável considerava adequadas para proteger os dados, sendo o nível de segurança estipulado pelo responsável, tendo em conta os riscos que o tratamento apresenta e a natureza dos dados.

Quanto ao terceiro aspecto, o do exercício do voto electrónico não presencial, a CNPD condicionou a autorização à garantia dos aspectos relativos à confidencialidade e secretismo do voto e expressou fortes preocupações quanto à fiabilidade do voto final registado face à opção efectivamente tomada pelo eleitor. Na aferição da CNPD, não se tinham eliminado, evitado ou diminuído os riscos de viciação do processo eleitoral a partir do computador do eleitor. A título de exemplo, a CNPD indicou os procedimentos conhecidos por *"The man in the middle", "DNS Spoofing"* ou *"Phishingscam"*, a par da introdução de vírus nos computadores dos eleitores ou naqueles que estes utilizariam para o exercício de voto (onde podem encontrar-se instalados ou serem introduzidos *Screenloggers* e, ou, *Keyloggers*), como ocorrências passíveis de acontecer e que desvirtuavam o sistema de voto electrónico não presencial, na medida em que o resultado final do voto exercido não coincidiria com a opção tomada pelo eleitor, ou então permitiam o conhecimento da opção tomada pelo mesmo eleitor.

Assim, a CNPD autorizou a comunicação de dados por parte do STAPE relativamente aos cidadãos eleitores residentes no estrangeiro para que a UMIC pudesse iniciar o processo de atribuição de *usernames* e *passwords*, bem como o seu envio aos eleitores. Não obstante, o tratamento de dados por parte da UMIC ficou condicionado ao cumprimento do direito de informação, à existência de um contrato ou acto jurídico com as entidades subcontratantes e sob condição das garantias de confidencialidade, secretismo e fiabilidade do voto, de acordo com o supra exposto.

B) As verificações críticas da CNPD após a experiência não vinculativa de votação electrónica presencial do dia 13 de Junho de 2004

A CNPD acompanhou os processos das experiências das votações electrónicas não vinculativas, presenciais e não presenciais.
Esse acompanhamento consistiu na observação, compreensão e avaliação dos procedimentos adoptados pela responsável pelo tratamento e outras entidades sub-

contratantes e co-participantes, à luz das recomendações e exigências previamente feitas pela própria CNPD e de acordo com os princípios e regras dos processos eleitorais democráticos – a oficiosidade, obrigatoriedade, permanência e unicidade do recenseamento eleitoral, o sufrágio directo, secreto e universal, a liberdade e unicidade do voto – princípios e regras atinentes, quer à qualidade (*v.g.* exactidão e actualidade) dos dados pessoais, quer à legitimidade do tratamento, em ambos os casos, condicionantes do tratamento dos dados pessoais dos eleitores para os efeitos das autorizações requeridas e emitidas.

O acompanhamento da CNPD aos procedimentos nessas experiências saldou-se por algumas verificações críticas que merecem ser destacadas.
Assim:

a) As máquinas de algumas mesas de voto não tinham qualquer palavra-chave de BIOS, ao contrário do que foi recomendado pela CNPD no processo de autorização;
b) Em algumas mesas de voto, os cadernos eleitorais não foram carregados nas mesas electrónicas de votação imediatamente antes da abertura das urnas de voto electrónicas, conforme o teor das autorizações concedidas pela CNPD, antes foram esses dados dos cadernos eleitorais transferidos para as mesas de voto dias antes da data do acto eleitoral;
c) Após a cópia do ficheiro dos eleitores do suporte digital para os discos rígidos dos computadores utilizados nos processos de votação electrónica, não foram aqueles ficheiros imediatamente destruídos, conforme prescrição da CNPD na autorização concedida;
d) Aliás, alguns desses ficheiros ficaram intactos até ao fecho das urnas de voto, tendo sido até guardados juntamente com os cadernos eleitorais em suporte de papel após o encerramento das urnas e tendo sido destruídos apenas por interpelação da CNPD ao representante da entidade responsável pela experiência;
e) Em algumas mesas de votação onde a experiência foi desenvolvida, além de não terem sido destruídos os suportes digitais que serviram para a comunicação dos dados pessoais dos eleitores, não estavam esses suportes protegidos por qualquer forma, nem por encriptação, conforme foi prescrito pela CNPD na autorização emitida;
f) As linhas telefónicas utilizadas para a transmissão electrónica dos resultados não eram novas, conforme a entidade responsável pela experiência havia declarado no processo de obtenção de autorização junto

da CNPD (esta entidade havia declarado que apenas seria utilizada uma linha já existente), mas eram antes as linhas telefónicas das escolas onde as assembleias eleitorais estavam instaladas;

g) Em pelo menos uma assembleia eleitoral onde a experiência de votação electrónica decorreu, os resultados eleitorais dessa experiência não foram apurados e não se verificou a eliminação dos dados pessoais e eleitorais constantes do disco da máquina utilizada na experiência;

h) Os motores das bases de dados (SQLServer) encontravam-se sem qualquer tipo de segurança acrescida, o que permitiria, caso essas bases de dados colocassem um registo temporal (*timestamp*) nas operações de *log*, relacionar eleitores com votos expressos, colocando em crise o secretismo da votação;

i) As máquinas utilizadas nas experiências de votação electrónica não respeitavam as normas básicas dos sistemas de informação recomendadas pela CNPD (normas para além da palavra-chave), uma vez que essas máquinas não estavam actualizadas no que toca aos sistemas operativos utilizados pelas máquinas envolvidas – não foram aplicados os últimos *packs* e *patches*.

j) O sistema de protecção contra falhas era insuficiente e defeituoso, não estando as máquinas preparadas nem configuradas para trabalharem em redundância;

II – ENQUADRAMENTO DO VOTO ELECTRÓNICO NO REGIME DA PROTECÇÃO DE DADOS PESSOAIS

A análise da votação electrónica, na perspectiva da CNPD, reclama a avaliação do tratamento dos dados pessoais dos eleitores nesse âmbito e para essa mesma finalidade – do exercício do voto através de meios electrónicos – à luz do regime jurídico da protecção de dados pessoais.

*

Em primeiro lugar, de acordo com o artigo 2º da LPD, para além do estrito respeito pela reserva da vida privada e pelos direitos, liberdades e garantias, o tratamento de dados pessoais deve processar-se de forma transparente. A transparência do tratamento dos dados pessoais significa, antes de mais, o conhecimento por parte dos titulares dos dados pessoais sobre a entidade que desenvolve o tratamento, a finalidade desse tratamento e os demais termos, condições e circunstâncias desse tratamento.

"O princípio da transparência significa que o responsável de um tratamento de dados, devidamente identificado, deve dar a conhecer ao titular dos dados a realização do tratamento que lhe respeita, indicando, nomeadamente, os seus fins, categorias de dados tratados, períodos de conservação de dados, eventuais comunicações dos mesmos, etc.
Estabelecido no art. 2.º, da Lei da Protecção de Dados, o princípio da transparência efectiva-se, designadamente, através dos direitos à informação (art. 10.º) e acesso (art.º 11º) garantidos ao titular dos dados pessoais, mas também tem expressão no dever de notificação – para registo ou autorização pela Comissão Nacional de Protecção de Dados – dos tratamentos de dados pessoais."[4]
Assim e concluindo, de acordo com o artigo 2º da LPD, o tratamento de dados pessoais no âmbito de e para a finalidade do exercício do voto através dos meios electrónicos deve contar com o pleno conhecimento por parte dos cidadãos eleitores, titulares desses dados, sobre todos os termos, modos e condições que esse

[4] Catarina Sarmento e Castro, "Direito da Informática, Privacidade e Dados Pessoais", Almedina, 2005, Coimbra, pag. 228.

tratamento conhece, pelo menos aqueles que são elencados no formulário da notificação junto da CNPD.[5]

*

Em segundo lugar, tendo presente a alínea a) do nº 1 do artigo 5º da LPD, os dados pessoais objecto de processamento devem ser tratados de forma lícita e com respeito pelo princípio da boa fé. Estes dois princípios – o da licitude e o da lealdade[6], para além de se encontrarem relacionados com o princípio da transparência[7], envolvem também, não apenas as *"garantias funcionais"* que *"abarcam todo o processo que se estende da recolha e obtenção de informação ao seu tratamento, utilização e eventual comunicação", "uma garantia funcional suplementar"* que *"consiste na obrigação de especial diligência por parte das entidades que procedem ao registo[8]no sentido de assegurar a segurança dos ficheiros contra a sua destruição ou perda acidental ou contra o acesso, modificação ou difusão não autorizados (art. 7º)[9]. Está-se aqui perante uma garantia de ordem técnica, juridicamente tutelada, que visa prevenir tanto a conduta negligente, como a conduta dolosa".[10]*

Destes dois princípios, da licitude e da lealdade, como também do da transparência, resulta a obrigação da entidade responsável pelo tratamento dos dados pessoais para efeitos de votação electrónica de dar resposta ao dever previsto no nº 1 do artigo 14º da LPD.[11] Nesta norma, impõe-se ao responsável pelo tratamento dos dados pessoais que tome as medidas técnicas e organizativas adequadas *"para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito".* Esta obrigação da entidade responsável pelo tratamento dos dados pessoais dos eleitores para efeitos de votação electrónica não é apenas uma obrigação de procedimento, é também uma obrigação de resultado:*" estas medidas devem assegurar, atendendo*

[5] Disponível em www.cnpd.pt/bin/legal/Formulario.doc
[6] Provenientes do artigo 5º da Convenção nº 108 do Conselho da Europa para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal e da alínea a) do nº 1 do artigo 6º da Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 26 de Outubro.
[7] Catarina Sarmento e Castro, *ob. cit.*, pag. 235.
[8] Registo, no contexto utilizado nesta passagem desta obra, na interpretação da CNPD, equivale ao conceito de tratamento de dados pessoais, reportando-nos à alínea b) do artigo 3º da LPD.
[9] O artigo 7º para o qual aqui se remete é o artigo 7º da Convenção nº 108 do Conselho da Europa.
[10] Maria Eduarda Gonçalves, "Direito da Informação. Novos Direitos e Formas de Regulação na Sociedade da Informação", Almedina, 2003, Coimbra, pag. 92.
[11] Caso exista a figura de sub-contratante no tratamento de dados pessoais dos eleitores para efeitos de votação electrónica, também os nº 2 a 4 do artigo 14º da LPD devem ser observados.

aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger".[12]

Se tivermos em conta que *i)* os dados pessoais a proteger, no caso do exercício electrónico do direito de voto por parte dos cidadãos titulares e eleitores, são o nome, a morada, o número de eleitor (constantes da BDRE) e a opção de voto efectivamente tomada[13] numa eleição política, que *ii)* existe um risco particularmente significativo de ataques externos aos dados pessoais dos eleitores no exercício electrónico do direito de voto político, atenta a vulnerabilidade dos computadores, sobretudo se estiverem ligados a uma rede aberta[14] e, ainda, que *iii)* a eleição política é, porventura, o cerne dos regimes e das sociedades democráticas[15], as regras e os resultados, no que toca à segurança dos dados pessoais objecto de tratamento, são, necessariamente, as mais exaustivas e os mais exigentes. *"A garantia de segurança traduz-se na salvaguarda da informação, mas também na manutenção da sua integridade, através da adopção de medidas que impeçam a alteração dos dados, que permitam detectar disfuncionalidades e corrigi-las",* e *" impõe que os responsáveis pelos tratamentos impossibilitem a difusão ou o acesso não autorizados de dados pessoais, assim se garantindo a sua confidencialidade".*[16] [17]

*

[12] 2ª parte do nº 1 do artigo 14º da LPD.

[13] Ver a noção de dado pessoal da 1ª parte da alínea a) do artigo 3º da LPD: "*qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável"*.

[14] Francisco Carneiro Pacheco Andrade, "Algumas Considerações Relativas ao Voto Electrónico", Eleições nº 9, Revista de Assuntos Eleitorais, Setembro de 2005, STAPE, 2005, Lisboa, pag. 15.

[15] "*Na democracia moderna, que é essencialmente representativa, o povo participa no poder sobretudo através da eleição"*: Diário da Assembleia Constituinte, nº 107, de 4 de Fevereiro de 1976, pag. 3517, *in* Jorge Miranda, "Estudos de Direito Eleitoral", Lex, 1995, Lisboa, pag. 68

[16] Catarina Sarmento e Castro, *ob. cit.*, pag.267

[17] Abstemo-nos de introduzir aqui a questão de nos colocarmos, ou não, perante dados pessoais sensíveis, na classificação do nº 1 do artigo 7º da LPD (decorrente do nº 3 do artigo 35º da CRP e do nº 1 do artigo 8º da Directiva 95/46/CE do Parlamento Europeu e do Conselho), uma vez que é objecto de tratamento a opção de voto do eleitor titular numa eleição política. Apenas referenciamos que, caso seja esse o entendimento, medidas especiais de segurança, como as previstas no artigo 15º da LPD, devem ser tomadas pela entidade responsável. De qualquer maneira, como dissemos, por imposição do nº 1 do artigo 14º da LPD, consideramos que no âmbito da votação política por meios electrónicos, a obrigação de procedimentos e de resultados no que toca à segurança da integridade, fiabilidade e confidencialidade dos dados pessoais é a mais exigente que se pode impor a qualquer entidade responsável pelo tratamento.

Por outro lado, para que se torne admissível o seu tratamento, os dados pessoais dos eleitores têm de ser recolhidos para finalidades determinadas, explícitas e legítimas[18], não podendo ser posteriormente tratados de forma incompatível com essas finalidades (alínea b) do nº 1 do artigo 5º da LPD); adequados, pertinentes e não excessivos relativamente à finalidade para que são recolhidos e posteriormente tratados (alínea c) do nº 1 do artigo 5º da LPD); exactos e actualizados (alínea d) do nº 1 do artigo 5º da LPD); e conservados apenas durante o período necessário à prossecução da finalidade (alínea e) do nº 1 do artigo 5º da LPD).

Em consonância com o que foi dito imediatamente atrás, é da responsabilidade do responsável pelo tratamento assegurar a observância do disposto nestas, através de medidas técnicas de segurança e actualização das informações, da facultação de acesso aos titulares para correcção ou eliminação de dados e, em geral, da sua diligência.

*

Mas estes princípios da transparência, da licitude e da lealdade no tratamento dos dados pessoais para efeitos de votação electrónica em eleição política significam, igualmente, o respeito pelas normas de direito eleitoral. Em especial, o princípio da licitude, expressamente enunciado na alínea a) do nº 1 do artigo 5º da LPD, o qual, portanto, vincula todo e qualquer tratamento de dados pessoais e apela à especial atenção aos preceitos legais de direito eleitoral. *"Licitude do tratamento é aferida pela verificação do cumprimento das regras nacionais, comunitárias, europeias e internacionais a que está sujeito"* e *"não pode ser contrário à boa fé".*[19] Ou, numa formulação negativa mas mais abrangente, a ilicitude é uma *"agressão à ordem estabelecida numa instituição, numa comunidade, quer estadual ou não. E, talvez, numa visão global da ordem normativa, se concebam também as ilicitudes como agressões a todas as normas de conduta social"*.[20]

Deste modo, o tratamento de dados pessoais dos eleitores para efeitos de votação electrónica em eleição política teria sempre de respeitar os princípios do direito de

[18] *"Quanto à noção de legitimidade, ela acha-se ligada ao exercício de poderes. Nesse sentido se afirma que uma autoridade é legítima, ou que alguém não tem legitimidade para recorrer de um acto administrativo, para impugnar um acto tributário, ou para interpor uma acção judicial"*. Parece, diferentemente, que o termo «legitimidade», nesta alínea b) do nº 1 do artigo 5º da LPD, mais se aproxima da noção mais ampla de «legalidade» como sinónimo *"de todas as normas criadas, ou recebidas, ou toleradas pelo poder político"*: Soares Martinez, *ob. cit.*, pag. 556.
[19] Ainda Catarina Sarmento e Castro, *ob. cit.*, pag. 235.
[20] Soares Martinez, Filosofia do Direito, Almedina, Coimbra, 2003, pag. 555.

sufrágio da universalidade do voto, da igualdade do voto, do voto directo e do voto secreto.[21]

*

"De acordo com a alínea a) do nº 1 do artigo 5º (da LPD), *o tratamento de dados pessoais, e de saúde, só é* ***lícito*** *desde que conforme os princípios jurídicos de legalidade deste tipo de dados. (…) A licitude reconduz-nos, assim, e desde logo, às condições de legitimidade deste tipo de tratamento".* [22]

Não importa, de novo se reconhece, agora a propósito das condições de legitimidade do tratamento, uma vez que o dado pessoal opção de voto numa eleição política é objecto de processamento, trazer aqui a questão de sabermos se estamos perante um tratamento de dados pessoais sensíveis.

Parece incontornável, no entanto, à CNPD, que o tratamento de dados pessoais dos eleitores para fins de eleição política através de exercício do voto por meios electrónicos tem de encontrar a sua legitimidade sedimentada em lei da Assembleia da República, atendendo, não ao nº 2 do artigo 7º da LPD e ao nº 3 do artigo 35º da CRP, mas agora, porque se trata de matéria eleitoral, à devida submissão à alínea a) do artigo 64º da Lei Fundamental. Se as experiências não vinculativas atrás descritas puderam encontrar a sua condição de legitimidade, no que toca ao tratamento dos dados pessoais dos eleitores, na alínea d) do artigo 6º da LPD – execução de uma missão de interesse público ou no exercício de autoridade pública em que esteja investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados – o tratamento de dados pessoais dos eleitores para efeitos de votação electrónica no âmbito das eleições políticas, para o efectivo exercício de direito de voto dos cidadãos eleitores, terá de encontrar a sua legitimidade em lei emanada da Assembleia da República. Aliás, tanto assim terá de ser que as normas legais das eleições políticas terão de ser alteradas de modo a que a votação electrónica se mostre compatível e/ou conforme algumas das regras de direito eleitoral: vejam-se os casos da exigência do voto presencial (artigo 79º nº 3 da Lei 14/79 de 16 de Maio, na actual redacção e artigo 70º nº 1 da Lei 319/76 de 3 de Maio), a pessoalidade do voto (nº 2 do artigo 70º da Lei 319/76 de 3 de Maio), os requisitos de exercício do voto (artigo 83º e 75º da Le 14/79 e da Lei 319/76, respectivamente), o local de exercício de

[21] Maria de Fátima Abrantes Mendes, Jorge Miguéis, "Lei Eleitoral da Assembleia da República", Edição dos Autores, 2002, Torres Novas, pag. 30.
[22] Autorização da CNPD nº 478/2003.

voto (artigos 84º e 76º das ditas Lei 14/79 e Lei 319/76, respectivamente), a proibição da presença de não eleitores no local da votação (artigo 93º e 84º das referidas Leis), os requisitos dos boletins de voto (artigo 95º e artigo 86º das referidas Leis e pela mesma ordem), bem como as normas do modo de votação, as regras de apuramento e os ilícitos eleitorais, todos exemplos da imprescindibilidade de diploma legal emergente do Parlamento que oferecesse condições de legitimidade para o tratamento (lícito) de dados pessoais dos eleitores para a finalidade da votação electrónica no âmbito de eleições políticas.[23]

[23] Trouxemos aqui, não mais do que para ilustrar as condições de legitimidade do tratamento de dados pessoais dos cidadãos eleitores no âmbito das eleições políticas, apenas as leis eleitorais para a Assembleia da República e para o Presidente da República, conforme se encontram actualizadas, anotadas e comentadas por Maria de Fátima Abrantes Mendes e Jorge Miguéis, a primeira na edição apontada na nota 19 e a segunda na "Lei Eleitoral do Presidente da República", Edição dos Autores, 2000, Torres Novas. Não se revelou necessário, porque excede a economia desta declaração de princípios da CNPD, trazer a Lei Eleitoral para as Autarquias Locais, a Lei do Referendo Nacional e a Lei do Referendo Local, pois não se trata aqui de estudar o exercício do direito de voto através de meios electrónicos no actual regime de direito eleitoral, mas sim e apenas analisar esse exercício no quadro do actual regime da protecção de dados pessoais.

III – CONSIDERANDOS E RECOMENDAÇÕES DA CNPD

Considerando que:

1. Os princípios e regras de direito eleitoral – a oficiosidade, obrigatoriedade, permanência e unicidade do recenseamento eleitoral, o sufrágio directo, secreto e universal, a liberdade e unicidade do voto – são alicerces incontornáveis e inabaláveis para a manutenção da democraticidade dos regimes e para a subsistência das sociedades democráticas;
2. O respeito por esses princípios e regras de direito eleitoral reflecte-se, no que concerne à protecção de dados pessoais, não apenas na qualidade dos dados pessoais dos eleitores, mas também na licitude, boa fé e legitimidade do tratamento de dados pessoais dos eleitores, condições que ditam a admissibilidade de qualquer tratamento de dados pessoais;
3. O desenvolvimento tecnológico deve servir a sociedade democrática e contribuir para o aprofundamento da democracia e aumento da participação cívica, colectiva e pública;
4. O desenvolvimento e alastramento das tecnologias de informação e comunicação (TIC´s), ao mesmo tempo que podem servir o aprofundamento da democracia e o aumento da participação, também podem comportar riscos de manipulação e viciação das regras democráticas e da autenticidade da participação;
5. A transparência e a linearidade dos processos eleitorais, nomeadamente dos processos de votação electrónica, são condições indispensáveis à criação e estabelecimento de um clima de confiança dos cidadãos nas instituições, nos regimes e nas sociedades democráticas;
6. A confiança dos cidadãos nos processos eleitorais democráticos, nomeadamente nos processos de votação electrónica, reside na imagem que os cidadãos representam e projectam sobre aqueles princípios e regras eleitorais;
7. A representação e projecção dos cidadãos sobre os ditos princípios e regras eleitorais, nomeadamente sobre o secretismo e fiabilidade do

voto, depende, em grande medida, do valor simbólico do respeito por esses princípios e regras no acto de votação;

8. Na ponderação entre as potenciais vantagens da introdução das TIC´s nos processos eleitorais – seja na votação electrónica – e os potenciais riscos decorrentes dessa utilização, devem ser tidos em conta os princípios jurídicos da prevenção e da precaução;
9. No que toca à protecção de dados pessoais, existem riscos de efectivos perigos e desvantagens na introdução das TIC´s nos processos eleitorais, nomeadamente nos processos electrónicos do exercício do direito de voto, tais como, entre outros:
    a. Riscos de manipulação do *software* e de desvirtuação do voto no momento da votação, intencionais ou decorrentes dos erros de concepção ou definição dos sistemas;
    b. Riscos de manipulação do *software* no momento do apuramento dos resultados, intencionais ou decorrentes de erros na concepção ou definição dos sistemas;
    c. Riscos de intromissão na comunicação da informação, intencionais ou decorrentes de erros de concepção ou definição dos sistemas;
    d. Fortes pressões informativas, propagandísticas e manipuladoras sobre os eleitores, exercidas pelos mesmos meios electrónicos que são utilizados no exercício do direito de voto e até ao momento do efectivo exercício do voto, que a ciência e a tecnologia ainda não permitem afastar;
    e. Risco de prejuízo dos princípios e regras de direito eleitoral;
    f. Relação de troca entre a segurança (encriptação, por exemplo) e a acessibilidade (desencriptação, eliminação de vírus, entre outras medidas de acessibilidade);
    g. Riscos de desigualdades decorrentes de diferentes níveis de conhecimentos por parte dos eleitores sobre os comportamentos adequados na votação electrónica;
    h. Riscos de distanciamento ou mesmo exclusão dos eleitores inadaptados às TIC´s (“info-excluídos”);
    i. Tendência, por princípio, para os sistemas registarem a identidade, o momento temporal e o local geográfico da votação, bem como a opção de voto;

j. Dificuldade ou mesmo impossibilidade de detecção de viciação que opera apenas no voto já depositado na urna electrónica;
k. Existem diferentes níveis de regras de segurança, consoante o espaço geográfico (local, regional, nacional ou internacional) da votação;

10. A introdução das TIC´S no processo eleitoral deve ser feita por etapas, de modo totalmente transparente, com inteira assimilação e aceitação por parte dos cidadãos e com absoluta segurança sobre o mérito e a vantagem da utilização dessas tecnologias;
11. O maior contributo para a redução da abstenção é a criação de circunstâncias que viabilizem a mobilidade geográfica dos eleitores de modo a permitir-lhes exercer o direito de voto em diferentes locais e em igualdade de condições.
12. A verificação de um erro ou viciação no processo de votação electrónica produz, não apenas prejuízos e danos que afectam de modo irreparável as instituições democráticas e o funcionamento da democracia, mas efectivos prejuízos para a protecção de dados pessoais dos eleitores;
13. Os países europeus pioneiros nas experiências de votação electrónica, vinculativas e não vinculativas, presenciais e não presenciais, tais como a Grã-Bretanha, a França, a Bélgica, a Irlanda, abandonaram a intenção de introduzirem os processos de votação electrónica, em virtude do nível actual de conhecimentos e garantias sobre esses processos;
14. No Brasil, país com dimensão geográfica tipicamente continental em que o recurso às TIC´s se justificou por essa mesma dimensão, o maior proveito desse recurso respeitou mais à diminuição do número de votos inválidos do que ao aumento da participação eleitoral;
15. Há países (alguns estados federados dos Estados Unidos da América, por exemplo) onde houve notícias que abalaram a fidelidade dos votos electrónicos e a fiabilidade dos resultados eleitorais, decorrentes directamente da utilização de TIC´s e dos processos de votação electrónica;

Tendo presente o teor da Recomendação R (2004) 11 do Comité de Ministros do Conselho da Europa;

Tendo presente a totalidade do conteúdo do Segundo Documento de Trabalho sobre a Protecção de Dados Pessoais na Votação Electrónica em Linha para as Eleições

Legislativas e Governamentais do Grupo Internacional de Trabalho sobre a Protecção de Dados Pessoais nas Telecomunicações adoptado em 31 de Março/1 de Abril de 2005, na ilha da Madeira, Portugal;

Tendo em conta as conclusões extraídas do acompanhamento e análise das experiências não vinculativas de voto electrónico, presencial e não presencial, atrás referenciadas;

A CNPD **recomenda** que:

1. Sobre a votação electrónica e a introdução das TIC´s nos processos eleitorais, devem ser observados os princípios jurídicos da prevenção e da precaução, em favor dos princípios e regras de direito eleitoral e em homenagem à democraticidade das instituições, dos regimes e das sociedades.
2. A introdução das TIC´s nos processos eleitorais e o recurso à votação electrónica não devem afectar, ameaçar ou sequer aparentar que podem afectar ou ameaçar os princípios e regras de direito eleitoral, nomeadamente, a oficiosidade, obrigatoriedade, permanência e unicidade do recenseamento eleitoral, o sufrágio directo, secreto e universal, a liberdade e a unicidade do voto.
3. Devem ser realizados, de forma alargada e aprofundada, por um lado, e com carácter regular e sucessivo, por outro, debates públicos com vasta divulgação sobre as experiências não vinculativas, presenciais e não presenciais, de votação electrónica, bem como sobre a eventual ou futura introdução de TIC´s e da votação electrónica nas eleições e referendos políticos.
4. Deve ser feita uma ampla e aprofundada campanha de informação da comunidade informática, política e líderes de opinião sobre as experiências não vinculativas, presenciais e não presenciais, de votação electrónica e sobre a eventual ou futura introdução das TIC´s nos processos políticos eleitorais, nomeadamente sobre as características das tecnologias e sobre a operacionalidade dos procedimentos, com identificação específica e avaliação concreta dos riscos inerentes às experiências e à dita introdução das TIC´s.
5. As experiências não vinculativas, presenciais e não presenciais, de votação electrónica e a eventual ou futura introdução das TIC´s nos processos políticos eleitorais devem conhecer processos faseados de concepção, definição e implementação, devendo as diversas etapas e fases ser abertas à participação

pública, quer das instituições políticas e sociais, quer dos peritos, quer ainda cidadãos.

6. Os eleitores e entidades envolvidas nos processos eleitorais devem ser informados detalhada e convenientemente sobre a organização das experiências e da utilização das TIC´s nos processos eleitorais de votação electrónica com grande antecedência temporal face à data das eleições.
7. A informação dos eleitores e das entidades envolvidas nos processos eleitorais deve ser prestada através de mais do que um canal de circulação da informação, tal como as campanhas publicitárias, os meios de propaganda e a divulgação dos guias de votação electrónica devem utilizar diversos meios de comunicação com os destinatários.
8. A tecnologia utilizada deve apresentar robustez, devem os sistemas e todas as suas alterações ser previamente notificados e, ainda, ser oficialmente publicado o *software*.
9. Os sistemas utilizados e todo o *software* empregue devem ser constituídos por códigos-fonte abertos, totalmente passíveis de serem auditados prévia e ulteriormente à realização das experiências não vinculativas, presenciais e não presenciais, de votação electrónica e da eventual introdução das TIC´s nos processos políticos eleitorais, sendo ainda permitida a avaliação, quer por entidades independentes, quer pelas entidades políticas envolvidas.
10. Os sistemas e os equipamentos utilizados devem ser efectiva e exaustivamente verificados e comparados com aqueles que foram notificados e publicados.
11. O recenseamento eleitoral, bem como a actualização, correcção e eliminação de dados de identificação dos eleitores, deve ser feito com recurso a meios electrónicos de funcionamento e registo.
12. Deve ser criada a rede electrónica dos cadernos eleitorais, com total cobertura do território nacional, que permita a mobilidade espacial dos eleitores e lhes faculte a possibilidade de exercerem o direito de voto em local diferente do da assembleia eleitoral onde se encontra recenseado.
13. A identificação dos eleitores, no caso de experiências de votação electrónica não presencial, deve ser feita em dois momentos diferentes, um com grande antecedência temporal face ao acto eleitoral e outro em altura mais próxima da data da eleição, em cada um dos casos atribuindo uma palavra-passe diferente aos eleitores.

14. A votação electrónica deve ser um meio adicional ou complementar de exercício do direito de voto, a par dos meios tradicionais de votação, presenciais e por via postal.
15. Além da votação electrónica e da urna de votos electrónica, deve ser emitido ao eleitor um recibo de voto em papel, onde conste a sua opção de voto, devendo o eleitor depositar esse recibo numa urna tradicional de boletins de votos expressos em papel.
16. Na mesma máquina electrónica não devem estar as bases de dados da identificação dos eleitores e dos votos dos eleitores. Estas duas bases de dados devem estar fisicamente separadas e, quando tal não seja possível, o registo dos dados pessoais dos eleitores e a sua autenticação devem ser feitos pelo método tradicional de papel.
17. Os procedimentos, os boletins e os *interfaces* de votação devem ser totalmente iguais em todo o território nacional ou, nas eleições regionais e locais, na respectiva circunscrição eleitoral, utilizando a mesma língua e a mesma linguagem, de forma interactiva e de fácil compreensão.
18. O tempo de votação electrónica deve ser sobejamente suficiente para os eleitores tomarem as suas opções e interagirem com os *interfaces* de modo a efectuarem as suas votações, sem precipitações e sem qualquer informação opinativa ou sugestiva sobre as opções de votos.
19. Aos eleitores deve ser oferecida a possibilidade de, num determinado hiato temporal durante a votação, alterarem as opções de voto que efectivamente tomaram e expressaram pelos meios electrónicos de votação, sem haver qualquer registo dessas mesmas alterações.
20. Após a votação, devem ser imediatamente eliminadas as opções de voto tomadas pelos eleitores, devendo ainda ser apagados os registos temporais e de ordem de entrada dos votos electronicamente expressos.
21. Após o encerramento das urnas de voto, depois do exacto momento do termo do acto eleitoral, os sistemas e o *software* não devem permitir a realização de novas votações, mas devem permitir a entrada dos votos já exercidos mas ainda não depositados nas urnas electrónicas.
22. Os sistemas e o *software* devem oferecer condições técnicas para a contagem electrónica de votos, a par da contagem de votos em suporte de papel.
23. A comunicação electrónica dos dados pessoais dos eleitores e dos resultados das votações, mesmos os parcelares e intercalares, deve ser feita de forma encriptada, através de uma infra-estrutura privada e protegida (não através de

redes públicas de comunicação como as telefónicas ou redes abertas tipo Internet).

24. Todas as ocorrências com possibilidades, efectivas ou potenciais, de interferência com os eleitores ou afectação dos votos devem ser registadas.
25. Todas as intervenções devem ser autorizadas e apenas o devem ser as que forem levadas a efeito por pessoas credenciadas, em equipas plurais e rotativas, sob tutela superior de entidades de composição mista mas de natureza pública.
26. Após as experiências não vinculativas, presenciais e não presenciais, de votação electrónica e depois da introdução das TIC´s nos processos políticos eleitorais, as conclusões das auditorias devem ser anunciadas e divulgadas com transparência, reservando e envolvendo sempre o anúncio dos resultados em prudentes sobriedade e discrição.
27. As experiências não vinculativas, presenciais e não presenciais, de votação electrónica e a introdução das TIC´s nos processos políticos eleitorais devem conduzir à intensificação da utilização ou re-utilização dos meios electrónicos, de toda a tecnologia e de todos os conhecimentos adquiridos e desenvolvidos, em outras formas de participação cívica e política diferentes das eleições legislativas e governamentais e dos referendos.
28. Sejam excluídas as experiências de votação electrónica não presencial e a utilização das TIC`s para o exercício, contagem de votações electrónicas e comunicação de resultados, em favor das experiências de votação electrónica presencial, concomitantes com a votação em moldes tradicionais, observando as considerações e recomendações atrás expostas.

* Deliberação aprovada pela Comissão Nacional de Protecção de Dados – CNPD, na sessão de 14 de Novembro de 2005