COMISSÃO NACIONAL
DE PROTEÇÃO DE DADOS

PARECER/2020/117

I – Pedido

A Comissão dos Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República solicitou à Comissão Nacional de Proteção de Dados (CNPD) que se pronunciasse sobre o Projeto de Lei n.º 498/XIV/1.ª, de iniciativa do grupo parlamentar do PAN – Pessoas Animais Natureza, que *aprova a Carta dos Direitos Digitais e um conjunto de medidas complementares que asseguram o reforço das garantias dos cidadãos no domínio digital.*

O pedido formulado e o presente parecer enquadram-se nas atribuições e competências da CNPD enquanto autoridade nacional de controlo dos tratamentos de dados pessoais, nos termos do disposto na alínea *c)* do n.º 1 do artigo 57.º e no n.º 4 do artigo 36,º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral de Proteção de Dados - RGPD), em conjugação com o disposto no artigo 3.º, n.º 2 do artigo 4.º e da alínea *a)* do n.º 1 do artigo 6.º, todos da Lei n.º 58/2019, de 8 de agosto, a qual tem por objeto assegurar a execução do RGPD na ordem jurídica interna.

A apreciação da CNPD cinge-se à apreciação das normas quer preveem ou regulam o tratamento de dados pessoais.

II – Apreciação

O Projeto de lei em apreço tem em vista assegurar *o reforço das garantias dos cidadãos no domínio digital, sem limitar os direitos fundamentais actualmente já previstos na Constituição e na lei.*

Todavia, o articulado do Projeto parece esquecer-se que muitos dos direitos, aqui consagrados como digitais, já estão reconhecidos, e com um âmbito bem delimitado, em instrumentos jurídicos vinculativos para o Estado português. E, portanto, consagrados e delimitados em termos tais que não podem agora, no plano legislativo nacional, ser alterados, mesmo que num sentido expansivo das posições subjetivas dos titulares dos dados.

É por este ponto que se inicia a presente análise, sem deixar de destacar que algumas das normas do presente Projeto empregam conceitos cuja definição consta de diplomas legais de Direito da União, tendo por isso um sentido específico, mas que não são, nem por

remissão, explicados no articulado do Projeto, o que dificulta a interpretação dessas normas, inclusive quanto ao seu âmbito de aplicação, prejudicando a previsibilidade e certeza jurídica que normas consagradoras de direitos, a que correspondem obrigações de terceiros, não podem deixar de assegurar.

1. A desconformidade de normas do Projeto com o Direito da União Europeia

Ao longo do Projeto são enunciados direitos já consagrados, não apenas na Constituição da República Portuguesa, na Carta dos Direitos Fundamentais da União Europeia e na Convenção Europeia dos Direitos do Homem, como também em convenções de âmbito mais específico[1] e ainda em diplomas da União Europeia diretamente aplicáveis na ordem jurídica portuguesa, como sucede com o RGPD.

Se se admite que o Projeto de lei não pretende afastar, no contexto do ciberespaço, as normas vigentes que consagram e tutelam direitos, liberdades e garantias (conforme o disposto no artigo 2.º do Projeto), a verdade é que várias das suas disposições aparentam repetir os direitos já previstos e regulados no Direito da União, em especial no RGPD, com a agravante de muitas vezes estarem redigidas em termos tais que modificam o sentido e o âmbito desses direitos.

A esse propósito recorda-se que o Tribunal de Justiça da União Europeia (TJUE) já censurou a prática de em lei nacional se replicar o teor de normas de regulamentos da União, sujeitando-as ao direito nacional e, nessa medida, afetando também a jurisdição do tribunal europeu. O TJUE sublinhou que tal cria um *equívoco no que se refere à natureza jurídica das disposições a serem* aplicadas, reiterando serem *contrárias ao Tratado quaisquer modalidades de execução que possam obstar ao efeito direto dos regulamentos*

[1] Destaque-se a Convenção 108 para a proteção das pessoas relativamente ao tratamento automatizado de dados de caracter pessoal, do Conselho da Europa, a qual foi alterada em 2018, por protocolo já assinado pelo Estado português, mas ainda não ratificado, cuja versão modernizada é comummente designada por Convenção 108+, disponível em https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808ac918

comunitários e, desse modo, possam comprometer a sua aplicação uniforme no espaço comunitário[2].

E quanto a normas nacionais que desvirtuem o sentido das normas de Direito da União, especificou o TJUE que *os Estados-Membros têm o dever de não obstruir a aplicabilidade direta inerente aos regulamentos*, sendo que *o cumprimento estrito dessa obrigação é condição indispensável para uma aplicação uniforme e simultânea dos Regulamentos por toda a Comunidade*[3].

Ora, o Projeto de Lei em análise, no esforço de congregar os direitos reconhecidos na ordem jurídica portuguesa no contexto digital, integra um conjunto de normas que se apresentam em desconformidade com o Direito da União Europeia, em termos que põem em crise o primado do Direito da União Europeia e a hierarquia das normas reconhecida pelo n.º 4 do artigo 8.º da Constituição da República Portuguesa. A CNPD entende que, em conformidade com a jurisprudência já citada, tais normas devem ser eliminadas do Projeto de Lei.

Não obstante, uma vez que, no âmbito do procedimento legislativo relativo à execução do RGPD, o legislador nacional optou, na Lei n.º 58/2019, de 8 de agosto, por manter as normas que, na perspetiva da CNPD, replicavam ou contrariavam normas do RGPD, a CNPD fará aqui recomendações que visam minorar a desconformidade com o Direito da União Europeia.

Vejamos.

1.1. Em primeiro lugar, destaca-se o **artigo 9.º**, onde se pretende regular o direito à privacidade digital.

No n.º 4, vem reconhecer-se um *direito à proteção contra a definição de perfis efetuada de forma ilegal.*

---

[2]Cf. Acórdão *Comissão/ vs. Itália* (proc. 39/72), ponto 17, in http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d2dc30ddbf94149c102f4a878610d7c0bd468c6f.e34KaxiLc3qMb40Rch0SaxyNbxz0?text=&docid=88354&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=601673

[3] Cf, o Acórdão *Variola* (proc. 34/73), ponto 10, in http://curia.europa.eu/juris/showPdf.jsf?text=&docid=88457&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=378305

Se esta previsão por si só não suscita reservas, por remeter implicitamente para o diploma onde se define os limites à definição de perfis, que, substancialmente, corresponde ao RGPD, já a exemplificação que se segue suscita as maiores reservas. Aí se explicita, como situação correspondente a uma definição de perfis efetuada de forma ilegal, *quando esteja em causa a tomada de decisões relativas a pessoa singular ou a análise das respetivas preferências, comportamento ou atitudes*.

Parece haver aqui, antes de mais, um equívoco: a tomada de decisões relativas a pessoa singular não é em si mesmo ilegal, nem a definição de perfis para servir de base à tomada de decisões relativas a pessoa singular contraria sempre a lei ou merece, *per se*, censura. A definição de perfis (*profiling*) pode ser legitimamente realizada, com o objetivo de servir a tomada de decisões sobre pessoas singulares e para analisar as suas preferências ou condutas (cf., por exemplo, o disposto na alínea *f)* do n.º 2 do artigo 13.º, alínea *g)* do n.º 2 do artigo 14.º e nos n.ºs 1 e 2 do artigo 21.º do RGPD).

O que se pretenderá eventualmente aqui ter em vista é a definição *automatizada* de perfis – a partir de informação recolhida no ambiente digital –, o que a norma em apreço não explicita – pelo que seria útil a remissão para o RGPD quanto a este conceito. Mas mesmo quanto a essa definição (*profiling*) o que se tem por ilegal, em determinadas circunstâncias, é o processo de decisão automatizado sobre uma pessoa singular a partir de perfis assim criados. Ora, essas circunstâncias estão reguladas no artigo 22.º do RGPD, não podendo o legislador nacional, independentemente da bondade do alcance que pretenda dar ao direito naquele consagrado, fixar um regime distinto do regime do Direito da União afirmando ser ilegal toda e qualquer utilização de definição de perfis *quando esteja em causa a tomada de decisões relativas a pessoa singular ou a análise das respetivas preferências, comportamento ou atitudes*.

Em suma, por um lado, o próprio conceito de *definição de perfis* utilizado no n.º 4 do artigo 9.º do Projeto só faz sentido, no âmbito deste Projeto, se se fizer uma remissão para o conceito consagrado na alínea *4)* do artigo 4.º do RGPD; por outro lado, a exemplificação contida na parte final daquela disposição contraria o regime do direito consagrado no artigo 22.º do RGPD, ao alargar os termos em que se terá por ilegal a utilização desses perfis.

A CNPD recomenda, por isso, a eliminação do n.º 4 do artigo 9.º do Projeto, ou, se assim não se entender, a revisão da sua redação em termos que não contrariem o disposto no artigo 22.º do RGPD.

Ainda no âmbito do artigo 9.º do Projeto, destaca-se a imposição, no n.º 5, de um dever de que a Administração Pública utilize ferramentas e sistemas informáticos que garantam os mais latos padrões de privacidade e segurança. Embora a CNPD subscreva que deve evita conservar-se a informação em fornecedores que comprovadamente não possam garantir a confidencialidade da informação, já tem sérias dúvidas que as regras de concorrência e de livre prestação de serviços dentro da União Europeia ou mesmo do espaço económico europeu (EEE) não sejam ameaçadas na parte em que vincula a Administração Pública a evitar, sempre que possível, manter informação em servidores não-nacionais. Recomenda-se, por isso, que esta parte seja eliminada e substituída pela referência a servidores situados em territórios de países terceiros em relação à União Europeia ou ao EEE, devendo exigir-se em todo o caso que a sua gestão esteja efetivamente atribuída às entidades administrativas.

1.2. Em relação ao artigo 12.º do Projeto, a CNPD começa por recordar que há normas do Direito da União Europeia que regulam a identificação eletrónica, destacando o Regulamento (UE) 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, pelo que o disposto no n.º 2 do artigo 12.º não pode deixar de ser lido à luz de tais regras.

Mas destaca sobretudo o preceituado no n.º 4 do artigo 12.º. Se bem se compreende o que aqui se pretende salvaguardar, a proibição de utilização de um código bidimensional não parece ser necessária, nem se afigura suficientemente garantística dos direitos das pessoas singulares.

Na verdade, não é suficientemente garantística porque não considera a possibilidade de representação de códigos de dimensão superior que afetem de igual modo os direitos das pessoas singulares, correndo por isso o risco de rapidamente se tornar obsoleta. É que ao código bidimensional, como o *QR* Code, pode seguir-se a utilização de códigos tridimensionais, ou *n* dimensionais, que permitam o tratamento de dados pessoais com igual ou, eventualmente, superior intensidade e impacto. Importa, por isso, que se encontre uma fórmula que acautele, não apenas a utilização de códigos bidimensionais, mas também de códigos de dimensão superior.

Ainda que não se desconheça que quanto maior for a dimensão mais informação contém o código, não se pode afirmar, sem mais, existir uma relação direta entre a dimensão do código e o risco para os direitos dos titulares. Com efeito, a introdução dos códigos bidimensionais,

para além da possibilidade de representação de mais informação, tornou possível, pela utilização de aplicações de fácil acesso (*v.g.,* por recurso a *smartphone*), a leitura da representação do código. Ora, é da facilidade de leitura da representação dos códigos e, portanto, da suscetibilidade do conhecimento generalizado da informação aí contida, que pode advir uma maior afetação dos direitos das pessoas singulares. É este resultado que é necessário evitar.

É nesta perspetiva, e considerando que os códigos dimensionais podem ser ferramentas de grande utilidade, que a CNPD considera que a proibição dos códigos bidimensionais, sem mais, como uma medida demasiado radical e desnecessária.

Deste modo, a CNPD recomenda que, em vez da proibição absoluta da utilização deste tipo de códigos, e em linha com as medidas de segurança previstas no artigo 32.º do RGPD, se admita, em alternativa à proibição, que a representação seja sujeita a um método de cifragem segura à informação previamente à geração do código.

A CNPD atreve-se a sugerir a seguinte redação para o n.º 4 do artigo 12.º do Projeto: É proibida qualquer forma de utilização de código bidimensional, *ou de dimensão superior,* para tratar informação sobre o estado de saúde ou qualquer outro aspeto relacionado com direitos de pessoas singulares, *salvo se for aplicada uma cifragem segura à informação previamente à geração do código.*

1.3. Ainda quanto aos direitos consagrados no RGPD e que no Projeto vêm reafirmados no contexto digital, importa agora analisar o direito previsto no **artigo 13.º** do Projeto.

Em primeiro lugar, assinala-se que a designação do direito como *direito ao esquecimento* não é a mais adequada (ainda que esteja vulgarizada), uma vez que o sentido do direito corresponde a uma pretensão "a ser esquecido" (cf. epígrafe do artigo 17.º do RGPD), o que não contradiz o direito à memória. A CNPD recomenda, por isso, a alteração da epígrafe do artigo 13.º do Projeto para *Direito a ser esquecido.*

Em segundo lugar, a CNPD reitera a sua preocupação pela opção legislativa de se procurar reproduzir as normas do RGPD no específico contexto digital com o risco de desvirtuamento do âmbito do direito definido naquele diploma, e que a referência aos "termos da lei" pode não ser suficiente para o afastar. Tome-se como exemplo, a menção no n.º 1 do artigo 13.º do Projeto, entre um curto elenco dos motivos justificativos deste direito, a "por outra razão

relevante". Tal referência parece deixar um espaço discricionário ao aplicador da norma legal, quando na verdade os fundamentos da titularidade e exercício deste direito estão *taxativamente* elencados no n.º 1 do artigo 17.º do RGPD e em termos mais extensos do que os aqui enumerados.

Mais uma vez se recomenda que, a persistir-se na referência a este direito no quadro do presente Projeto de diploma, se remeta para os fundamentos ou motivos previstos no artigo 17.º do RGPD.

No que diz respeito ao n.º 2 do mesmo artigo 13.º do Projeto, recomenda-se a revisão da redação do mesmo, porquanto ele comporta uma interpretação que ultrapassaria o âmbito do direito à desassociação do resultado de uma pesquisa a partir do nome do titular dos dados no motor de busca, tal como ele foi reconhecido pelo TJUE[4] e está consagrado no citado artigo 17.º do RGPD.

Na verdade, a redação atual permite a interpretação de que a pesquisa *na fonte digital* da qual consta a informação sobre o titular dos dados não pode ser feita a partir do nome do titular, quando a *ratio* da norma parece ser a de reconhecer que o direito de eliminação dos resultados da pesquisa no motor de busca a partir do nome do titular não prejudica uma pesquisa *no motor de busca* a partir de outro termo, que não o nome do titular. É importante aqui distinguir, pelo impacto completamente diferente que tem nos direitos dos titulares, uma pesquisa realizada num motor de busca de âmbito nacional ou internacional, ou uma pesquisa cingida apenas a um sítio da Internet e, por conseguinte, apenas agregadora da informação constante daquele *website* e não de toda a Internet.

A CNPD recomenda, por isso, uma clarificação da redação deste n.º 2 do artigo 13.º do Projeto.

Em terceiro lugar, a imposição, no n.º 3 do artigo 13.º, do exercício do direito ao apagamento dos dados pessoais fornecidos a redes sociais ou serviços da sociedade de informação *mediante formulário digital simples* e da sua garantia *em prazo razoável,* vai mais longe do que estatui – em termos vinculativos para os Estados-Membros – o artigo 12.º do RGPD. Aí se impõe ao responsável pelo tratamento a obrigação de facilitar o exercício dos direitos, e

[4] Cf. Acórdão *Google Spain SL Google Inc v. Agencia Española de Protección de Datos*, de 13 de maio de 2014, no processo C-131/12.

se determina um prazo máximo de um mês a contar da receção do pedido, prorrogável (cf. n.ºs 2 e 3 do artigo 12.º do RGPD).

Acresce que se está a limitar os fundamentos de eliminação dos dados pessoais aos casos de dados obsoletos ou inexatos, o que, reitera-se, contraria grosseiramente o estatuído no n.º 1 do artigo 17.º do RGPD.

De resto, a CNPD chama a atenção para a delimitação do contexto em que se pretende aqui regular este direito, uma vez que o conceito de *serviços da sociedade de informação* tem um sentido bem delimitado na Diretiva (UE) 2015/1535, do Parlamento Europeu e do Conselho, e não se alcança o que sejam serviços *similares*. Razões de previsibilidade das normas legais justificam, pois, também aqui rigor nos conceitos empregues e a clarificação dos mesmos.

Nessa medida, a norma deve ser eliminada ou revista, por estar a impor o meio de cumprimento da obrigação quando o RGPD não o fez e por se reportar a um prazo razoável que foi já concretizado pelo legislador europeu, em desrespeito pelo artigo 12.º do RGPD, e ainda por restringir o âmbito do direito ao apagamento de dados pessoais previsto no artigo 17.º do RGPD.

Finalmente, não se compreende o alcance do n.º 4 do artigo 13.º do Projeto. A previsão de que os *dados respeitantes a menores são eliminados sem a limitação prevista no número anterior* tanto pode reportar-se-á à exigência de um formulário digital para o exercício do direito e à garantia do mesmo num prazo razoável, como aos fundamentos de exercício desse direito, que no n.º 3 vêm limitados à inexatidão ou ao carácter obsoleto dos dados. Importa, por isso, clarificar o sentido da norma.

De todo o modo, qualquer que seja o seu sentido, esta disposição é desnecessária, porquanto o direito de apagamento dos dados pessoais de menores recolhidos no contexto da oferta serviços da informação referidos no artigo 8.º, n.º 1, do RGPD, está consagrado na alínea *f)* do n.º 1 do artigo 17.º do mesmo diploma.

1.4. Atente-se ainda no n.º 1 do **artigo 14.º** do Projeto, quando se reporta ao direito dos utilizadores de plataformas digitais, de serviços *over-the-top* e similares de obterem *cópia dos dados que lhe[s] dizem respeito de forma interoperável e o apagamento desses dados na plataforma.*

Em primeiro lugar, por razões de previsibilidade normativa, conviria uma definição, para efeito deste diploma, do conceito de plataformas digitais e de serviços *over-the-top*, de forma que, desde logo, se possa compreender a que correspondem os serviços similares, sob pena de falta de previsibilidade e certeza jurídica deste regime legal. De todo o modo, o direito que parece estar aqui em causa é o direito de portabilidade dos dados, consagrado no artigo 20.º do RGPD, o qual, aqui, por se reportar à alteração das condições contratuais, se enquadra na alínea *a)* do n.º 1 do artigo 20.º do RGPD, mas restrito aos tratamentos de dados pessoais realizados com fundamento em contrato.

Todavia, o direito de portabilidade não implica necessariamente a eliminação dos dados pessoais por parte do responsável pelo tratamento. O direito à eliminação existe nos casos previstos no n.º 1 do artigo 17.º do RGPD e, para o que aqui releva, poder-se-á afirmar quando cesse o fundamento de licitude do tratamento ou os dados deixem de ser necessários (por ter terminado a relação contratual). Simplesmente, há circunstâncias, de acordo com o n.º 3 do artigo 17.º, que podem justificar a conservação dos dados (*v.g.*, para defesa de direitos em processos judiciais, para cumprimento de obrigações legais em matéria fiscal e de combate ao branqueamento de capitais).

Sendo certo que o legislador nacional pode criar obrigações legais de eliminação dos dados, nos termos da alínea *e)* do n.º 1 do artigo 17.º do RGPD, a CNPD recorda, ainda assim, que podem existir razões para a conservação dos dados, recomendando por isso a reponderação desta disposição.

1.5. No que diz respeito ao *direito à proteção contra a geolocalização abusiva*, consagrado no artigo 16.º do Projeto, a CNPD começa por insistir, mais uma vez, na necessidade de se esclarecerem os conceitos empregues, que correspondem, na verdade, a conceitos definidos em diplomas do Direito da União.

É o que sucede com vários termos utilizados neste artigo (por exemplo, o conceito de *chamada*), que se reportam à Lei da Privacidade das Comunicações Eletrónicas (Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto), a qual transpôs a Diretiva *e-Privacy* (Diretiva 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, com as alterações introduzidas pela Diretiva 2009/136/ CE, do Parlamento Europeu e do Conselho, de 25 de novembro).

Não tendo a CNPD reservas quanto à generalidade das disposições deste artigo, entende, porém, que a redação do n.º 2 carece de clarificação e de revisão.

Decorre deste preceito que os dados pessoais de geolocalização, no âmbito de redes públicas móveis ou fixas, *só podem ser utilizados pelas autoridade[s] legalmente competentes nos domínios da proteção civil, saúde pública e investigação criminal.*

Sucede que o regime do tratamento destes dados encontra-se regulado na Lei da Privacidade das Comunicações Eletrónica, a qual transpôs a Diretiva *e-Privacy,* onde se admite o tratamento dos dados de geolocalização pelas operadoras de comunicações eletrónicas em determinadas circunstâncias (cf. artigo 7.º da Lei da Privacidade das Comunicações Eletrónicas). No entanto, tal como se encontra redigido, o n.º 2 do artigo 16.º do Projeto parece proibir o tratamento desses dados nos casos previstos no artigo 7.º daquela lei nacional, o que contaria a Diretiva *e-Privacy.*

Por outro lado, a autorização de tratamento destes dados pelas *autoridades legalmente competentes nos domínios da proteção civil, saúde pública e investigação criminal* alarga o universo de entidades legitimadas pela Lei n.º 41/2004 (n.º 2 do artigo 7.º) e pela própria Diretiva *e-Privacy* (alínea *b)* do artigo 10.º e considerando 36) a tratar os dados de geolocalização: nestes diplomas apenas autoridades competentes por lei para receber e responder a chamadas de emergência estão autorizadas a tratar tais dados e não todas as autoridades com competência em matéria de proteção civil e de saúde pública.

Ainda que a Diretiva *e-Privacy* reconheça, no seu artigo 15.º, aos Estados-Membros o poder de, por lei, a restringir os direitos à inviolabilidade e confidencialidade das comunicações eletrónicas, dos dados de tráfego e dos dados de geolocalização, essa restrição deve revelar-se adequada, necessária e não excessiva em relação às finalidades visadas, uma vez que está em causa a restrição aos direitos fundamentais ao respeito pela vida privada e da inviolabilidade das comunicações, consagrados no artigo 7.º da Carta dos Direitos Fundamentais, e nos artigos 26.º e 34.º da Constituição Portuguesa. Sobretudo nos termos abertos, não circunstanciados, em que se prevê tal acesso. Tendo também em conta que esta norma derroga a alínea *b)* do artigo 10.º da Diretiva e altera parcialmente o disposto no n.º 2 do artigo 7.º da Lei n.º 41/2004, estranha-se que a exposição de motivos não o refira expressamente, nem seja demonstrada a adequação e necessidade do alargamento do universo de entidades administrativas com poder para conhecer os dados de localização no contexto das comunicações eletrónicas.

A CNPD recomenda, por isso, a ponderação do estatuído no n.º 2 do artigo 15.º, sublinhando que ele traduz a derrogação parcial de normas previstas na Lei n.º 41/2004 e na Diretiva *e-Privacy*, e que, também pelos termos abertos em que vem previsto o acesso, parece violar o princípio da proporcionalidade (cf. n.º 2 do artigo 18.º da CRP e n.º 1 do artigo 52.º da Carta).

2. Análise de outras disposições legais

Ainda na perspetiva da compatibilidade das normas do Projeto com o regime de proteção de dados pessoais e de segurança dos dados pessoais, a CNPD chama a atenção para os seguintes aspetos de regime.

2.1. Em primeiro lugar, uma curta observação quanto ao regime consagrado no **artigo 7.º** do Projeto, onde se consagra o direito à proteção contra a *desinformação on-line*.

O n.º 3 deste artigo apresenta a definição do conceito em causa, especificando-se que o mesmo pressupõe a suscetibilidade de causar *um prejuízo público*, aí se indicando, a título exemplificativo, *ameaças aos processos políticos democráticos*. Mais se especifica na alínea *e)* do n.º 4 que se considera informação comprovadamente falsa ou enganadora *as comunicações políticas ou comerciais dirigidas, trolling organizado*.

A CNPD reconhece a sensibilidade do processo de harmonização dos direitos fundamentais à liberdade de expressão com outros direitos fundamentais ou interesses constitucionalmente relevantes e, especificamente, a dificuldade dessa conciliação com o objetivo de proteção pública contra a desinformação *on-line*.

De todo o modo, tendo em conta que aqui se pretende especificamente regular a proteção contra desinformação no contexto de campanhas políticas ou que afetem os processos políticos democráticos, a CNPD recorda que o exercício do direito de liberdade de expressão e de opinião pode envolver tratamento de dados pessoais (*v.g.*, a utilização destes dados, em especial no âmbito de processos de criação de perfis a partir da informação pessoal recolhida em redes sociais), sublinhando que no específico contexto da campanha política a União Europeia previu um regime de sancionamento *apenas* quando o *processo de desinformação assente na, ou se aproveite, da violação das regras de proteção de dados* pessoais – cf. artigo 10.º-A do Regulamento (UE/Euratom) 1141/2014 do Parlamento

Europeu e do Conselho, de 22 de outubro de 2014, alterado por último pelo Regulamento (UE/Euratom) 2019/493 do Parlamento Europeu e do Conselho, de 25 de março de 2019[5].

2.2. No artigo 8.º do Projeto, a propósito do direito de participação dos cidadãos na atividade pública, prevê-se no n.º 3 o dever de gravação em suporte de vídeo das reuniões da Assembleia da República, das assembleias municipais e das câmaras municipais, quanto estas sejam reuniões públicas, bem como a sua divulgação em acesso livre no respetivo portal na Internet. No n.º 4 prevê-se inclusive a transmissão em direto dessas reuniões dos referidos órgãos municipais através do portal ou de outra plataforma digital.

Compreendendo o interesse público na divulgação das reuniões de natureza pública dos órgãos municipais, a CNPD recorda que essas reuniões têm uma característica bem distinta das reuniões da Assembleia da República. É que nestas, os cidadãos ou não têm participação ativa, ou quando participam, não o fazem na qualidade de cidadãos para expor as suas necessidades ou as suas perspetivas pessoais quanto às necessidades públicas, mas antes na qualidade de representantes de entidades públicas ou privadas ou enquanto peritos em determinada matéria. Ao contrário do que sucede nas reuniões de natureza pública das assembleias municipais e das câmaras municipais, que permitem, nos termos legais, a intervenção de cidadãos nas reuniões em termos que facilmente resultam na exposição da vida privada e familiar.

Importa por isso, aqui, neste contexto, atender aos riscos de exposição e de reutilização indevida das imagens e das declarações proferidas pelos cidadãos nesse contexto, ponderação que deve ser feita tendo presente o regime de proteção de dados pessoais constante do RGPD e da Lei n.º 58/2019, de 8 de agosto. Aliás, a preocupação demonstrada no presente Projeto de lei, em especial, no artigo 7.º, com a manipulação de vídeos e com o *trolling*, não pode deixar de se fazer sentir também aqui de forma intensa.

Nesse sentido, a CNPD recomenda a reponderação do equilíbrio entre os direitos fundamentais aqui em tensão, sublinhando a importância de, neste contexto, se respeitar os princípios e as regras básicas do RGPD.

Nos termos do RGPD, ainda que esta norma legal possa constituir o fundamento de licitude deste tratamento de dados pessoais, a mesma não pode apresentar-se despida de garantias

[5] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02014R1141-20190327&from=EN

dos direitos dos cidadãos. Em especial, tem aqui que ser considerado e concretizado o princípio da minimização dos dados pessoais, consagrado na alínea *c)* do n.º 1 do artigo 5.º do RGPD, à luz do qual parece justificar-se a limitação da gravação, e sobretudo da transmissão *on-line* e da disponibilização permanente na Internet da gravação, às intervenções dos cidadãos que expressa e livremente nisso consintam, sendo evidente que, em qualquer caso, é imprescindível assegurar um direito de informação completo e com a definição clara das condições para a divulgação *on-line* das suas declarações (cf. artigo 13.º do RGPD). De outro modo, o direito fundamental à reserva da vida privada pode ficar seriamente afetado, sobretudo, insiste-se, tendo em conta a natureza das intervenções dos cidadãos nas reuniões de órgãos municipais e os riscos associados à disponibilização permanente na Internet deste tipo de informação.

Assim, a CNPD recomenda a eliminação da imposição legal contida nos n.ºs 3 e 4 do artigo 8.º, ou, caso se persista na sua manutenção, a previsão de garantias dos direitos dos cidadãos, em conformidade com o estatuído no RGPD.

2.3. No **n.º 5 do artigo 12.º** do Projeto impõe-se um dever de respeitar a indicação do titular de perfis pessoais em redes sociais ou similares quanto à eventual supressão dos mesmos após a sua morte.

A norma carece de uma maior densificação, designadamente especificando-se o meio adequado para a demonstração dessa vontade do titular dos dados, bem como junto de quem pode tal manifestação de vontade ser formulada (*v.g.*, junto do responsável pela rede social em causa).

Esta recomendação tem na sua base as dificuldades que têm sido sentidas pelos responsáveis pelos tratamentos de dados pessoais em verificar os pressupostos de aplicação do n.ºs 2 e 3 do artigo 17.º da Lei n.º 58/2019, de 8 de agosto, relativos ao exercício dos direitos relativos aos tratamentos de dados das pessoas falecidas.

Insiste-se, por isso, sob pena de também esta norma do Projeto correr o risco de inexequibilidade, na sua densificação.

2.4. Reconhecendo a importância da afirmação dos direitos dos cidadãos na interação com a Administração Pública através de meios eletrónicos, a CNPD assinala aqui algumas reservas aos termos da sua previsão no artigo 17.º do Projeto.

Em primeiro lugar, nota que a previsão genérica de um *direito a não repetir o fornecimento de dados já prestados*, carece de uma maior densificação, desde logo quanto ao destinatário dessa prestação. Ainda que a tendência político-legislativa seja a de garantir a interoperabilidade da informação disponível na Administração Pública, há condicionantes que têm de ser consideradas, também por razões de segurança dos sistemas de informação, pelo que a desejável simplificação da interação entre os cidadãos e a Administração Pública conhece, de facto, limites.

O mesmo se diga *do direito à adoção de procedimento administrativo digital*. A transformação da atividade administrativa decisória da Administração Pública num modelo exclusivamente eletrónico tem sido progressiva, não apenas pelos custos económicos, que nem todas as entidades públicas estão em condições de suportar imediatamente, mas também pelas garantias de segurança da informação e dos sistemas de informação que não podem ser descuradas. Esta norma deve ser afirmada mais como princípio ou norma programática do que como um direito imediatamente exequível, porque a segurança dos sistemas de informação da Administração Pública (e com isso a segurança do próprio Estado português, bem como a privacidade dos cidadãos) não é compatível com a garantia imediata de tal direito.

A CNPD recomenda assim uma densificação dos direitos previstos nas alíneas *a)* e *d)*, para salvaguarda da segurança da informação e dos sistemas de informação da Administração Pública.

Em terceiro lugar, o *direito de beneficiar de regimes de "Dados Abertos" que facultem o acesso a dados constantes das aplicações informáticas de serviços públicos e permitam a sua reutilização*, consagrado na alínea *e)* do artigo 17.º do Projeto está previsto com um grau de indeterminação não compatível com a previsibilidade, proporcionalidade e certeza jurídica de que uma norma legal atributiva de direitos deve estar dotada, sobretudo quando, como é aqui o caso, a afirmação desse direito é suscetível de restringir outros direitos fundamentais.

Na verdade, na ausência de uma explicação do conceito de *dados abertos*, é imprescindível delimitar o conjunto da informação existente nas aplicações informáticas de serviços

públicos, sob pena de se estar a consagrar um direito de acesso aberto a dados pessoais. Não pode ser esse, seguramente, o sentido da consagração deste direito de acesso, até porque o mesmo está, desde logo, delimitado entre outros diplomas, pelo Código do Procedimento Administrativo e pela Lei n.º 26/2016, de 22 de agosto, e Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho de 20 de junho de 2019, relativa aos dados aberto e à reutilização de informações no setor público (reformulação).

Por essa razão, a CNPD recomenda a clarificação da redação da alínea *e)* do artigo 17.º do Projeto, sugerindo que se acrescente, eventualmente no final, *nos termos previstos na lei.*

2.5. Finalmente, considera-se o disposto no **artigo 18.º** do Projeto.

Aí se prevê um conjunto de deveres da Administração Pública em matéria digital, nem todos apresentados com o mesmo grau de clareza e, sobretudo, muitos deles de difícil exequibilidade.

É, desde logo, o caso do dever de *criar sistemas gráficos de notificação de todos os atos administrativos e regulamentos administrativos dirigidos aos consumidores*, a que se refere a alínea *b).* Também aqui parece imprescindível a explicação, na norma, do conceito de *sistemas gráficos.* No pressuposto de que se reporte a um sistema visual passível de ser interpretado diretamente por um utilizador, reconduzindo-se a um portal, a CNPD recomenda que se imponha o dever de adoção de medidas que garantam a confidencialidade dos dados pessoais de cada cidadão.

De resto, fica a dúvida se o dever de criar sistemas gráficos de notificação é restrito à relação entre a Administração Pública e os consumidores, ou se a referência no final da alínea a consumidores é restrita aos regulamentos administrativos. Ainda assim, não se compreende que universo de consumidores está aqui em causa (*v.g.,* consumidores de bens e serviços prestados pela Administração Pública, consumires de bens e serviços essenciais prestados por entidades privadas), e consequentemente que universo de regulamentos administrativos estão sujeitos a notificação, uma vez que esta forma de comunicação está, nos termos do Código Procedimento Administrativo, reservada aos atos administrativos.

Mas as dificuldades de execução podem acentuar-se a propósito do dever de migração de todo o software para *open-source*, a que se refere a alínea *d),* pela complexidade em assegurar, nesse tipo de *software*, as atualizações necessárias e a interoperabilidade com

outros sistemas. Nessa medida, a CNPD recomenda que se repense esta imposição legal, e que, pelo menos, se acrescente no final da alínea a exigência de garantia de interoperabilidade com outros sistemas.

III – Conclusão

1. Embora reconhecendo préstimo a um diploma que pretende congregar o conjunto dos direitos no contexto digital, a CNPD não pode deixar de assinalar as normas que repetem direitos regulados por normas do Direito da União Europeia, em desconformidade com a jurisprudência do TJUE, algumas das quais, procurando replicar direitos já reconhecidos no RGPD, alteram o conteúdo desses direitos, ao inovar onde o RGPD define taxativamente os pressupostos dos mesmos ou ao desvirtuar o seu sentido ou âmbito de aplicação, em contradição com o Direito da União. Não obstante a CNPD entender que tais normas devem ser eliminadas do Projeto de Lei, apresenta recomendações que visam minorar a desconformidade com o Direito da União.

Acresce que algumas das normas previstas no Projeto de Lei empregam conceitos cuja definição consta de diplomas legais de Direito da União, tendo por isso um sentido específico, mas que não são, nem por remissão, explicados no articulado do Projeto, dificultando com isso a sua interpretação e afetando a previsibilidade e a certeza jurídica exigíveis a normas consagradoras de direitos a que correspondem obrigações de terceiros.

Assim, a CNPD à luz destes argumentos e dos específicos fundamentos acima expostos, quanto às normas que em seguida se elencam, a CNPD recomenda:

a) A eliminação do n.º 4 do artigo 9.º do Projeto, ou, se assim não se entender, a sua redação em termos que não contrariem o disposto no artigo 22.º do RGPD;

b) A alteração da redação do n.º 4 do artigo 12.º, com introdução dos termos assinalados em itálico: É proibida qualquer forma de utilização de código bidimensional, *ou de dimensão superior,* para tratar informação sobre o estado de saúde ou qualquer outros aspeto relacionado com direitos de pessoas singulares, *salvo se for aplicada uma cifragem segura à informação previamente à geração do código.;*

c) No artigo 13.º:

i. A revisão do n.º 1, remetendo para os fundamentos do direito a ser esquecido previsto no artigo 17.º do RGPD;

ii. A clarificação da redação do n.º 2;

iii. A eliminação do n.º 3, ou, se assim não se entender, a sua revisão em termos que não contrariem o disposto nos n.ºs 2 e 3 do artigo 12.º do RGPD, nem restrinjam os fundamentos do direito ao apagamento de dados pessoais previsto no artigo 17.º do RGPD;

iv. A eliminação do n.º 4, por nada acrescentar em relação à alínea *f)* do n.º 1 do artigo 17.º do RGPD;

d) No n.º 1 do artigo 14.º, a reponderação da previsão de um direito ao apagamento dos dados no âmbito de plataformas digitais, à luz das exceções previstas no n.º 3 do artigo 17.º do RGPD;

e) No artigo 16.º, a reponderação do previsto no n.º 2, sublinhando que traduz a derrogação parcial de normas previstas na Lei n.º 41/2004 e na Diretiva *e-Privacy*, e que, também pelos termos abertos em que vem previsto o acesso, parece violar o princípio da proporcionalidade (cf. n.º 2 do artigo 18.º da CRP e n.º 1 do artigo 52.º da Carta).

2. A CNPD, com os fundamentos expostos no ponto II.2., recomenda ainda:

a) A eliminação da imposição legal contida nos n.ºs 3 e 4 do artigo 8.º, ou, caso se persista na sua manutenção, a previsão de garantias dos direitos dos cidadãos, em conformidade com o estatuído no RGPD, designadamente limitando a gravação e, sobretudo, a transmissão e disponibilização na Internet, das intervenções dos cidadãos que tenham expressa e livremente nisso consentido;

b) A densificação do n.º 5 do artigo 12.º, seja para que se especifique o meio e junto de quem pode tal manifestação de vontade do titular de perfis pessoais em redes socais relativamente à supressão *post-mortem* de tais perfis;

c) A densificação dos direitos previstos nas alíneas *a)* e *d)* do artigo 17.º do Projeto, para salvaguarda da segurança da informação e dos sistemas de informação da Administração Pública; e

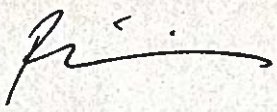
d) A clarificação da redação da alínea *e)* do artigo 17.º do Projeto, sugerindo que se acrescente, eventualmente no final, *nos termos previstos na lei;*

e) A clarificação e a reponderação de alguns dos deveres previstos no artigo 18.º, pela dificuldade na exequibilidade, e em especial:

   i. Na alínea *b)* do artigo 18.º, a clarificação da sua redação, e a previsão de um dever de adoção de medidas que garantam a confidencialidade dos dados pessoais de cada cidadão;

   ii. Na alínea *d),* que, pelo menos, se acrescente no final a exigência de garantia de interoperabilidade com outros sistemas.

Aprovado na reunião de 28 setembro de 2020



Filipa Calvão (Presidente)