PARECER/2020/116

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 473/XIV/1.ª, de iniciativa do grupo parlamentar do Partido Socialista, que aprova a Carta dos Direitos Fundamentais na Era 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 reforçar os direitos das pessoas no contexto digital, como se explica na exposição de motivos, «*sem se limitar a uma mera compilação das normas que na ordem jurídica portuguesa já consagram direitos digitais, previstos na própria Constituição ou constantes de diplomas que transpuseram diretivas europeias.*» Assim, com o Projeto, procura-se «*enunciar um elenco de direitos, liberdades e garantias diversificado e abrangente que inove, clarifique e valha também como bases de um programa de ação vinculativa dos órgãos do poder.*»

Com especial relevância para a garantia dos direitos no âmbito de tratamentos de dados pessoais, a CNPD saúda a preocupação revelada ao longo do Projeto com as consequências para os utilizadores da Internet de soluções tecnológicas de Inteligência Artificial, em especial quando envolvam aprendizagem automatizada (*machine learning*), e de decisões tomadas de modo automatizado sobre cada indivíduo a partir de perfis e de outra informação sobre o mesmo recolhida.

Não obstante a invocação de um extenso conjunto de instrumentos jurídicos, a maior parte deles de cariz internacional ou europeu, e de outras iniciativas de debate sobre a matéria, no 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 muitas 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.

Não pode também deixar de se assinalar que um diploma com a natureza de uma *Carta de Direitos Fundamentais na Era Digital,* como é intitulado o Projeto, deve apresentar uma natureza tendencialmente perene, portanto, que não valha apenas para situações de normalidade das relações jurídicas. Ora, a exclusão de regulação dos direitos digitais em vários tipos de relações jurídicas, bem como «em diversos domínios cujo êxito tem sido uma das faces do combate à pandemia COVOD-19» (como se lê na exposição de motivos), parece prejudicar a força jurídica desta Carta de Direitos Fundamentais.

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.

---

[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

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 n.º 2 do artigo 1.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 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

---

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808ac918

[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

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, no n.º 1 do **artigo 4.º** do Projeto, a proibição de interrupção intencional de acesso à Internet, total ou parcial, ou a limitação da informação que nela possa ser disseminada. Ainda que se compreenda a intenção garantística de acesso universal a este meio de comunicação e de acesso à informação, a verdade é que os casos ressalvados na segunda parte desta norma deixam de fora outras situações previstas em lei, onde, para garantia de direitos fundamentais, se atribui a outras autoridades administrativas o poder de determinar o bloqueio do acesso à Internet ou a limitação da informação a divulgar: é precisamente esse o caso dos poderes da autoridade de controlo dos tratamentos de dados pessoais previstos na alínea *f)* do n.º 2 do artigo 58.º do RGPD, os quais têm obviamente aplicação aos tratamentos de dados pessoais realizados na Internet, ou ainda dos poderes das autoridades competentes para efeitos de aplicação do Regulamento (UE) 2017/2394 relativo à proteção dos consumidores[4]. Em ambos os casos, os regulamentos da União preveem ações de assistência mútua entre as autoridades dos Estados-Membros, cuja concretização depende do conjunto de poderes mínimos, definido no direito da União, de que essas autoridades gozam, e o qual não pode ser restringido pelo direito interno.

Para obviar a uma contradição com o disposto nesta norma de Direito da União Europeia, diretamente aplicável na ordem jurídica portuguesa, recomenda a CNPD que, na parte final

---

[4] Regulamento (UE) 2017/2394 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2017, relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de proteção de consumidores e que revoga o Regulamento (CE) 2006/2004. Este regulamento é aplicável desde 17 de janeiro de 2020. Ver, em especial, artigo 9.º que regula os poderes mínimos das autoridades competentes, e demais artigos quanto a assistência mútua.

do n.º 1 do artigo 4.º do Projeto, a ressalva abranja os *casos previstos na presente lei e em outros diplomas legais*, para além dos casos em que exista uma decisão judicial nesse sentido.

Paralelamente, o **n.º 2 do artigo 7.º** do Projeto deve também ressalvar, para além dos casos previstos na lei processual penal e com autorização de um juiz, outros casos previstos em lei. Isto porque, não sendo claro se o sentido de segurança e sigilo das comunicações diz somente respeito ao conteúdo comunicado ou também a outros dados relativos a tais comunicações, importa notar que são várias as contraordenações legalmente previstas que pressupõem o poder de identificar, pelo menos, o remetente ou o destinatário de tais comunicações, o que obriga as autoridades administrativas competentes para a investigação de tais ilícitos a conhecer dados de tráfego, ou mesmo o conteúdo de algumas mensagens para verificar se têm conteúdo de *marketing* não solicitado (*spam*).

Aliás, esta disposição, sem mais clarificação, parece prejudicar o poder reconhecido à Entidade Reguladora para a Comunicação Social (ERC), no n.º 2 do artigo 5.º do Projeto, de apreciar queixas quanto a conteúdos *on-line* falsos ou enganadores.

1.2. Ainda no âmbito do **artigo 7.º** do Projeto, que consagra o direito à privacidade digital, o seu **n.º 4** vem reconhecer-se um *direito à proteção contra a definição de perfis efetuada de forma ilegal*. 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 todo 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 7.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 7.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.

1.3. Também no **artigo 8.º** do Projeto se consagram direitos, agora a propósito do uso da Inteligência Artificial e de robôs, que mais não são do que a repetição de direitos já consagrados e regulados no RGPD e, mais grave, em termos diferentes do neste estatuído.

Desde logo, atente-se no n.º 2 do artigo 8.º: aí se determina que qualquer *decisão individual tomada com base num tratamento algorítmico de[v]e informar desse facto a pessoa interessada.* Deixando de lado o facto de o sujeito da frase ser aqui a decisão e de a esta se imputar um dever de fazer, o que parece pressupor uma perspetiva de imputabilidade de deveres jurídicos e de responsabilidades a robôs e a tecnologia, mais uma vez se afigura estar perante um equívoco quanto aos conceitos empregues.

Na verdade, parece que no Projeto se confunde, como se da mesma realidade se tratasse, o tratamento algorítmico de informação sobre pessoas singulares com o tratamento dessa informação através de tecnologias de Inteligência Artificial. Ora, os algoritmos são,

consabidamente, relevantes para a Inteligência Artificial, mas nem toda a análise de informação com recurso a algoritmos corresponde a essa nova realidade. Nessa medida, a CNPD recomenda a revisão desta disposição.

De todo o modo, o que aqui parece ter-se em vista é, na verdade, o que as alíneas *f)* do n.º 2 do artigo 13.º e *g)* do n.º 2 do artigo 14.º do RGPD já preveem, pelo que, em conformidade com a jurisprudência do TJUE já citada, a CNPD sublinha a desnecessidade desta norma e a conveniência da sua eliminação para que não prejudique o sentido e a força jurídica do disposto naquelas disposições do RGPD.

O mesmo vale para o n.º 3 do artigo 8.º, que vem complementar as informações a prestar aos titulares dos dados pessoais. Se o legislador nacional pretendia com esta disposição alargar o âmbito do direito de informação previsto nas alíneas *f)* do n.º 2 do artigo 13.º e *g)* do n.º 2 do artigo 14.º do RGPD, para consagrar um direito a uma explicação sobre o tratamento de dados realizado por recurso a técnicas de aprendizagem automática, a CNPD, saudando a intenção garantística, chama a atenção para as dificuldades de uma densificação de um tal direito diferente da que consta do RGPD.

1.4. Em relação ao **artigo 11.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 11.º não pode deixar de ser lido à luz de tais regras.

Mas destaca sobretudo o preceituado no n.º 4 do artigo 11.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 11.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.*

1.5. Ainda quanto aos direitos consagrados no RGPD e que no Projeto vêm reafirmados no contexto digital, importa agora analisar o direito previsto no **artigo 12.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 12.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 12.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 dos 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 12.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[5] 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 12.º do Projeto.

Em terceiro lugar, a imposição, no n.º 3 do artigo 12.º, do exercício do direito ao apagamento dos dados pessoais fornecidos a redes sociais ou serviços da sociedade de informação

[5] 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.

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 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 o 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 12.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.

1.6. Atente-se ainda no n.º 1 do **artigo 13.º** do Projeto, quando se reporta ao direito dos utilizadores de plataformas digitais 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. 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.

1.7. No que diz respeito ao *direito à proteção contra a geolocalização abusiva*, consagrado no **artigo 15.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 georreferenciação, 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 15.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 3.º** e no **artigo 5.º** do Projeto de Lei.

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 certos conteúdos opinativos e de desinformação.

De todo o modo, tendo em conta 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), vem aqui recordar que, num outro contexto (que é o 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[6].

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

2.2. No **artigo 16.º** do Projeto prevê-se o *direito ao testamento digital*.
Ainda que a epígrafe ajude a interpretar o teor da norma, importa desde logo esclarecer que a supressão de perfis pessoais em redes sociais e similares aqui em vista é a que ocorra após a morte do titular dos perfis.

Além disso, 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 dos 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.

2.3. 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 imediatos, 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.*

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 muitas 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) No artigo 4.º do Projeto, que a ressalva no n.º 1 abranja os *casos previstos na presente lei e em outros diplomas legais*, para além dos casos em que exista uma decisão judicial nesse sentido;
b) No artigo 7.º do Projeto, que a ressalva no n.º 2 abarque, para além dos casos previstos na lei processual penal e com autorização de um juiz, *outros casos previstos em lei*;
c) A eliminação do n.º 4 do artigo 7.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;
d) A eliminação do n.º 2 e do n.º 3 do artigo 8.º, ou, se assim não se entender, a sua redação em termos que não difiram do disposto na alínea *f)* do n.º 2 do artigo 13.º e na alínea *g)* do n.º 2 do artigo 14.º do RGPD;
e) A alteração da redação do n.º 4 do artigo 11.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.;*

f) No artigo 12.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;

g) No n.º 1 do artigo 13.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;

h) No artigo 15.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 densificação do artigo 16.º, seja para que se especifique que a supressão de perfis pessoais em redes sociais e similares nele regulada respeita a um momento *post-mortem* do respetivo titular, bem como o meio e junto de quem pode tal manifestação de vontade ser formulada;

b) 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

c) 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.*

Aprovado na reunião de 28 de setembro de 2020

Filipa Calvão (Presidente)