PARECER N.º 20/2018

I. Pedido

O Presidente da Comissão dos Assuntos Constitucionais, Direitos, Liberdades e Garantias remeteu à Comissão Nacional de Protecção de Dados (CNPD), para parecer, a Proposta de Lei n.º 120/XIII/3.ª (Gov), que «Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito aos tratamentos de dados pessoais e à livre circulação desses dados».

O pedido formulado decorre das atribuições conferidas à CNPD pelo n.º 2 do artigo 22.º da Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto – Lei de Proteção de Dados Pessoais (doravante, LPDP) –, e o parecer é emitido no uso da competência fixada na alínea *a)* do n.º 1 do artigo 23.º do mesmo diploma legal.

Considerando o objeto da Proposta, a sua apreciação será feita não em relação ao regime legal de proteção de dados vigente (a LPDP), mas sim tomando como referência o Regulamento (UE) 2016/679 – Regulamento Geral sobre a Proteção de Dados (RGPD) – e as normas constitucionais pertinentes.

A título de nota prévia, a CNPD sublinha ainda que a extensão e densidade do presente parecer se deve não apenas à complexidade da matéria como também ao facto de não lhe ter sido dada oportunidade de se pronunciar sobre o anteprojeto de Proposta de Lei, o que poderia ter contribuído para uma redação final da mesma mais conforme com o RGPD e o direito da União Europeia.

De todo o modo, no sentido de facilitar a compreensão do teor do parecer e a eventual ponderação da adaptação do articulado da Proposta de Lei, a CNPD apresenta propostas de redação das normas do diploma em anexo ao presente parecer.

II. Questões prévias

1. Exposição de motivos e sistematização

Em primeiro lugar, destaca-se que a exposição de motivos que acompanha o articulado da Proposta de Lei apresenta algumas imprecisões quanto ao RGPD para as quais aqui se entende dever alertar.

Sem prejuízo das considerações a apresentar no ponto III.2.2., é duvidoso que se possa afirmar que o «*paradigma que esteve subjacente ao legislador europeu foi o das grandes multinacionais que gerem redes sociais ou aplicações informáticas à escala global, envolvendo a recolha e utilização intensiva de dados pessoais. Por esse motivo, algumas das soluções jurídicas que foram plasmadas para esse universo revelam-se por vezes desproporcionadas ou mesmo desadequadas para a generalidade do tecido empresarial nacional e para a Administração Pública […]*».

Na verdade, o que o RGPD toma como paradigma é a tecnologia hoje disponível para a realização de tratamentos de dados pessoais e, portanto, visa conciliar a utilização de soluções tecnológicas no seu estado atual e futuro de desenvolvimento, e os riscos que comportam, com a defesa dos direitos e liberdades das pessoas cujos dados são objeto de tratamento.

Por outras palavras, o RGPD não pretende apenas regular, ou regular sobretudo, os tratamentos de dados pessoais de grandes empresas, porque esses tratamentos não têm necessariamente maior impacto sobre os direitos fundamentais dos cidadãos do que os tratamentos realizados por pequenas ou médias empresas, por entidades privadas sem fins lucrativos ou por entidades públicas. Sendo certo que, relevando o impacto dos tratamentos sobre os direitos dos titulares dos dados na realidade portuguesa, tão invocada na exposição de motivos, o Estado português e a sua administração indireta se destacam e mereceriam por isso um intenso regime jurídico dos tratamentos por si realizados (basta pensar, para além dos ministérios, em organismos como a Autoridade Tributária e Aduaneira, o Instituto da Segurança Social, IP, e os vários Hospitais, EPEs).

Acresce que a afirmação de que «*a aplicação deste regulamento resultará em encargos administrativos elevados, que em muitos casos não se encontram suficientemente justificados pelos benefícios obtidos com o novo regime de proteção de dados pessoais relativamente ao regime atual*» traduz uma crítica às ponderações do legislador europeu vertidas no RGPD e um incentivo implícito às entidades públicas para retardar o cumprimento do RGPD, pelo menos numa primeira fase da sua aplicação, o que não pode deixar de suscitar elevada preocupação na CNPD, enquanto autoridade administrativa independente encarregue de garantir o cumprimento do regime jurídico de proteção de dados no território nacional.

Afirma-se ainda, na página 2 da exposição de motivos (4.º §), que o RGPD estabelece regras mais exigentes quanto ao tratamento de categorias especiais de dados pessoais, quando, em rigor, o que se pode dizer é apenas que alargou essas categorias (passando a abranger, por exemplo, dados biométricos), mas não que o regime aplicável esteja mais exigente.

Quanto às novidades do RGPD, declara-se, na página 4, que o *«papel do controlo prévio das autoridades de controlo é eliminado e substituído por registos das atividades de tratamento*», quando em rigor aquele papel é substituído por um dever prévio de verificação do cumprimento do RGPD por parte dos responsáveis e dos subcontratantes, de que o registo é apenas uma obrigação complementar.

No mais, algumas das inovações introduzidas pela Proposta e nessa sede explicadas são de questionável conformidade com o RGPD, como de seguida se procurará demonstrar.

Finalmente, uma palavra para a sistematização do articulado da Proposta de Lei, cuja lógica na parte referente aos capítulos V e VI não é evidente. Em causa estão, aparentemente, matérias em relação às quais o legislador europeu reconheceu autonomia normativa aos Estados-Membros, mas que não só contêm previsões sobre matérias excluídas dessa autonomia como não se entende a diferença entre disposições especiais e situações específicas de tratamento de dados pessoais. Por exemplo, as disposições sobre videovigilância ou o tratamento de dados de pessoas falecidas são tão especiais como as relativas aos dados de saúde. Recomenda-se, por isso, uma reformulação dessa sistematização.

2. O desrespeito pelo direito da União

A CNPD não pode deixar de chamar a atenção para uma questão incontornável, e que é decisiva na apreciação desta Proposta de Lei, uma vez que se traduz em violação objetiva do direito da União.

Em primeiro lugar, a presente Proposta pretende reproduzir em alguns artigos parte do articulado do RGPD. É esse, designadamente, o caso do artigo 2.º (âmbito de aplicação), do artigo 11.º (funções do encarregado de proteção de dados) ou do artigo 13.º (encarregados de proteção de dados em entidades privadas). E não se trata aqui sequer de legislar sobre

aspetos específicos que o Regulamento remeta para o campo de ação do Estado-Membro, mas apenas de uma tentativa de replicar disposições, com a agravante de, em alguns casos concretos, desvirtuar por completo o teor do RGPD, contrariando-o grosseiramente.

Em segundo lugar, a Proposta pretende introduzir no direito nacional norma que difere a aplicação do RGPD para momento posterior à data prescrita no artigo 99.º do próprio Regulamento. Assim, apesar do RGPD ser aplicável a partir de 25 de maio de 2018, seria possível, nos termos do proposto no **artigo 61.º** (renovação do consentimento) da Proposta, demorar seis meses desde a entrada em vigor da lei nacional para obter um consentimento que constituiria o fundamento de legitimidade para certos tratamentos de dados, admitindo-se portanto *a contrario* a existência de tratamentos ilícitos durante esse período de tempo.

Ora, nos termos do artigo 288.º do Tratado de Funcionamento da União Europeia (TFUE), o *regulamento tem carácter geral. É obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros*. Sem prejuízo da análise detalhada que se faz ao longo deste parecer sobre todas as normas contidas na Proposta em que a CNPD considera haver violação evidente dos termos do RGPD, salienta-se desde logo o facto de o legislador português não poder alongar o prazo de aplicabilidade de uma obrigação do RGPD. Sobre isto já se pronunciou o Tribunal de Justiça da União Europeia (TJUE), no Acórdão Costa/ENEL (proc. 6/64)[1], ao afirmar que esta disposição dos tratados *seria destituída de significado se um Estado pudesse, unilateralmente, anular os seus efeitos através de um ato legislativo oponível aos textos comunitários*.

Também o Acórdão *Variola* do Tribunal de Justiça (proc. 34/73)[2] considera que a *aplicação direta de um Regulamento significa que a sua entrada em vigor e a sua aplicação a favor ou contra aqueles que lhe estão sujeitos são independentes de qualquer medida de execução na lei nacional* (Ponto 10 do Acórdão).

Por outro lado, no que diz respeito à questão de esta Proposta replicar o teor de normas do RGPD, sujeitando-as ao direito nacional e, nessa medida, afetando também a jurisdição do tribunal europeu, o Acórdão *Variola* é igualmente muito claro quando afirma que *os Estados-*

[1] https://institutoeuropeu.eu/images/stories/Cosa_Enel.pdf

[2] http://curia.europa.eu/juris/showPdf.jsf?text=&docid=88457&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=378305

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* (Ponto10).

Admite-se tão-só a incorporação de *elementos* de um regulamento no direito nacional apenas *na medida do necessário para manter a coerência e tornar as disposições nacionais compreensíveis*, tal como prevê o considerando 8 do RGPD[3], caso estejam previstas especificações das regras pelo direito do Estado-Membro.

Daqui se pode concluir que, à luz do direito da União interpretado pelo Tribunal de Justiça, as disposições de um Regulamento não podem ser introduzidas na ordem jurídica dos Estados-Membros através de disposições internas que se limitem a reproduzir aquelas normas. Por força dos Tratados, *os Estados-Membros estão sob a obrigação de não introduzir qualquer medida que possa afetar a jurisdição do tribunal* (Ponto 11 do Acórdão *Variola*).

Há um outro Acórdão do TJUE, Comissão/Itália (proc. 39/72)[4], no qual se encontra vertida jurisprudência relevante para os dois tipos de violação acima indicados.

Assim, o Tribunal de Justiça, referindo-se à fixação de prazos concretos pelos regulamentos, considerou que *a observância desses prazos era indispensável para a eficácia das medidas em questão, dado que estas apenas podiam atingir plenamente os seus objetivos se fossem executadas simultaneamente em todos os Estados-Membros, no momento estabelecido* (…) (cf. Ponto 14).

Por outro lado, sobre a mera reprodução de disposições dos regulamentos comunitários na legislação nacional, o mesmo Acórdão afirma que tal cria um *equívoco no que se refere à natureza jurídica das disposições a serem* aplicadas e reitera que são *contrárias ao Tratado quaisquer modalidades de execução que possam obstar ao efeito direito dos regulamentos*

---

[3] Considerando que assenta nos pontos 26 e 27 do Acórdão do Tribunal de Justiça, de 28 de março de 1985, proc. 272/83.

[4] 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

comunitários e desse modo comprometer a sua aplicação uniforme no espaço comunitário (cf. ponto 17).

Com este quadro legislativo e jurisprudencial, o legislador nacional está efetivamente limitado na sua atuação e tem de ter especial cuidado ao legislar em execução de um Regulamento, sob pena de infringir o direito da União. O esforço de repetição de normas do Regulamento na lei nacional assume ainda maior gravidade quando o texto da Proposta entra em clara contradição com o conteúdo dos preceitos do RGPD.

Sobre a execução do RGPD, a Comissão Europeia emitiu Orientações, em janeiro deste ano, numa Comunicação ao Parlamento Europeu e ao Conselho[5], na qual defendeu que o *regulamento constitui uma oportunidade para simplificar o ambiente jurídico, passando assim a existir menos regras nacionais e maior clareza para os operadores.*

Nesse contexto, a Comissão explica que *quaisquer medidas nacionais que resultem na criação de um obstáculo à aplicabilidade direta do regulamento e ponham em perigo a sua aplicação simultânea e uniforme em toda a UE são contrárias aos Tratados*.

Por outro lado, a Comissão Europeia é taxativa ao afirmar que: [R]*epetir o texto dos regulamentos no direito nacional também é proibido* (…) *Reproduzir o texto do regulamento palavra por palavra no direito nacional que visa a especificação deve ser algo excecional e justificado, não podendo ser utilizado para acrescentar condições ou interpretações adicionais ao texto do regulamento.*

Assente na vasta jurisprudência sobre esta matéria, e que é acima citada, a Comissão Europeia reitera que a interpretação do regulamento cabe aos tribunais europeus (…) e não aos legisladores dos Estados-Membros, pelo que o legislador nacional não pode copiar o texto do RGPD, nem interpretá-lo ou acrescentar condições adicionais às regras diretamente aplicáveis ao abrigo do regulamento. Se o fizessem, os operadores de toda a União ficariam novamente perante uma situação de fragmentação e não saberiam a que regras obedecer.

A Comissão Europeia alerta para a possibilidade de procedimento por infração se os Estados-Membros incumprirem estas regras. Ora, o texto desta Proposta de Lei vai

---

[5] http://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A52018DC0043&qid=1517578296944&from=EN

inequivocamente ao arrepio do direito da União, da jurisprudência europeia e das recentes orientações da Comissão Europeia especificamente sobre o RGPD.

Acresce que nas matérias em que a competência legislativa dos Estados-Membros não fica esgotada pelo RGPD e, portanto, podem ser estabelecidas regras que adaptem o estatuído às especificidades nacionais, a Proposta de Lei assume um teor vago e aberto, não conseguindo com isso criar um regime efetivamente disciplinador dos tratamentos de dados. Umas vezes, limitando-se a reproduzir critérios de regulamentação previstos na própria norma do RGPD que confere autonomia legislativa, outras vezes incumprindo mesmo o dever de conciliar direitos fundamentais, imposto pelo RGPD, através da previsão de limites ou medidas materiais e procedimentais precisas. E é de todos conhecido que a normação sobre direitos, liberdades e garantias tem, por imposição constitucional, de revestir uma densidade superior, não se bastando com normas abertas ou programáticas.

3. A proteção da vida privada

Uma nota ainda para o facto de a presente Proposta de Lei não dispor especificamente sobre os dados relativos à vida privada. Tal opção dever-se-á, porventura, ao facto de o RGPD não deixar espaço para os Estados-Membros legislarem sobre o catálogo de dados pessoais especialmente protegidos previsto no n.º 1 do artigo 9.º. Com efeito, dessas categorias de dados pessoais não consta a vida privada, a qual é objeto de proteção reforçada no n.º 3 do artigo 35.º da Constituição da República Portuguesa (CRP) – proteção constitucional que se reflete na ainda vigente LPDP, a qual, no catálogo de dados sensíveis previsto no artigo 7.º, inclui os dados relativos à vida privada.

No entanto, a proteção da vida privada e a definição de um regime específico de proteção reforçada são impostas não apenas pela Constituição portuguesa (cf. também n.º 1 do artigo 26.º), como também pela Convenção Europeia dos Direitos do Homem (CEDH), no artigo 8º, e pela Carta dos Direitos Fundamentais da União Europeia (artigo 7.º).

Importa, a este propósito, recordar que a *ratio* subjacente a este regime de proteção reforçado é a de garantir a dignidade da pessoa humana no contexto do processamento de informação relativa a dimensões da vida humana cujo tratamento historicamente gerou e é suscetível de gerar discriminação. Daí que, desde logo, as condições para se ter por lícito o

seu tratamento, elencadas no artigo 9.º do RGPD, sejam mais restritas do que as previstas no artigo 6.º do mesmo diploma.

Certo é que todas essas categorias de informação pessoal revelam dimensões da vida privada dos seus titulares, mas não a esgotam. Por isso mesmo, ainda que o RGPD sujeite as restantes dimensões da vida privada ao regime dos dados abrangidos pelo artigo 6.º, esse regime tem de ser interpretado em conformidade com os artigos 26.º, n.º 1, e 35.º, n.º 3, da CRP, e com o artigo 8.º da CEDH e o artigo 7.º da Carta dos Direitos Fundamentais, garantindo sempre o resultado da proteção efetiva da vida privada. É, aliás, este o entendimento do TJUE[6].

Daqui resulta que um conjunto de tratamentos de dados relativos à vida privada que dependia, ao abrigo da LPDP, de previsão legal específica ou, na falta de consentimento, do reconhecimento de que a respetiva finalidade correspondia a um interesse público importante, pode agora ser realizado com base numa das condições previstas no artigo 6.º do RGPD. Todavia, a apreciação da licitude dos tratamentos de dados relativos à vida privada passa, numa interpretação conforme com as normas constitucionais e convencionais acima citadas, pela verificação em concreto das garantias de proteção efetiva da vida privada e de não discriminação. Em especial, os tratamentos que assentem no interesse legítimo do responsável, cuja licitude depende de em cada caso não prevalecerem os direitos e interesses dos titulares, só se poderão ter por lícitos se com isso não for exposta desnecessariamente ou de modo insuportável a vida privada dos titulares ou se houver um risco sério de resultado discriminatório para os mesmos.

III. Análise do articulado da Proposta de Lei

Na análise que se segue, serão consideradas, em primeiro lugar, as disposições da Proposta de Lei que traduzem uma direta violação do RGPD, seja por contrariarem o aí disposto, seja por se limitarem a reproduzir as normas nele contidas, desvirtuando o seu valor de norma de direito da União.

---

[6] Cf. Acórdãos *Schrems*, *Digital Rights* e *Tele 2*, disponíveis respetivamente em (http://curia.europa.eu/juris/liste.jsf?td=ALL&language=pt&jur=C,T,F&num=C-362/14) (http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=PT) e (http://curia.europa.eu/juris/liste.jsf?num=C-203/15&language=PT).

Depois, será apreciado o regime para as entidades públicas que na Proposta se entendeu fixar.

Em terceiro lugar, focar-se-á um conjunto de disposições sobre matérias quanto às quais há dever de legislar no plano nacional, procurando-se alertar para algumas incongruências e incompletudes. Desse grupo destacar-se-á o regime das contraordenações, que merecerá uma análise mais detalhada.

A terminar, após a análise das sanções penais, serão apreciadas as demais disposições da Proposta que incidem sobre matérias cuja regulação específica nacional é permitida pelo RGPD.

E fechar-se-á com um breve comentário crítico sobre algumas disposições finais ou transitórias.

1. Normas violadoras do direito da União

1.1 Âmbito de aplicação

Analisemos, a este propósito, o **artigo 2.º** da Proposta sobre o âmbito de aplicação da lei nacional. O n.º 1 deste artigo prescreve: «[A] presente lei aplica-se aos tratamentos de dados pessoais realizados no território nacional, independentemente da natureza pública ou privada do responsável pelo tratamento ou do subcontratante (…), aplicando-se todas as exclusões previstas no artigo 2.º do RGPD». A alínea *a)* do n.º 2 determina que: «[A] presente lei aplica-se aos tratamentos de dados pessoais realizados fora do território nacional quando sejam efetuados no âmbito da atividade de um estabelecimento situado no território nacional».

Com efeito, estas normas traduzem-se numa manifesta violação do artigo 3.º, n.º 1, do RGPD, pondo em causa o mecanismo de balcão único que constitui uma das características mais emblemáticas deste regulamento.

Por um lado, de acordo com o RGPD, não releva o local onde os tratamentos de dados efetivamente ocorrem, seja em território nacional, em outro Estado-Membro ou fora da União, aplicando-se antes o critério do estabelecimento no território da União, desde que os tratamentos de dados se efetuem no contexto das atividades desse estabelecimento. Por

outro lado, havendo mais do que um estabelecimento na União, a lei aplicável será a do estabelecimento principal.

Por conseguinte, não é possível fazer aplicar a lei portuguesa a todos os tratamentos de dados realizados em território nacional ou no contexto de atividades de um estabelecimento situado em Portugal. Estas disposições da Proposta contradizem inequivocamente o que está definido no RGPD quanto ao âmbito de aplicação territorial.

De igual modo, a alínea *b)* do n.º 2 do artigo 2.º da Proposta, que pretende ter correspondência ao artigo 3.º, n.º 2, do RGPD, restringe a sua aplicação à afetação de titulares de dados «que residam no território nacional». Neste preceito, persiste-se num erro que já consta da versão portuguesa do RGPD, mas que limita a proteção dada pelo Regulamento aos *titulares residentes no território da União*, quando de facto a aplicação do RGPD se estende a todos os titulares que se encontrem na União. Senão, confira-se a versão inglesa, na qual a proposta de Regulamento foi apresentada, discutida e aprovada: «the processing of personal data of *data subjects who are in* the Union»[7].

Não há, pois, qualquer fundamento para que a Proposta de lei imponha uma restrição do âmbito de aplicação do RGPD, o qual aliás explicita no seu considerando 14 que *a proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência*, criando consequentemente uma diferenciação do regime jurídico de proteção de dados pessoais para os titulares que se encontrem em território português mas não residam cá. Recorda-se que a Constituição portuguesa reconhece a titularidade do direito à proteção de dados a qualquer pessoa, mesmo que não seja cidadão português ou residente em território nacional (cf. artigo 15.º), pelo que estamos perante uma violação do princípio da igualdade na garantia dos direitos fundamentais, nos termos dos artigos 13.º, 15.º e 35.º da CRP. O artigo 8.º da Carta dos Direitos Fundamentais da União Europeia reconhece o mesmo direito a todas as pessoas, sem delimitar, em função da nacionalidade ou da residência, o âmbito de aplicação da norma impositiva de proteção jurídica.

7 Itálico nosso. Cf. ainda nas versões francesa «qui se trouve sur le territoire de l'Union», italiana «che si trovano nell' Unione», alemã «die sich in der Union befinden» e holandesa «die zich in dir Unie bevinden».

Por último, ainda no que diz respeito ao âmbito de aplicação, a alínea *c)* do n.º 2 do artigo 2.º da Proposta prevê que a lei nacional se aplique a tratamentos de dados realizados fora do território nacional quando: «*afetem titulares de dados que, sendo portugueses, residam no estrangeiro e cujos dados estejam inscritos nos postos consulares*». Ora, isto contraria notoriamente o n.º 3 do artigo 3.º do RGPD que estende a sua aplicação a responsável pelo tratamento estabelecido em lugar onde se aplique o direito de um Estado-membro por força do direito internacional público.

Deste modo, o âmbito de aplicação é bem mais vasto do que os postos consulares, incluindo também as embaixadas, as aeronaves ou as embarcações portuguesas, e abrangendo qualquer tipo de tratamento de dados pessoais que seja realizado, independentemente das categorias de titulares dos dados que, naturalmente, podem abarcar portugueses não residentes, visitantes estrangeiros, trabalhadores estrangeiros e por aí adiante, algo até contraditório com o limitado âmbito de aplicação que criticámos supra, então a propósito da exclusão de não residentes.

Não dando o RGPD, nesta matéria, qualquer margem aos Estados-Membros para legislar, não se entende a razão de ser deste artigo, que acaba a infringir duplamente o direito da União, seja ao pretender replicar normas do regulamento no direito nacional, seja ao, fazendo-o, desvirtuar inteiramente o âmbito de aplicação territorial do RGPD. Deve, nesse sentido, ser eliminado, considerando-se suficiente para efeito de delimitação do âmbito de aplicação da Proposta a definição do seu objeto, contida no artigo 1.º, ao definir que a lei assegura a execução, *na ordem jurídica interna,* do RGPD.

1.2. Normas relativas à CNPD

No que diz respeito ao Capítulo II da Proposta, relativo à autoridade de controlo em matéria de proteção de dados, verifica-se haver também normas em desconformidade com o direito da União.

Assim, os nºs 3 e 4 do **artigo 4.º** (natureza e independência) limitam-se a replicar disposições do RGPD, respetivamente previstas nos n.ºs 1 e 2 do artigo 52.º do Regulamento, pelo que, pelas razões acima expostas (cf. II. 2), devem ser suprimidos.

Quanto ao **artigo 6.º** (atribuições e competências), o preceituado nas alíneas *d)* e *e)* do n.º 1 também repete o que vem previsto nos artigos 41.º, n.ºs 3 e 5, 42.º, n.º 5, 43.º, n.ºs 3 e 6, e 57.º, n.º 1, alíneas *p)* e *q),* do RGPD. Nessa medida, com os fundamentos já enunciados, devem estas disposições ser eliminadas da Proposta.

Ainda em relação à alínea *g)* do n.º 1 do **artigo 6.º**, em que se prevê como atribuição da CNPD «*promover ações de formação adequadas e regulares destinadas aos encarregados de proteção de dados*», não poderá deixar de se realçar que esta não é uma competência das autoridades de controlo ao abrigo do RGPD, não podendo nesse sentido o legislador nacional vir acrescentar atribuições sem que o Regulamento admita essa interferência do Estado-Membro, o que não acontece neste caso.

Além disso, nos termos do n.º 2 do artigo 38.º do RGPD, é sobre o responsável pelo tratamento e o subcontratante que recai a obrigação de fornecer ao encarregado de proteção de dados os recursos necessários para o desempenho das suas funções e a *manutenção dos seus conhecimentos*. Transferir, de certa forma, esse ónus formativo para a CNPD – ademais em concorrência aberta com o mercado – é claramente uma subversão das regras. O RGPD apenas prevê que a autoridade de controlo promova a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações nos termos do Regulamento[8], o que, atentas as funções do encarregado de proteção de dados na organização, já significa poder este desempenhar um papel relevante na intermediação das ações de sensibilização. Deve pois esta norma, porque contrária ao direito da União, ser eliminada do articulado.

No que diz respeito ao n.º 1 do **artigo 7.º** da Proposta (avaliações prévias de impacto), em que é imposto à CNPD o dever de elaborar «uma lista de tipos de tratamentos de dados cuja avaliação prévia de impacto não é obrigatória», entende-se que esta disposição contraria o RGPD, na medida em que este obriga à elaboração de uma lista positiva (cf. n.º 4 do artigo 35.º), mas deixa à discricionariedade da autoridade de controlo a possibilidade de fazer uma lista negativa (cf. n.º 5 do mesmo artigo do Regulamento).

Assim, atribuindo o RGPD esta faculdade diretamente à autoridade de controlo e não ao Estado-Membro, não deu margem ao legislador nacional para regular esta matéria, pelo que esta norma deve ser igualmente suprimida.

---

[8] Cf. Artigo 57.º, n.º 1, alínea *d)* do RGPD.

Contudo, o princípio subjacente ao n.º 2 do artigo 7.º da Proposta de promover a realização de avaliações de impacto voluntariamente, isto é, quando não dependam de qualquer tipo de obrigação, é muito bem-vindo e pode estar vertido na lei, uma vez que não contraria o disposto no RGPD. Assim, propõe-se a seguinte redação para o artigo:

1 – Nas situações em que não seja obrigatória a realização da avaliação de impacto a que se refere o artigo 35.º do RGPD, os responsáveis pelo tratamento e os subcontratantes podem efetuar essa avaliação prévia de impacto por iniciativa própria, ainda que nos mesmos termos em que ocorre qualquer avaliação de impacto obrigatória.
2 – As listas referidas nos n.ºs 4 e 5 do artigo 35.º do RGPD são publicitadas no sítio da CNPD na Internet.

Em relação ao **artigo 8.º** da Proposta (Dever de colaboração), suscitam-se sérias reservas quanto ao seu teor. Desde logo, em relação aos n.ºs 1 e 2 do artigo, pois limitam-se a reproduzir o conteúdo das normas constantes do artigo 58.º, n.º 1, alíneas *a), e)* e *f)* do RGPD, sendo que o dever genérico de cooperação com a autoridade de controlo, *a pedido desta, na prossecução das suas atribuições* está igualmente previsto no artigo 31.º do RGPD. Deste modo, em conformidade com o direito da União, estas duas disposições devem ser eliminadas.

No que diz respeito ao n.º 3 do artigo 8.º, que impõe um dever de sigilo aos «membros da CNPD, bem como aos técnicos por esta mandatados», convém analisar com atenção o preceito. Em primeiro lugar, esta é a única norma em toda a Proposta que menciona o sigilo profissional a que fica sujeito quem exerça funções na CNPD. Todavia, fica aquém do previsto no artigo 54.º, n.º 2, do RGPD, uma vez que tem como referência apenas o contexto de ação inspetiva da CNPD e não o conjunto da atividade de uma autoridade de controlo. Com efeito, o universo de pessoas sujeitas a sigilo profissional deve abranger os membros e todo o pessoal da autoridade, como resulta do Regulamento e não apenas o pessoal mandatado para uma fiscalização. Essa é, aliás, a realidade atual patente no artigo 17.º da LPDP, que alarga o dever de sigilo profissional a todos quantos exerçam funções na CNPD.

Assim, de novo, verifica-se que o legislador nacional está a violar o direito da União. Embora o artigo 54.º, n.º 2, do RGPD admita alguma regulação por parte do Estado-Membro, esta não pode contrariar o alcance da disposição regulamentar europeia, isto é, quer

relativamente ao universo das pessoas sujeitas a sigilo, quer quanto à sua duração e alcance, o que efetivamente acontece.

Em segundo lugar, não se compreende a autonomização do «segredo comercial» uma vez que o RGPD já inclui no dever de sigilo dos membros e pessoal da autoridade de controlo *quaisquer informações confidenciais*, e há um conjunto de outro tipo de segredos legalmente protegidos e que seriam igualmente valoráveis, tais como: sigilo médico, sigilo fiscal, sigilo das comunicações (na vertente de dados de tráfego e de localização), sigilo bancário ou sigilo da segurança social.

Por último, o **n.º 4 do** artigo 8.º da Proposta, na forma como está redigido, constitui um manifesto incumprimento do RGPD, pois faz cessar automaticamente os poderes da autoridade de controlo de aceder aos dados pessoais tratados e obter todas as informações relevantes ao desempenho das suas funções. Como acima já exemplificado, existem vários tipos de segredo, em diversos setores de atividade, e que espelham precisamente a proteção acrescida que é dada a informação especialmente sensível – o que é extremamente relevante também do ponto de vista da proteção de dados pessoais, sendo nessa medida até merecedora de controlo reforçado.

Assim, para defesa dos direitos, liberdades e garantias dos cidadãos, poder verificar com eficácia o cumprimento das normas de proteção de dados é indispensável à atividade da CNPD. Ademais neste novo quadro legislativo em que o modelo de supervisão mudou para um controlo *a posteriori*. Ora uma norma aberta que estabelece que os poderes de fiscalização da CNPD não prejudicam o dever de segredo é impeditiva, na prática, de realizar qualquer tipo de ação fiscalizadora e recolher eventual prova, uma vez que tal lhe fica vedado, podendo os responsáveis pelos tratamentos escudar-se a não dar acesso aos seus sistemas de informação invocando o dever de segredo.

Deste modo, deixaria de ser possível, por exemplo, a CNPD realizar uma fiscalização eficaz a uma instituição bancária, à Autoridade Tributária, aos serviços da Segurança Social, a qualquer estabelecimento de saúde, a uma operadora de telecomunicações.

O RGPD permite ao Estado-Membro adotar no seu ordenamento jurídico regras que permitam conciliar determinadas obrigações de sigilo com o direito à proteção de dados pessoais, *caso tal seja necessário e proporcionado* mas sempre *dentro dos limites* do Regulamento (cf. artigo 90.º e considerando 164 do RGPD).

Não é o que se verifica no n.º 4 do artigo 8.º da Proposta, no qual não são especificadas medidas nem existe qualquer compatibilização concreta, assente num juízo de proporcionalidade, que permitisse interferir nos poderes atribuídos pelo RGPD às autoridades de controlo, limitando-se genericamente a fazer soçobrar a ação da CNPD perante a invocação por parte do responsável pelo tratamento ou do subcontratante de qualquer sigilo profissional.

Não tendo existindo até ao momento no ordenamento jurídico português limitações dessa ordem à fiscalização da CNPD, à semelhança de outras entidades públicas com competências de inspeção, a menos que o legislador nacional queira agora introduzir restrições de acesso pela CNPD – o que teria de ser feito nos moldes previstos no Regulamento – considera-se que o artigo 8.º deve ser eliminado, pois a redação de todos os seus números não respeita o direito da União.

Todavia, não havendo outra norma nesta Proposta que preveja o dever de sigilo dos membros e pessoal da CNPD, considera-se que o artigo 8.º possa regular essa matéria, em moldes idênticos ao que existe atualmente e em linha com o RGPD, sugerindo-se a seguinte redação para o artigo 8.º, cuja epígrafe passaria a ser sobre o sigilo profissional:

1 - Os membros e o pessoal da CNPD ficam obrigados a sigilo profissional quanto aos dados pessoais ou a informações confidenciais a que tenham acesso no exercício das suas funções.

2 – A obrigação de sigilo mantém-se mesmo após o termo das suas funções.

1.3. Normas relativas ao encarregado de proteção de dados

O Capítulo III da Proposta diz respeito à figura do encarregado de proteção de dados (EPD). Nesta matéria, o RGPD deixa muito pouca margem aos Estados-Membros para legislar.

Assim, em relação ao **artigo 9.º** da Proposta (disposição geral), a norma nacional repete o n.º 5 do artigo 37.º do RGPD, quanto às qualificações profissionais do encarregado de proteção de dados, determinando no final que este não carece de certificação para o exercício de funções.

Sendo o RGPD omisso quanto a isso, não estabelecendo por isso qualquer obrigação de certificação, considera-se que pode ser relevante e clarificador para os responsáveis e subcontratantes introduzir essa disposição na lei nacional, uma vez que não contradiz o

Regulamento. Contudo, para evitar reproduzir o texto do RGPD e uma remissão errónea para funções referidas no artigo 11.º da Proposta (como adiante se explicará), sugere-se a seguinte redação para o artigo 9.º:

O encarregado de proteção de dados, designado com base nos requisitos previstos no n.º 5 do artigo 37.º do RGPD, não carece de certificação profissional para o desempenho das funções a que se refere o artigo 39.º do RGPD.

Quanto ao **artigo 11.º** da Proposta, pretende-se estabelecer funções adicionais aos encarregados de proteção de dados, quando tal não é permitido pelo Regulamento, constituindo assim este artigo uma infração ao direito da União.

Além disso, o proémio do artigo faz referência aos artigos 37.º a 39.º do RGPD como se estes regulassem as funções do encarregado de proteção e dados, quando apenas o artigo 39.º o faz. Acresce que a alínea *a)* do artigo 11.º da Proposta, ao atribuir ao EPD a função de «[a]ssegurar a realização de auditorias, quer periódicas, quer não programadas» parece contradizer o vertido na alínea *b)* do n.º 1 do artigo 39.º do RGPD, que prevê apenas que o encarregado de proteção de dados controle a *conformidade com o presente regulamento (…) e com as políticas do responsável pelo tratamento (….) incluindo (…) as auditorias correspondentes*.

Por tudo isto, não sendo dado ao Estado-Membro a possibilidade de legislar sobre as funções do encarregado de proteção de dados, deve o artigo 11.º ser eliminado do texto da Proposta.

Relativamente ao **artigo 12.º** (Encarregados de proteção de dados em entidades públicas), considera-se que apenas os n.ºs 1, 2 e 5 do artigo respeitam o direito da União.

Já quanto aos n.ºs 3 e 4, não cumprem o preceituado no Regulamento, pelo que devem ser suprimidos. Com efeito, pretende-se aí dispor sobre matéria que não está na disponibilidade do Estados-Membros. Por um lado, porque o legislador está a interferir na designação dos encarregados de proteção de dados, quando é ao responsável e ao subcontratante que compete designar o EPD. Por outro lado, porque está a condicionar a distribuição e a partilha de EPD nas entidades públicas, sem ter em devida conta, no caso concreto, as respetivas estruturas organizacionais e dimensão das entidades envolvidas.

E ainda que esta matéria estivesse na disponibilidade dos Estados-Membros, o aí estatuído parece contradizer o RGPD.

Desde logo, no n.º 3 do artigo 12.º não se alcança o significado da ressalva «Independentemente de quem seja responsável pelo tratamento», uma vez que o n.º 1 do artigo 37.º do RGPD especifica que cada responsável e cada subcontratante designa um EPD, pelo que o disposto na alínea *a)* do n.º 3 do artigo 12.º da Proposta suscita as maiores reservas; até porque, lido em conjunto com o disposto no n.º 4, em limite admite um EPD para toda a administração central do Estado.

Ora, a legislação nacional não pode afastar a obrigação imposta pelo RGPD, na alínea *a)* do n.º 1 do artigo 37.º, de cada autoridade ou organismo público se dotar de um EPD. Não se ignora que o n.º 3 do artigo 37.º do RGPD permite a partilha de EPD, mas aí impõe-se também que seja tomada em conta a respetiva estrutura organizacional e dimensão. E os n.ºs 3 e 4 do artigo 12.º da Proposta não refletem essa ponderação. Importa esclarecer que a designação do mesmo EPD por vários serviços ou entidades públicos é uma opção que só pode ser seguida se ainda assim forem asseguradas condições ao encarregado de cumprir eficientemente os seus deveres, não podendo daqui resultar prejudicada a garantia dos direitos dos cidadãos.

Acresce que a previsão da alínea *d)* do n.º 3 é, em si mesma, contraditória com o disposto na alínea *a)* do n.º 1 do artigo 37.º do RGPD, porque as freguesias, enquanto pessoas coletivas de direito público, estão obrigadas a ter um encarregado de proteção de dados independentemente da natureza ou volume dos dados tratados. Sendo certo que hoje, com as atribuições e competências destas entidades, fruto do incremento da descentralização administrativa, dificilmente se pode conceber que o volume dos dados pessoais não seja significativo.

Compreende-se que na Proposta se tenha querido acautelar a definição do órgão competente para designar um EPD. Todavia, é duvidoso que se possa reconhecer que esta competência não seja exclusiva do responsável pelo tratamento de dados, por força do RGPD, e, nessa medida, não suscetível de ser imputada ao máximo superior hierárquico de uma organização administrativa – isto é evidente quando as leis, ao legitimarem um tratamento de dados, definem quem é o responsável e não o fazem coincidir com o órgão do topo da hierarquia administrativa.

Deste modo, a CNPD entende que o n.º 3 do artigo 12.º deve ser eliminado de modo a assegurar a conformidade com o disposto no n.º 1 do artigo 37.º do RGPD, valendo este último preceito como norma atributiva de competência de designação a cada responsável, em conjunto com as leis que identificam a responsabilidade dos tratamentos.

Pelos mesmos motivos, o n.º 4 do artigo 12.º deve ser eliminado, uma vez que o RGPD já prevê a partilha de EPD por diferentes responsáveis.

De igual modo, o **artigo 13.º** (Encarregados de proteção de dados em entidades privadas) limita-se a reproduzir, palavra por palavra, as alíneas *b)* e *c)* do n.º 1 do artigo 37.º do RGPD, pelo que, com os fundamentos acima expostos (cf. II.2), se afigura violador do direito da União, devendo ser, por isso, também eliminado.

1.4. Portabilidade

No **artigo 18.º** (Portabilidade e interoperabilidade dos dados) pretende-se, de novo, legislar sobre matéria não permitida pelo Regulamento europeu, ao mesmo tempo que se altera o alcance das disposições do RGPD. O n.º 1 do artigo, na forma como está redigido, torna-se interpretativo do texto do Regulamento, o que não é admissível (cf. II.2); por outro lado, o teor do n.º 2 contradiz de forma evidente o que vem previsto no artigo 20.º do RGPD. Enquanto o Regulamento dispõe que o *titular dos dados tem o direito de receber os dados pessoais (…) num formato estruturado, de uso corrente e de leitura automática (…)*, desde que o tratamento de dados se processe obviamente por meios automatizados e nas condições da alínea *a)* do n.º 1 do artigo 20.º, o legislador nacional determina que a portabilidade dos dados «deve, sempre que possível, ter lugar em formato aberto».

Adicionalmente, o n.º 3 do artigo 18.º da Proposta introduz uma novidade no regime da portabilidade, particular para o âmbito da administração pública, quando de facto o RGPD estabelece que o direito de portabilidade dos dados *não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável* (cf. n.º 3 do artigo 20.º). Aliás, o direito de portabilidade só é reconhecido pelo RGPD quando os tratamentos de dados tiverem como fundamentos de licitude um *contrato* ou o *consentimento* do titular dos dados (cf. alínea *a)* do n.º 1 do artigo 20.º). Ora estas duas regras conjugadas excluem quase na totalidade a possibilidade de

exercício do direito de portabilidade no âmbito de tratamentos de dados pela administração pública. E mesmo que pudesse haver eventuais situações em que este direito se aplicaria, teria de ser nos exatos termos do RGPD. Daí que a totalidade do artigo 18.º da Proposta deva ser também suprimido por não estar conforme o direito da União.

1.5. Dever de segredo

O **artigo 20.º** da Proposta (Dever de segredo) suscita uma crítica veemente da CNPD pela violação flagrante da nossa Constituição e da Carta dos Direitos Fundamentais da União Europeia, além do incumprimento manifesto do RGPD, ao impedir liminarmente o exercício do direito de acesso.

Nos termos da Proposta «[O]s direitos de informação e de acesso a dados pessoais previstos nos artigos 13.º a 15.º do RGPD não podem ser exercidos quando a lei imponha ao responsável pelo tratamento ou ao subcontratante um dever de segredo que seja oponível ao próprio titular dos dados».

Os artigos 13.º e 14.º do RGPD regulam, respetivamente, quais as informações a facultar ao titular quando os dados pessoais são recolhidos direta ou indiretamente. Nestes dois artigos, apenas na situação prevista no artigo 14.º, em que os dados não são recolhidos junto do seu titular mas em outra fonte, se prevê que o titular dos dados possa não ser informado sobre um determinado tratamento de dados que esteja a ser realizado em virtude de uma *obrigação legal de confidencialidade*[9] (como será, designadamente, o caso dos advogados). Essa obrigação de sigilo resultará de disposição legal específica relativa à matéria em questão e não por via de um artigo genérico embutido na lei nacional de execução do RGPD.

O artigo 15.º do RGPD regula o exercício do direito de acesso do titular aos seus dados pessoais e não prevê no próprio artigo qualquer situação de exceção. Apenas no artigo 23.º do RGPD se prevê a possibilidade de os Estados-Membros poderem *limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º,* mas apenas *desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática* para

[9] Cf. alínea *d)* do n.º 5 do artigo 14.º do RGPD.

assegurar um vasto conjunto de finalidades que vêm elencadas no n.º 1 do artigo. Além disso, quanto mais não fosse pelas exigências contidas no n.º 2 do artigo 23.º do RGPD, é evidente que as medidas legislativas referidas dizem respeito a legislação que regule concretamente tratamentos de dados específicos, pois determina, nomeadamente, que sejam incluídas disposições explícitas relativas às finalidades do tratamento, às categorias de dados pessoais tratados, aos prazos de conservação, à identificação dos responsáveis pelos tratamentos e, deveras relevante, *ao alcance das limitações impostas*.

Com efeito, qualquer limitação que seja introduzida por lei ao exercício de direitos, em particular ao exercício de um direito fundamental como é o direito de acesso, reconhecido de forma autónoma no n.º 2 do artigo 8.º da Carta e no n.º 1 do artigo 35.º da CRP, não poderá nunca resultar do teor da norma constante do artigo 20.º desta Proposta. Nem a supressão liminar do exercício de um direito é admissível, nem este é o contexto legislativo adequado para regular qualquer tipo de restrição, pois esta só poderá ocorrer no caso concreto e não de modo geral, nem um genérico "dever de segredo" é sequer uma finalidade prevista no RGPD.

Se o objetivo do legislador nacional é admitir limitações ao exercício do direito de informação e de acesso, possibilidade que o RGPD dá ao direito nacional, terá de o fazer, não no contexto desta Proposta, em particular nos termos genéricos em que está feito, mas nas medidas legislativas específicas, em cada tipo de casos. Além disso, as medidas que imponham restrições ao exercício de direitos têm de respeitar as exigências do artigo 23.º do RGPD; caso contrário não constituirão fundamento legal para o efeito.

Mesmo no contexto da investigação criminal e repressão de infrações penais, regulado pela Diretiva (UE) 2016/680, os direitos dos titulares dos dados não podem ser completamente anulados. Aos titulares é sempre garantido o exercício do seu direito de acesso. As situações de eventual derrogação têm de estar devidamente especificadas e qualquer recusa parcial ou total em fornecer informações tem de ser justificada e documentada, à luz de exceções determinadas por lei. A apreciação é casuística mas não arbitrária. Por maioria de razão, o artigo 20.º da Proposta não fornece a legitimidade necessária para tal e contraria as disposições do artigo 23.º do RGPD, pelo que deve ser suprimido.

1.6. Prazos de conservação dos dados

Quanto ao artigo 21.º da Proposta (prazo de conservação de dados pessoais), merece esta previsão vigoroso reparo por parte da CNPD, na medida em que se trata de um dos princípios relativos aos tratamentos de dados.

Clarifique-se desde já que quando o RGPD, como aliás a atual lei de proteção de dados, se refere a prazos de conservação está a reportar-se a prazos máximos de conservação, uma vez que o princípio da *limitação da conservação* prescreve que os dados pessoais devem ser conservados *apenas durante o período necessário para as finalidades para as quais são tratados* [10].

Com efeito, independentemente da definição de um prazo máximo de conservação, os dados pessoais devem ser eliminados ou tornados anónimos assim que estiver cumprida, no caso concreto, a finalidade do tratamento. Significa isto que em relação a determinados titulares dos dados, quando a finalidade do tratamento já tiver sido alcançada, devem os respetivos dados pessoais ser apagados, em vez de continuarem a ser tratados até estar vencido o prazo máximo de conservação.

A aplicação deste princípio não prejudica, obviamente, a necessidade de conservar dados quando haja lei que a tal obrigue. Porém, mesmo nestas circunstâncias, só devem ser conservados os dados que forem necessários para o cumprimento da obrigação legal e não outros que para o efeito não sejam necessários. Será o exemplo clássico de um tratamento de dados de gestão de clientes, em que é obrigatório a empresa manter os dados de faturação do cliente por um período de 10 anos para fins fiscais, daí não decorrendo o dever de conservar outros dados relativos ao cliente (tais como contactos, idade, consumos detalhados, interesses e preferências) se a relação contratual for terminada ao fim de dois anos.

A redação proposta no artigo 21.º desvirtua por completo este princípio basilar do regime de proteção de dados, constante em todos os instrumentos jurídicos internacionais de proteção de dados desde 1981 com a Convenção 108 do Conselho da Europa (Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal).

---

[10] Cf. Alínea *e)* do n.º 1 do artigo 5.º do RGPD.

Em primeiro lugar, o RGPD só admite ao Estado-Membro legislar nesta matéria, e mesmo assim dentro dos parâmetros definidos pelo Regulamento, quanto à conservação de dados *durante períodos mais longos* quando em causa esteja a prossecução exclusiva de fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos.

Ora, não é isso que acontece. A Proposta de Lei pretende regular outras vertentes – aliás de forma incompreensível –, o que é por si só violador do direito da União, uma vez que o legislador nacional está adstrito a disciplinar apenas as matérias permitidas pelo Regulamento da União, conforme já bastamente explicado à luz da jurisprudência europeia.

Assim, os n.ºs 1 e 4 do artigo 21.º subvertem o princípio da limitação da conservação com assomos de repetição ademais incorreta do direito da União, como acima já explanado.

O n.º 3 introduz uma finalidade autónoma e genérica – *comprovar o cumprimento de obrigações* – que seria comum a todos os tratamentos e paralela às finalidades legítimas e determinadas de cada um deles, para dar cobertura a uma conservação de dados por tempo quase ilimitado, o que é verdadeiramente intolerável. Por um lado, o prazo de conservação dos dados está sempre adstrito à finalidade específica do tratamento que esteve na base da sua recolha ou tratamento posterior; por outro lado, comprovar o cumprimento de obrigações não é uma finalidade em si mesma; por último, esta norma pretende também abranger os subcontratantes, quando estes não têm na sua disponibilidade estabelecer prazos de conservação de dados pessoais, que tratam apenas por conta e em nome do responsável pelo tratamento.

O n.º 5 deste artigo dispõe que caso exista «*um prazo de conservação de dados imposto por lei, só pode ser exercido o direito ao apagamento previsto no artigo 17.º do RGPD findo esse prazo».* Esta disposição opõe-se manifestamente ao teor do próprio artigo 17.º do Regulamento. Aqui se prevê, designadamente, que o titular dos dados tem o direito ao apagamento dos seus dados pessoais, caso se oponha ao seu tratamento por motivos relacionados com a sua situação particular e não existam interesses legítimos prevalecentes[11], ou quando os dados forem tratados ilicitamente.

---

[11] Nos termos do artigo 21.º, n.º 1, do RGPD, o direito de oposição do titular pode ser exercido mesmo quando estejam em causa tratamentos de dados pessoais, baseados na alínea e) do n.º 1 do artigo 6.º, ou seja, tratamentos necessários ao exercício de funções de interesse público ou ao exercício da autoridade pública de que o responsável está investido. Aliás à semelhança do que já acontece no atual regime de proteção de dados.

Deste modo, não é o facto de existir um prazo de conservação de dados, legalmente fixado, que poderá ser impeditivo de o titular dos dados exercer o seu direito ao apagamento, desde que reunidas as condições legais para esse apagamento, o que terá de ser apreciado caso-a-caso. Na verdade, não existe relação entre os dois vetores, sendo o n.º 5 contrário ao RGPD ao pretender coartar o exercício de um direito por motivo não atendível de acordo com o regulamento europeu.

Nesse sentido, os n.ºs 1, 3, 4 e 5 do artigo 21.º deveriam ser suprimidos da Proposta por serem violadores do direito da União.

Analisemos agora o teor do n.º 2 do artigo 21.º, que versa sobre matéria que, essa sim, é remetida para o direito do Estado-Membro. Aí se prevê que, quando «*não seja possível determinar antecipadamente o momento em que o* [tratamento] *deixa de ser necessário, é lícita a conservação dos dados pessoais».*

A este propósito, convém recordar o considerando 39 do RGPD: *os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo*. Esta relação estreita entre o princípio da limitação da conservação e o princípio da minimização dos dados, enquanto manifestação do princípio da proporcionalidade no âmbito dos tratamentos de dados, obriga a que os dados sejam apenas conservados enquanto forem necessários à prossecução da finalidade que está na base da sua recolha.

Tendo isto presente, causa a maior perplexidade a opção vertida nesta Proposta, no n.º 2, de dispensar a limitação da conservação dos dados, e de a dispensar com uma tal amplitude.

Na verdade, tal como está redigida, a norma permite a conservação ilimitada de dados pessoais *para qualquer finalidade*, por consideração ainda de um fator que não vem considerado no RGPD – o da *natureza* do tratamento –, desde que não seja possível determinar antecipadamente o momento em que o mesmo deixa de ser necessário. Portanto, estamos perante uma previsão legal que não só abre uma exceção à regra da limitação da conservação dos dados para além dos casos excecionados no RGPD (que só admite exceções quanto a tratamentos que visam os fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos), como também permite a

conservação *ad eternum* dos mesmos, em clara violação do princípio da proporcionalidade, na vertente de necessidade – recorda-se que o RGPD admite prazos de conservação *mais longos*, mas não que a conservação se faça sem limite.

Acresce que o RGPD exige ainda que, quando haja lugar à conservação de dados por períodos mais longos exclusivamente para as finalidades elencadas na alínea *e)* do n.º 1 do artigo 5.º do RGPD, os dados fiquem sujeitos à obrigação de adoção de medidas técnicas e organizativas adequadas para salvaguardar os direitos fundamentais dos titulares de dados. E quanto a estas, o n.º 2 do artigo 21.º é completamente omisso.

É inconcebível como se pretende de forma tão indeterminada outorgar licitude a tratamentos de dados em patente subversão de um dos princípios basilares da proteção de dados. Além disso, apesar de estarem em causa fins tão diferenciados, que implicam necessidades distintas em contextos diversificados, não há sequer uma tentativa de segregação das especificidades de cada um, regulando tudo em bloco como se do mesmo universo se tratasse.

Em suma, o n.º 2 do artigo 21.º viola o princípio da proporcionalidade e o previsto expressamente na alínea *e)* do n.º 1 do artigo 5.º e o n.º 1 do artigo 89.º do RGPD, sendo por isso imperiosa a sua revisão.

1.7. Transferências de dados

No que diz respeito ao **artigo 22.º** (Transferência de dados), padece esta norma exatamente do mesmo vício já assinalado em outros artigos desta Proposta. Pretende-se regular numa disposição geral aquilo que deve estar preceituado com precisão no caso concreto.

Na verdade, a possibilidade de realizar transferência de dados pessoais para países terceiros ou organizações internacionais que não tenham um nível de proteção adequado, quando a transferência *for necessária por importantes razões de interesse público*, devendo este interesse púbico ser reconhecido *pelo direito da União ou pelo direito do Estado-Membro a que o responsável pelo tratamento se encontre sujeito*[12], não se consubstancia numa norma que dispõe, em abstrato, haver *interesse público* sempre que uma entidade

12 Cf. alínea d) do n.º 1 e n.º 4 do artigo 49.º do RGPD.

pública no exercício dos seus poderes de autoridade transfira dados pessoais em cumprimento de uma obrigação legal sem aferir o contexto real.

Derrogação idêntica já existe atualmente na Diretiva 95/46/CE e na LPDP, carecendo a sua aplicação naturalmente da apreciação, no caso específico, se tal transferência (quanto ao responsável pelo tratamento, à finalidade da transferência, ao seu objeto e à existência de garantias adequadas) é *legalmente exigida para a proteção de um interesse público importante*[13]. O reconhecimento do interesse público de um tratamento de dados pessoais – ou de uma operação de tratamento, como seja uma transferência de dados – deve assim estar legalmente previsto no ato legislativo que prevê esse tratamento.

2. O regime excecional dos tratamentos de dados por entidades públicas

A Proposta de Lei apresenta um conjunto de artigos consagradores de um regime diferenciado para os tratamentos de dados em que os responsáveis ou subcontratantes são entidades públicas. As disposições que suscitam perplexidade constam do artigo 23.º e dos artigos 44.º e 54.º da Proposta.

2.1. Desvio de finalidade

Começando pelo **artigo 23.º** da Proposta de Lei, constata-se que aí se admite que os tratamentos de dados pessoais por entidades públicas podem ser realizados para finalidades diferentes das que justificaram a recolha dos dados, desde que esteja em causa a prossecução do interesse público. Invocam-se no artigo 23.º várias normas do RGPD, as quais, porém, como se procurará demonstrar, não conferem ao Estado-Membro o poder de admitir de modo genérico e permanente desvios de finalidade dos tratamentos.

Em primeiro lugar, importa atentar na ressalva inscrita no artigo 23.º de que as finalidades diferentes têm de corresponder a interesse público, como se tal constituísse uma garantia suficiente da tutela dos direitos dos cidadãos ou um fundamento suficiente para excecionar o princípio consagrado na alínea *b)* do n.º 1 do artigo 5.º do RGPD. Com efeito, o legislador parece esquecer que todas as finalidades de tratamentos de dados realizados por entidades públicas só podem ser de interesse público, porque a função da administração pública é

13 Cf. alínea c) do n.º 1 do artigo 20.º da LPDP.

exclusivamente a da prossecução de interesses públicos. Por essa razão, aquela ressalva é, em si mesma, supérflua. De resto, essa previsão choca ainda com o facto de as entidades públicas só poderem prosseguir os interesses públicos que coincidam com as respetivas atribuições legalmente definidas, e não todo e qualquer interesse público.

Em segundo lugar, cabe esclarecer que o princípio da finalidade, consagrado na alínea *b)* do n.º 1 do artigo 5.º do RGPD, é um princípio fundamental da proteção de dados pessoais na Europa. É, aliás, um princípio que vem explicitado no n.º 2 do artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, bem como no artigo 5.º, alínea *b),* da Convenção 108 do Conselho da Europa. Significa isto que os dados pessoais são recolhidos para a prossecução de finalidades específicas, determinadas, e que, em princípio, só podem ser utilizados para essas finalidades; o princípio admite, porém, a utilização dos dados para finalidades diferentes na medida em que estas não sejam incompatíveis com a finalidade originária. O que não é consentâneo com o princípio, tal como ele está consagrado, é a determinação de que todo e qualquer tratamento de dados, desde que realizado por entidades públicas, pode ter em vista qualquer finalidade distinta da originária, uma vez que essa determinação corresponde à negação do próprio princípio.

Assim, é evidente que uma norma do direito nacional que admita a utilização de dados pessoais dos cidadãos para qualquer fim de interesse público viola ostensivamente o princípio da finalidade e o disposto na alínea *b)* do n.º 1 do artigo 5.º do RGDP.

Em terceiro lugar, as referências normativas contidas no artigo 23.º não legitimam, como se afirmou supra, o aí disposto. Tanto a alínea *e)* do n.º 1 do artigo 6.º, como a alínea *g)* do n.º 1 do artigo 9.º do RGPD, se limitam a reconhecer a licitude do tratamento de dados pessoais quando realizado para prosseguir o interesse público (o qual tem de ser qualificado, «importante», quando em causa estejam certas categorias especiais de dados), ou seja legitimando a recolha e subsequentes operações sobre dados pessoais quando justificadas por um *específico* interesse público. A utilização subsequente dos mesmos dados para outros fins, ainda que de interesse público, não está justificada por estas alíneas, nem poderia estar, atento o estatuído na alínea *b)* do n.º 1 do artigo 5.º do RGPD.

Uma explicação mais detida exige a referência ao n.º 4 do artigo 6.º do RGPD. O que decorre desta norma é que os dados pessoais podem ser utilizados para outras finalidades sempre que se consiga concluir pela não incompatibilidade destas com a finalidade

originária que justificou a sua recolha, aí sendo elencados os critérios que o Grupo de Trabalho do Artigo 29.º (GT29)[14] já havia definido num parecer[15]. Sucede que na primeira parte do n.º 4 do artigo 6.º se exclui a possibilidade de fazer este juízo de não incompatibilidade em relação a dados pessoais tratados originariamente com fundamento no consentimento dos titulares dos dados ou com fundamento em disposição legal. Precisamente porque nestes casos, os dados pessoais só podem ser tratados para a finalidade ou as finalidades quanto às quais foi emitido o consentimento *específico* (e a especificidade do consentimento prende-se essencialmente com a finalidade do tratamento) ou para a finalidade legalmente prevista quando o tratamento assenta em norma legal, pois é certo que a lei não prevê, nem pode prever, de acordo com o princípio da finalidade, tratamentos de dados sem uma finalidade delimitada ou para finalidades genéricas.

Ora, precisamente o que se retira da primeira parte do n.º 4 do artigo 6.º é que os dados pessoais cujo tratamento assente em previsão legal não podem ser tratados para outras finalidades, salvo previsão legal específica nesse sentido, a qual «constitua uma medida necessária e proporcionada», o que supõe uma análise e ponderação para cada nova finalidade (cf. considerando 50, 2.º §). Portanto, essa previsão legal tem, obviamente, sob pena de violação do princípio da finalidade, de corresponder a uma disposição legal que admita o tratamento dos dados para uma finalidade ou finalidades específicas, determinadas, o que claramente não sucede no artigo 23.º da Proposta de Lei.

Em suma, o disposto no n.º 1 do artigo 23.º da Proposta de Lei viola ostensivamente o princípio da finalidade, consagrado na alínea *b)* do n.º 1 do artigo 5.º do RGPD, não se enquadrando no previsto no n.º 4 do artigo 6.º do mesmo diploma, pelo que deve este artigo ser eliminado.

2.2. Não sujeição ao regime sancionatório

Uma outra solução que suscita as maiores reservas à CNPD vem contida nos **artigos 44.º e 54.º** da Proposta de Lei. Aí se determina que as coimas previstas no RGPD e na própria

[14] Grupo constituído por representantes das autoridades de proteção de dados da União Europeia, previsto no artigo 29.º da Diretiva 95/46/CE – Diretiva de Proteção de Dados.

[15] Cf. Parecer 6/2014 sobre o interesse legítimo do responsável, disponível em http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf .

Proposta de Lei não se aplicam às entidades públicas, invocando-se o disposto no n.º 7 do artigo 83.º do RGPD, quanto ao regime contraordenacional.

É certo que o n.º 7 do artigo 83.º do RGPD admite que os Estados-Membros definam se as autoridades públicas ficam sujeitas a coimas e em que medida (cf. também o considerando 150), pelo que uma disposição como a do artigo 44.º da Proposta de Lei não viola o teor literal do RGPD. Todavia, importa compreender a *ratio* do n.º 7 do artigo 83.º.

Na verdade, a Diretiva 95/46/CE (cf. artigo 24.º), que o RGPD vem revogar, deu autonomia aos Estados-Membros para definirem as medidas adequadas para assegurar a plena aplicação do regime nela definido, exemplificando com a previsão da aplicação de sanções. Nessa sequência, alguns Estados-Membros não previram nas respetivas legislações sanções para o incumprimento do regime de proteção de dados pessoais por parte de entidades públicas. É essa realidade que o RGPD toma em conta, quando admite que a lei nacional não preveja, ou preveja numa determinada medida, coimas para as entidades públicas (veja-se, aliás, a referência no considerando 151 do RGPD a dois ordenamentos jurídicos onde não existem sanções pecuniárias para ilícitos administrativos ou de mera ordenação social). Ora, a opção legislativa assumida no ordenamento jurídico português foi, desde 1991, a de estabelecer o mesmo e exato regime jurídico de proteção de dados pessoais para todos os responsáveis por tratamentos de dados, independentemente da natureza jurídica privada ou pública dos mesmos.

Para afastar uma tal tradição jurídica e criar um regime diferenciado para as entidades públicas em matéria de sanções, seria de esperar que a Proposta de Lei apresentasse motivos pertinentes exclusivos das entidades públicas e que, portanto, se não verificassem quanto a entidades privadas. Estranhamente, tal opção não vem especificamente fundamentada na exposição de motivos que acompanha a Proposta de Lei, apenas se referindo genericamente que, em face do «*paradigma que esteve subjacente ao legislador europeu [ter sido] o das grandes multinacionais que gerem redes sociais ou aplicações informáticas à escala global, envolvendo a recolha e utilização intensiva de dados pessoais, […] algumas das soluções jurídicas que foram plasmadas para esse universo revelam-se por vezes desproporcionadas ou mesmo desadequadas para a generalidade do tecido empresarial nacional e para a Administração Pública […]*», acrescentando-se que «*a aplicação deste regulamento resultará em encargos administrativos elevados, que em*

muitos casos não se encontram suficientemente justificados pelos benefícios obtidos com o novo regime de proteção de dados pessoais relativamente ao regime atual».

Não se desconhecendo que o RGPD tem também em vista acautelar os dados pessoais dos cidadãos no âmbito das atividades comerciais de empresas multinacionais, não se afigura exato afirmar que o paradigma subjacente às opções nele vertidas sejam as grandes multinacionais. Em rigor, o que o RGPD toma como paradigma é a tecnologia disponível hoje para a realização de tratamentos de dados pessoais e, portanto, procura regular a utilização de soluções tecnológicas no seu estado atual de desenvolvimento e, previsivelmente, futuro.

Por outras palavras, o RGPD não pretende apenas regular, ou regular sobretudo, os tratamentos de dados pessoais de grandes empresas, porque esses tratamentos não têm necessariamente maior impacto sobre os direitos fundamentais dos cidadãos do que os tratamentos realizados por entidades públicas, que tratam dados à escala nacional e relativos ao universo populacional de um país, não tendo os cidadãos, na maior parte dos casos, como em relação a entidades privadas, alternativa ou possibilidade de escolha. Como também não pretende apenas sancionar as entidades que se dedicam a realizar lucro à custa da recolha e análise da informação sobre as pessoas, abrangendo também todas as entidades que recolhem e analisam a informação sobre as pessoas para finalidades não lucrativas, públicas ou privadas.

Assim, o regime do RGPD, o qual foi aprovado também pelo Estado português no seio das instituições europeias que intervieram no respetivo procedimento legislativo, está pensado tanto para as empresas globais que se dedicam a processar dados pessoais como para todos aqueles que, a nível global ou local, desenvolvem atividades que implicam tratamentos de dados pessoais, porque todas elas têm impacto sobre os direitos fundamentais dos cidadãos.

Desse ponto de vista, importa destacar que os tratamentos de dados pessoais realizados pelas entidades públicas (bastando, para o efeito, pensar no Estado e nos vários ministérios que o compõem) são tão ou mais intensamente intrusivos da privacidade e da liberdade dos cidadãos, do que os levados a cabo por entidades privadas, e portanto tão ou mais potencialmente restritivos de direitos fundamentais dos cidadãos. Pelo que os riscos para a

proteção e segurança dos dados pessoais se afirmam nesse contexto com tanta ou mais intensidade do que no âmbito de atividades de entidades privadas.

Sendo certo que, na perspetiva, que é a que aqui interessa a título principal, da tutela dos direitos fundamentais dos titulares dos dados, a aplicação de uma sanção ou, pelo menos, a possibilidade de aplicação de uma sanção tem uma função dissuasora da violação ou da reiteração da violação daqueles direitos, a exclusão de entidades públicas do regime sancionatório deixa fragilizados os titulares dos dados em relação aos tratamentos de dados pessoais realizados pelo Estado e demais entidades públicas.

Mesmo conhecendo-se que o artigo 11.º do Código Penal afasta, enquanto lei geral, a responsabilidade criminal das pessoas coletivas públicas, a CNPD reitera que a lesão dos bens fundamentais protegidos pelo RGPD e pela Proposta de lei pode ser perpetrada com tanta ou mais intensidade por entidades públicas do que por entidades privadas, considerando ainda que a missão que a Constituição Portuguesa atribui ao Estado português na defesa daqueles bens fundamentais justificaria uma maior responsabilização deste e não a sua isenção.

Acresce que a afirmação de que «*a aplicação deste regulamento resultará em encargos administrativos elevados, que em muitos casos não se encontram suficientemente justificados pelos benefícios obtidos com o novo regime de proteção de dados pessoais relativamente ao regime atual*», constitui, como se referiu supra, uma afirmação de princípio de que as ponderações do legislador europeu vertidas no RGPD não tiveram um resultado equilibrado e de que, por isso, às entidades públicas compensará, numa primeira fase de aplicação do RGPD (cf. artigo 59.º da Proposta), não cumprir o regulamento. Ora, a expressão deste juízo não só incentiva as entidades públicas ao retardar do cumprimento do RGPD, como corre o risco de inspirar as entidades privadas a seguir o mesmo trilho, para além de pôr em cheque o papel e atuação do Estado português enquanto colegislador no seio do Conselho.

Não se vê, por isso, razão para excluir do regime sancionatório contraordenacional e penal as entidades públicas. Sob pena de ter de se concluir pela violação do princípio da igualdade, consagrado no artigo 13.º da CRP: uma mesma restrição do direito fundamental à proteção de dados de um concreto cidadão, em violação do RGPD e da Constituição e lei

portuguesas, perpetrada por uma entidade privada justifica a aplicação de uma sanção pecuniária a esta entidade, mas já não quando realizada por uma entidade pública.

Reitera-se que, ao contrário do que sucede noutros ordenamentos jurídicos nacionais na União Europeia, onde a suscetibilidade de uma entidade pública aplicar sanções pecuniárias a outra entidade pública constituiria uma novidade, colocando portanto novos desafios jurídicos, designadamente no plano orçamental e de gestão de contas públicas, essa previsão em Portugal não importa qualquer novidade.

Aliás, importa lembrar que no ordenamento jurídico nacional essa possibilidade não está restrita ao regime sancionatório contraordenacional. Recorde-se que o Estado português aprovou, no âmbito da reforma do contencioso administrativo em 2002, uma norma que sujeita as entidades públicas à obrigação de pagar custas judiciais no âmbito dos processos em que sejam parte. E, na recente Proposta de Lei n.º 119/XIII/3ª (GOV), que estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, a solução encontrada foi a de sancionar as entidades públicas, sem portanto entender que a necessidade de regulação da tecnologia é mais intensa no setor privado do que no setor público.

Não existem, pois, questões jurídicas ou de natureza financeira novas que possam justificar esta solução discriminatória.

Em suma, a CNPD entende que o disposto nos artigos 44.º e 54.º da Proposta de Lei, ao não sujeitar ou ao isentar as entidades públicas do regime sancionatório, viola o princípio da igualdade e fragiliza a tutela dos direitos fundamentais dos cidadãos no contexto de tratamentos de dados pessoais realizados por entidades públicas.

3. As matérias de regulação obrigatória pelo legislador nacional

3.1. A acreditação e a certificação

No que diz respeito ao **artigo 14.º** da Proposta, a opção aqui assumida é a de atribuir ao IPAC, IP (Instituto Português de Acreditação, IP), a competência de acreditação de entidades às quais, por esta via, vão ser reconhecidos poderes de certificação de

tratamentos de dados. Essa opção é permitida pelo n.º 1 do artigo 43.º do RGPD[16], mas depende da definição em abstrato pela CNPD de requisitos ou critérios adicionais de acreditação.

Todavia, o n.º 2 do artigo 14.º, ao prescrever que o IPAC tome em consideração os requisitos adicionais estabelecidos pela CNPD, *quando existam*, parece pressupor que o ato de acreditação pode ser emitido sem mais pelo IPAC, IP, enquanto aqueles requisitos adicionais não forem aprovados.

Ora, já se referiu que o legislador europeu não deixou espaço aos Estados-Membros para regularem o regime da acreditação e da certificação em termos diferentes ou para além do que vem estatuído nos artigos 43.º e 42.º, respetivamente. Pelo que os n.ºs 2 e 3 do artigo 14.º devem, nesta perspetiva, ser eliminados.

Sem prejuízo do que se acaba de afirmar, importa assinalar aspetos que, de todo o modo, sempre mereceriam ser corrigidos.

Em primeiro lugar, os referidos requisitos adicionais podem não ser apenas os aprovados pela CNPD, uma vez que o RGPD reconhece ao próprio Comité Europeu para a Proteção de Dados o poder de adotar critérios adicionais (cf. n.º 3 do artigo 43.º).

Por outro lado, é indiscutível que o artigo 43.º faz depender a acreditação da definição prévia dos requisitos adicionais pela CNPD ou pelo Comité. Este não é, pois, um pressuposto dispensável; ao contrário, o RGPD pressupõe que, quando a entidade acreditadora seja outra que não a autoridade nacional de proteção de dados, aquela não tem conhecimentos especializados em matéria de proteção de dados pessoais, pelo que a acreditação de entidades de certificação nesta área depende necessariamente do preenchimento dos requisitos que esta autoridade ou o Comité venha a fixar.

Por conseguinte, ainda que fosse possível ao legislador nacional regular esta matéria, nunca o poderia fazer sem eliminar a parte final do n.º 2 do artigo 14.º em que se lê «quando existam», sob pena de violação ostensiva do artigo 43.º do RGPD.

Do mesmo modo, a redação do n.º 3 do artigo 14.º revela um erro quanto à definição do objeto da certificação. Em rigor, de acordo com o n.º 1 do artigo 42.º do RGPD – onde se

[16] Mas não na versão portuguesa do RGPD, onde, mais uma vez por erro grosseiro, a intervenção das duas entidades apresenta-se como cumulativa.

reconhece a criação de mecanismos de certificação *para efeitos de comprovação da conformidade das operações de tratamento* realizadas por responsáveis e subcontratantes–, objeto da certificação são os tratamentos de dados (operação ou conjunto de operações de tratamento de dados) realizados por um responsável ou subcontratante adstritos a uma específica finalidade ou a específicas finalidades.

Assim, ainda que fosse possível dispor sobre a certificação, a redação do n.º 3 do artigo 14.º, ao estabelecer que a certificação incide sobre procedimentos, estaria a violar o artigo 43.º do RGPD. Com efeito, se é certo que a certificação pode incidir sobre um procedimento, também é certo que pode incidir sobre *produtos* (um *software*, por exemplo) implementados por um responsável ou subcontratante, bem como sobre um *serviço* na medida em que este implique operações de tratamento de dados na relação entre o responsável ou um subcontratante, por um lado, e o cliente ou utilizador, por outro (por exemplo, o serviço de correio eletrónico).

Em suma, a redação do n.º 3 do artigo 14.º não está conforme ao RGPD e sempre teria pelo menos de garantir que o objeto da certificação não fosse mais restrito do que o que decorre do RGPD.

3.2. Consentimento das crianças

No que diz respeito ao n.º 1 do **artigo 16.º**, a CNPD entende que a redação do preceito precisa de ser revista, sob pena de gerar dúvidas quanto ao seu âmbito de aplicação.

Com efeito, do artigo 8.º do RGPD resulta que quando esteja em causa tratamento relativo à oferta daquele tipo de serviços, e apenas neste caso, o consentimento da criança só releva se ela tiver pelo menos a idade determinada pela legislação nacional (entre 13 e 16 anos).

Relativamente ao limite de idade fixado na Proposta de Lei, a CNPD limita-se a notar que a *ratio* do RGPD foi a de deixar que cada Estado-membro adequasse o regime do consentimento das crianças ao regime jurídico nacional, em função, portanto, da idade tida como relevante em cada ordenamento jurídico para decisões sobre a sua vida. Nesse ponto, portanto, o RGPD não pretendeu a homogeneização do regime, admitindo soluções diferenciadas em cada Estado. Ora, estando em causa determinar a partir de que idade se reconhece ter uma criança capacidade para consentir na restrição a um direito fundamental,

seria porventura expectável que na Proposta se tomasse por referência o critério fixado no Código Penal, no artigo 38.º, n.º 3, quanto ao consentimento como causa de exclusão da ilicitude penal: 16 anos. O argumento, expresso na exposição de motivos de que 13 anos foi a idade considerada em grande número de Estados-Membros[17] não se afigura, pois, decisivo numa matéria que o legislador europeu deixou claramente em aberto para harmonização da solução em cada Estado com o critério assumido no respetivo ordenamento jurídico nacional.

3.3. Tratamentos de dados para fins de liberdade de expressão e de informação

No **artigo 24.º** da Proposta de Lei, procura-se concretizar o comando contido no artigo 85.º do RGPD no sentido de conciliar, por lei, o direito à proteção de dados com os direitos à liberdade de expressão e de informação.

Porém, a simples afirmação, no n.º 1 do artigo 24.º da Proposta de Lei, de que a proteção de dados pessoais não prejudica o exercício daquelas liberdades afigura-se pouco esclarecedora e, nessa medida, irrelevante. Do mesmo modo, a determinação de que alguns direitos dos titulares dos dados pessoais deverem ser «exercidos *num quadro de ponderação* com o exercício da liberdade de informação, de imprensa e de expressão académica, artística ou literal» constitui um pobre contributo para a definição de um regime regulatório do exercício desses direitos.

Na verdade, se se compreende que o direito à proteção dos dados pessoais não pode prevalecer sobre as liberdades de expressão, informação e de imprensa, sob pena de a expressão individual e a atividade jornalística, essenciais numa sociedade democrática, não se desenvolverem, também se compreende que aquelas liberdades não podem esmagar as dimensões jurídicas substantivas protegidas pelo regime de proteção de dados, em especial a vida privada e familiar, a liberdade individual e o direito a um tratamento não discriminatório. Por isso mesmo, o próprio estatuto dos jornalistas ressalva a proteção dos dados pessoais, facto que a presente Proposta de diploma não podia ignorar.

Impunha-se, por esta razão, definir aqui um conjunto de normas suficientemente precisas para assegurar o equilíbrio entre tais direitos fundamentais. Para o efeito, seria melhor

[17] Só cinco Estados-Membros já aprovaram a legislação nacional de execução do RGPD

diferenciar a liberdade de informação e a liberdade de imprensa, por um lado, da liberdade de expressão, designadamente para fins académicos, artísticos ou literários, por outro.

As liberdades de informação e de imprensa, por serem concretizadas no âmbito do exercício de uma atividade profissional regulada – a atividade jornalística –, encontram já no estatuto dos jornalistas um regime harmonizador dos direitos em tensão, não carecendo por isso de especial normação. De todo o modo, é importante a nota de que a liberdade de informação deve ser desenvolvida com respeito pelos direitos dos titulares dos dados e pelo princípio da dignidade da pessoa humana, justificando-se inserir no n.º 4 do artigo 24.º que o seu exercício deve ser feito no quadro da atividade profissional regulada, em vez de essa referência estar prevista em número autónomo.

Ao contrário, a harmonização entre a liberdade de expressão e os direitos dos titulares dos dados pessoais reclama uma maior atenção do legislador, que não se bastam com fórmulas genéricas como as que constam do n.º 1 e do n.º 2 do artigo 24.º da Proposta de Lei e que nada acrescentam ao disposto no artigo 18.º da CRP. Em princípio, a liberdade de expressão, designadamente académica, artística e literária, está sujeita ao regime de proteção de dados pessoais, em especial às condições de licitude previstas nos artigos 6.º e 9.º do RGPD e ao princípio da minimização, devendo por isso ser especificamente justificada pelo legislador nacional qualquer disposição que afaste aquelas regras.

Nesse sentido, afigura-se adequada uma previsão do tipo da constante do n.º 6 do artigo 24.º, que concretiza o princípio da proporcionalidade no âmbito do exercício da liberdade de expressão. Todavia, a sua redação suscita dúvidas. Com efeito, ou falta uma vírgula a seguir a dados pessoais, ou está a limitar-se o juízo de proporcionalidade aos dados de morada e contactos, o que é objetivamente inadmissível, quando se pensa em todos os dados sensíveis que o legislador europeu e o legislador constituinte quiseram proteger especialmente, proibindo por regra o seu tratamento.

3.4. Tratamentos de dados para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos

O RGPD prevê um conjunto de situações de tratamentos de dados em que reconhece aos Estados-Membros autonomia regulatória para garantir a aplicação do regime nele previsto e

definir um equilíbrio adequado entre os interesses de arquivo público, de investigação científica ou histórica e estatísticos e os direitos fundamentais dos titulares dos dados pessoais. Para o efeito impõe a adoção de medidas adequadas de proteção dos dados pessoais e admite derrogações em relação a certos direitos dos titulares dos dados – cf. artigo 89.º e considerandos 156-163.

Desde logo, importa notar que o artigo 89.º do RGPD, embora reconhecendo autonomia aos Estados-Membros para regularem os tratamentos de dados com fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos, impõe *em primeiro lugar* o dever de previsão de garantias adequadas dos direitos fundamentais dos titulares de dados, nos termos do RGPD. Aliás, em coerência com o disposto na alínea *j)* do n.º 2 do artigo 9.º do RGPD, que faz depender a circunstância de a lei nacional ser suficiente para legitimar os tratamentos de dados para estas finalidades da *previsão legal de medidas adequadas e específicas para a defesa dos direitos fundamentais* dos titulares dos dados, com respeito pelo princípio da proporcionalidade e do conteúdo essencial do direito à proteção de dados pessoais. *Só depois*, no n.º 2 do artigo 89.º, se admite que sejam estabelecidas derrogações a alguns direitos dos titulares previstos no RGPD.

Pelo que o legislador nacional não pode limitar-se a repetir o estatuído no n.º 1 do artigo 89.º, com afirmações genéricas quanto à necessidade de adoção de medidas técnicas e organizativas e à sua subordinação aos princípios do artigo 5.º do RGPD, e a definir derrogações também genéricas aos direitos, se de facto pretende criar regimes especiais para os tratamentos de dados pessoais com estas finalidades. É imperioso definir *o específico* regime de tratamento de dados pessoais.

Mas importa ainda chamar a atenção para o facto de as soluções a que o legislador nacional chegue, neste âmbito, dificilmente poderem ser comuns às diferentes finalidades enunciadas no artigo 89.º, porque cada uma delas justifica ou pode justificar soluções de regime distintas. Aliás, tanto é assim, que existem leis nacionais a regular especificamente o arquivo de interesse público, bem como a atividade estatística e a investigação clínica. Por isso mesmo, a CNPD entende que os regimes legais nacionais admitidos pelo artigo 89.º do RGPD têm de conter normas densificadas e específicas, que traduzam uma efetiva ponderação entre cada um dos interesses em vista e os direitos fundamentais dos titulares dos dados, com previsão de medidas técnicas e organizativas que para cada tipo de

finalidade se revelem adequadas à salvaguarda do direito à proteção de dados pessoais e com previsão das condições para o exercício dos direitos dos titulares dos dados previstos no RGPD na medida em que eventuais derrogações se revelem imprescindíveis para assegurar a prossecução de cada tipo de finalidade.

Assim, analisado o **artigo 31.º** da Proposta de Lei, conclui-se que a norma do n.º 1 pouco acrescenta ao disposto no n.º 1 do artigo 89.º do RGPD, limitando-se a mencionar as medidas de anonimização e pseudonimização, sem especificar a imprescindibilidade de que tais medidas sejam aptas e suficientes para a tutela dos direitos fundamentais dos titulares dos dados, como impõe a alínea *j)* do n.º 2 do artigo 9.º do RGPD. Nessa medida, a CNPD recomenda a sua eliminação.

No que diz respeito aos direitos dos titulares dos dados, no n.º 2 do artigo 31.º da Proposta, nenhuma ponderação é, em rigor, feita à luz do princípio da proporcionalidade, em especial, na vertente de necessidade. Afirma-se que os direitos aí enunciados *ficam prejudicados na medida do necessário*, sem qualquer juízo valorativo em função das diferentes finalidades consideradas. E, no entanto, quando se pensa que alguns dos direitos em causa correspondem ao conteúdo essencial do direito fundamental à autodeterminação informativa, consagrado no n.º 1 do artigo 35.º da CRP e no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, como sucede com o direito de acesso, facilmente se percebe que ele não pode ser negado salvo circunstâncias muito excecionais. Nesse sentido, a CNPD recomenda que este preceito seja revisto, diferenciando os regimes em função das finalidades dos tratamentos. Assim, entende a CNPD que quando o tratamento visa fins de arquivo de interesse público não se afigura fazer sentido a negação do direito de acesso aos titulares dos dados, dificilmente se concebendo ser possível negar os direitos de retificação e de limitação. Na verdade, não se vê em que medida possa o exercício destes direitos prejudicar gravemente ou tornar impossível a realização do fim de arquivo de interesse público. Apenas o direito de oposição parece poder ser sacrificado em face da finalidade de interesse público do tratamento dos dados.

Juízo de necessidade similar se aplica quando a finalidade do tratamento é a investigação científica ou histórica. Na verdade, o exercício dos direitos de acesso e de retificação por parte do titular dos dados parecem ser compatíveis com a finalidade de investigação, não se vislumbrando em que circunstâncias pode a sua prossecução ser prejudicada ou

impossibilitada por aquele. Mas também os direitos de limitação e de oposição não impossibilitam nem parecem ser suscetíveis de prejudicar gravemente a investigação científica (onde o tratamento por regra assenta no consentimento do titular), ao contrário do que sucede na investigação histórica em que o direito de oposição pode prejudicar gravemente a mesma, pelo que a CNPD entende ser admissível a derrogação legal deste direito para essa finalidade.

No que diz respeito aos fins estatísticos, salvo situações excecionais a prever na legislação especial, o exercício dos direitos de acesso, retificação e de limitação não afeta a sua prossecução. Já em relação ao direito de oposição, na medida em que em causa está a realização de uma atividade de interesse público e, nalguns casos, correspondendo a uma obrigação legal, justifica-se o seu afastamento, sob pena de se prejudicar gravemente a finalidade estatística.

Em suma, considerando que em jogo estão dimensões fundamentais no contexto de tratamentos de dados pessoais, a derrogação dos direitos de acesso e retificação não pode ser determinada sem um fundamento específico que concretize a sua necessidade, o que por regra não acontecerá. Já os direitos de limitação e oposição poderão, em relação a algumas daquelas finalidades, ser afastados por determinação legal.

Quanto ao n.º 3 do artigo 31.º, não se alcança a remissão para o Decreto-Lei n.º 16/93, de 23 de janeiro, uma vez que ele não contém qualquer norma de proteção de dados pessoais, pelo que se desconhece em que termos são ponderados os direitos dos titulares dos dados com aquele interesse. Em consequência, a CNPD recomenda a sua densificação ou, caso assim não se entenda, a eliminação deste n.º 3.

Finalmente, o n.º 4 do artigo 31.º prevê uma derrogação ao princípio da finalidade também em termos que merecem crítica. A norma centra-se no consentimento para fins de investigação científica, para admitir um consentimento genérico. De facto, aí se determina que o consentimento pode abranger diversas áreas de investigação, o que contraria o requisito da especificidade do consentimento desenvolvida no n.º 11 do artigo 4.º do RGPD. A especificidade diz, desde logo, respeito ao fim que o tratamento tem em vista, não podendo ser considerado específico, isto é circunstanciado, uma declaração de concordância com o tratamento de dados pessoais para qualquer investigação ou para qualquer investigação em diferentes áreas da ciência. O consentimento tem de ser dado

para projetos concretos e delimitados, sob pena de não ser possível perceber aquilo em que se está a consentir, admitindo-se apenas que em situações excecionais e devidamente justificadas o consentimento abranja partes do projeto que possam não estar determinadas numa fase inicial da investigação (cf. considerando 33 do RGPD) Aliás, mesmo o direito de informação, pressuposto de um consentimento livre e informado, tem de ser prestado em relação a finalidades delimitadas, não se podendo considerá-lo cumprido com uma informação genérica sobre finalidades abertas do tratamento (cf. a alínea *c)* do n.º 1 dos artigos 13.º e 14.º do RGPD).

A CNPD recomenda, por isso, a revisão do n.º 4 do artigo 31.º, de modo a cumprir o princípio da finalidade e os requisitos do consentimento previstos no RGPD, sob pena de se ter aquela norma por desconforme com o RGPD.

3.5. Audiência dos interessados e os mecanismos de cooperação e coerência

Importa ainda acautelar um outro aspeto que decorre do modelo de balcão único adotado pelo RGPD no âmbito de tratamentos transfronteiriços (*i.e.,* uma única autoridade de controlo competente para interagir e apreciar a conformidade dos tratamentos de dados realizados por uma empresa com estabelecimento(s) no território de vários Estados-Membros, ou o tratamento de dados que afete pessoas em mais do que um Estado-Membro – cf. artigo 4.º, n.º 23, do RGPD) e da aplicação do mecanismo de coerência previsto no artigo 63.º do RGPD e que se prende com a garantia de contraditório ou de defesa dos interessados, em especial dos titulares dos dados.

De acordo com o mecanismo de balcão único, no âmbito de um tratamento transfronteiriço em que o responsável do tratamento[18] ou o subcontratante[19] tenha o seu estabelecimento principal[20] num outro Estado da União e o tratamento afetar pessoas que se encontrem no território português, a autoridade de controlo competente para o apreciar e decidir não será

[18] Cfr. artigo 4.º, n.º 16, alínea a), do RGPD.

[19] Cfr. artigo 4.º, n.º 16, alínea b), do RGPD.

[20] Sobre a densificação do conceito de "estabelecimento principal" para efeitos de classificação de uma determinada autoridade de controlo como autoridade principal, remete-se para o ponto 2 das Orientações sobre a identificação da autoridade de controlo principal do responsável pelo tratamento ou do subcontratante, do GT29, disponíveis em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611235.

a CNPD mas sim a autoridade nacional do outro Estado (cf. artigo 56.º do RGPD). Ainda assim, a CNPD, nos termos do artigo 4.º, n.º 22, do RGPD, deverá ser considerada uma autoridade de controlo interessada[21] em razão, por hipótese, de ter recebido uma eventual participação do titular dos dados, sendo por regra através dela que o titular faz valer os seus interesses no procedimento (desde logo, garantindo-se assim que o faça em língua portuguesa). De resto, a CNPD terá oportunidade de expor a sua perspetiva perante a autoridade nacional competente, e caso não haja consenso quanto ao teor da decisão entre as duas autoridades, será o Comité Europeu, no âmbito do mecanismo de coerência, a dirimir o litígio e a determinar o sentido ou os critérios atendíveis à tomada da decisão a aplicar no caso concreto (cf. artigos 63.º e 65.º do RGPD).

Reflexamente o mesmo acontecerá, por caber primeiramente ao responsável pelo tratamento ou subcontratante definir qual a autoridade de controlo principal com quem deverá interagir, quando a CNPD seja apenas considerada uma autoridade de controlo interessada e discordar dessa classificação, o que deverá esclarecer diretamente junto daquele responsável pelo tratamento ou do subcontratante, sem que se prescinda da necessária concertação com as demais autoridades de controlo interessadas (ou principais). Aí e até que se esclareça a dúvida, a CNPD manterá a qualidade de autoridade de controlo interessada, podendo, todavia, «exigir [diretamente] ao responsável pelo tratamento a prestação das informações suplementares necessárias para demonstrar onde se situa o seu estabelecimento principal»[22].

Outra das situações em que a CNPD manterá um papel liderante, mas não será originariamente considerada autoridade principal nos termos do RGPD, serão aquelas em que a autoridade controlo legalmente definida como autoridade principal decide não tratar o caso[23] e a autoridade de controlo interessada seja a portuguesa. Caber-lhe-á, portanto,

---

[21] Isto é, «uma autoridade de controlo afetada pelo tratamento de dados pessoais pelo facto de: a) O responsável pelo tratamento ou o subcontratante estar estabelecido no território do Estado-Membro dessa autoridade de controlo; b) Os titulares de dados que residem no Estado-Membro dessa autoridade de controlo serem substancialmente afetados, ou suscetíveis de o ser, pelo tratamento dos dados; ou c) Ter sido apresentada uma reclamação junto dessa autoridade de controlo».

[22] Ponto 2.1.1 e 2.1.2 das orientações citadas.

[23] Cfr. ponto 3.1 das orientações citadas.

conduzir todos os procedimentos necessários à "boa decisão da causa" e assumir a totalidade do processo.

Ora, no âmbito destes procedimentos importa assegurar o direito de audiência dos interessados, em especial, do interessado perante o organismo com poder decisório. Numa primeira fase, é possível que essa audiência decorra perante a CNPD, que depois remeterá as declarações do interessado para a autoridade nacional competente. Mas surgindo elementos novos relevantes para a decisão importa garantir que o interessado seja novamente ouvido, o que, para agilizar o procedimento, pode ter de decorrer perante o Comité (que deve garantir o exercício do direito expresso em língua portuguesa). É precisamente esta possibilidade que tem de ser prevista em lei, de modo a que se considere cumprido, em face da lei portuguesa, o dever de audiência quando o mesmo tenha de ser exercido perante outra entidade que não a CNPD. Nesse sentido, a CNPD recomenda a introdução de uma norma que acautele o direito de audiência dos interessados, nos termos do artigo 121.º do Código do Procedimento Administrativo e nos termos do artigo 50.º do Regime Geral das Contraordenações, e que especifique a legitimidade de uma autoridade de controlo de outro Estado-membro ou do Comité para cumprir o dever de audiência.

Como resulta claro do que atrás se descreveu, quando a CNPD assumir a qualidade de autoridade de controlo principal, competir-lhe-á liderar o processo em causa e interagir com o(s) responsável(eis) pelo tratamento ou subcontratante(s) na medida do necessário e levar em devida conta as opiniões das demais autoridades de controlo (interessadas). Para tanto, importante será prever na legislação portuguesa causas de suspensão do processo diretamente ligadas a esta circunstância de concertação plurinacional, para evitar que estes novos procedimentos possam, por si só, afetar a efetividade das decisões da CNPD em Portugal e, com isso, pôr em causa todo o mecanismo de balcão único, bem como a coerência da aplicação do RGPD no espaço da União.

4. O regime das contraordenações

Importa agora centrar a atenção no regime das contraordenações de que se ocupam os artigos 37.º a 45.º da Proposta de Lei, com exceção do disposto no artigo 44.º, que foi já objeto de apreciação supra, em III. 2.2.

A título introdutório, esclarece-se que a CNPD não é indiferente às preocupações quanto ao quadro sancionatório previsto no RGPD sentidas pelos diferentes intervenientes nos tratamentos de dados pessoais, em especial por quem assume o papel de responsável pelo tratamento ou de subcontratante. Os limites máximos definidos no artigo 83.º, n.ºs 4 e 5, do RGPD, são objetivamente elevados e porventura excessivos quando se considera o nível geral de rendimentos em Portugal e a situação económica das organizações com estabelecimento em Portugal que realizam tratamentos de dados pessoais. A CNPD está, pois, ciente de que a aplicação em concreto daquele artigo e a fixação em cada caso de uma coima tem de ser acompanhada de uma cuidadosa ponderação de diferentes fatores (*v.g.,* a situação económica do agente e o benefício económico decorrente da infração), no contexto da realidade portuguesa.

Não deve, contudo, ser esquecido o modelo sobre que assenta o RGPD, quando reserva para as autoridades de controlo prerrogativas de atuação que não se esgotam necessariamente nos "agentes" nacionais a quem potencialmente se poderão aplicar sanções deste tipo. Recorde-se, a este título, o caso do procedimento de controlo de coerência, explicitamente previsto no artigo 63.º, mas concretizado em diversas normas do RGPD[24]. Nesses casos de tratamentos transfronteiriços (cfr. artigo 4.º, n.º 23) e independentemente de a autoridade de controlo nacional (CNPD) surgir como autoridade de controlo principal (cfr. artigo 56.º) ou autoridade de controlo interessada (artigo 4.º, n.º 22), a ponderação que haverá de ser levada a cabo, também e ainda no caso de eventuais aplicações de coimas (cfr. considerando 130), respeitará a situações de responsáveis pelo tratamento com capacidade económica e técnica para realizar tratamentos de dados simultâneos em vários países da União. Não sendo necessariamente indisputável que quem o faça nesse contexto transnacional revela já e em abstrato uma situação económica distinta de uma grande parte das empresas nacionais (mais robusta, portanto), teremos, todavia, de admitir que tal indiciará um contexto onde a consideração dos fatores económicos poderá justificar plenamente a aplicação de coimas mais próximas dos limites máximos determinados pelo RGPD.

A CNPD reconhece também que, em matéria sancionatória, os diplomas legais (da União ou nacionais) devem delimitar o exercício do poder das autoridades administrativas de

[24] Destacando-se o artigo 65.º, n.º 1, al. a), em conjugação com o artigo 60.º, n.º 4.

determinação de uma sanção contraordenacional através de critérios o mais objetivos possível, sem com isso esgotar a autonomia decisória necessária à indispensável apreciação das circunstâncias concretas de um caso. Nessa medida, são sempre preferíveis soluções legais que definam molduras sancionatórias com menor amplitude (entre os mínimos e os máximos). Mesmo quando a opção legislativa seja outra, como sucede no RGPD, devem ser previstos critérios de valoração precisos, não apenas para que sirvam como orientação sólida da valoração a concretizar pela autoridade administrativa, como também para que o caminho percorrido pela entidade administrativa possa ser repetido e, porventura corrigido, pelos tribunais.

4.1. Moldura legal das sanções

Num quadro regulatório que se pretende uniforme no espaço europeu, os limites máximos definidos nos n.ºs 4 e 5 do artigo 83.º do RGPD não parecem poder ser afastados pelos Estados-Membros da União.

a. É este o primeiro ponto que importa focar. Avaliar se o RGPD deixa ou não margem para que os Estados-Membros definam limites máximos inferiores ao estabelecido naquele artigo.

A solução vertida no n.º 2 dos **artigos 37.º e 38.º** da Proposta de Lei parece assentar no entendimento de que a autonomia regulatória reconhecida pelo legislador europeu aos legisladores nacionais permite reduzir, em abstrato, os limites máximos do RGPD em função de certos critérios. Na verdade, os dois artigos definem molduras sancionatórias distintas em função da dimensão das empresas e da natureza coletiva ou singular dos sujeitos que realizem tratamentos de dados.

É certo que o proémio dos n.ºs 4 e 5 do artigo 83.º do RGPD assume claramente que os valores pecuniários aí inscritos – 10 milhões de euros e 20 milhões de euros, consoante seja contraordenação grave ou muito grave, ou uma percentagem do volume de negócios no caso de empresa – são limites máximos e, portanto, dele diretamente decorre que as coimas não os podem ultrapassar em caso algum.

Mas uma leitura atenta do artigo 83.º demonstra que o mesmo está voltado para definir os limites de aplicação de coimas pelas autoridades de controlo, *i.e.,* tem por destinatário *cada autoridade nacional de controlo* (num juízo obviamente suscetível de ser controlado pelos

tribunais) e não o legislador nacional. Basta, aliás, comparar a redação do n.º 1 do artigo 83.º com a do n.º 1 do artigo 84.º: naquele os destinatários da norma são as autoridades de controlo, neste os destinatários são os Estados-Membros, na qualidade de legislador. Aliás, a única disposição do artigo 83.º dirigida diretamente ao legislador nacional, a constante do n.º 7, teve, precisamente por isso, que adotar uma redação distinta da dos restantes números do artigo: «os Estados-Membros podem prever».

Tanto assim é que o n.º 9 do artigo 83.º prevê expressamente a aplicabilidade direta do artigo pelas autoridades de controlo quando não exista lei nacional[25]. E a leitura dos considerandos 150 e 148 reforça esta interpretação, pondo em evidência que o disposto no artigo 83.º pretende orientar direta e vinculativamente as autoridades de controlo – no considerando 150 pode ler-se «*O presente regulamento deverá definir* as violações e *o montante máximo e o critério de fixação do valor das coimas daí decorrentes, que deverá ser determinado pela autoridade de controlo competente*, em cada caso individual».

Com o mesmo sentido olharam as demais autoridades de controlo da União para esta questão. Nas diretrizes sobre a aplicação e fixação de coimas para efeitos do Regulamento 2016/679[26], do GT29, em nenhum momento se considera, admite ou problematiza a possibilidade de os Estados-Membros poderem determinar outros critérios que não sejam os previstos no artigo 83.º, n.º 2, e distintas molduras das que se fixam no artigo 83.º, n.ºs 4 e 5. A única circunstância em que se admite liberdade de modelação por parte de cada Estado é a respeitante à execução das sanções, sendo que «Tal pode nomeadamente incluir notificações de endereço, formulários, prazos para apresentação de alegações, recursos, execução e pagamento»[27]. Logo de seguida, porém, adverte-se para a necessidade de «tais requisitos não deve[re]m impedir, na prática, a consecução da efetividade, da proporcionalidade ou do caráter dissuasivo. Uma determinação mais precisa da efetividade, da proporcionalidade ou do caráter dissuasivo será efetuada com base na prática emergente no seio das autoridades de controlo (em matéria de proteção de dados, mas também de lições retiradas de outros domínios regulados), assim como na jurisprudência resultante da interpretação desses princípios.».

---

[25] Aliás, a ausência dessa lei nacional nada tem que ver com a ausência de definição nacional de limites às sanções, mas antes com a ausência de regulação, em certos Estados-Membros, de sanções deste tipo.

[26] Disponíveis em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237.

[27] Cfr. p. 6 das diretrizes citadas.

Assim, tem de se concluir que o RGPD deixou às autoridades de controlo o poder de aplicar em concreto coimas nos montantes máximos aí previstos, naturalmente com a ponderação dos critérios orientadores do cálculo da coima a que se refere o artigo 83.º.

Donde, a fixação em abstrato, em lei nacional, de limites máximos inferiores aos previstos nos n.ºs 4 e 5 do artigo 83.º do RGPD constituir uma violação dos mesmos. Esta conclusão é corroborada pela jurisprudência do TJUE, no acórdão *Comissão/República Italiana* (proc. 39/72); reportando-se à legislação aprovado na República Italiana, o Tribunal afirma serem «*contrárias ao Tratado quaisquer modalidades de execução que possam obstar ao efeito direto dos regulamentos comunitários e desse modo comprometer a sua aplicação simultânea e uniforme no espaço comunitário*» – jurisprudência reiterada no acórdão *Variola* (proc. 34/73).

Sendo certo que do princípio do primado do Direito da União Europeia, consagrado no artigo 288.º do TFUE, decorre que os regulamentos têm valor obrigatório e são diretamente aplicáveis em todos os Estados-Membros, afastando com isso qualquer possibilidade de um «*Estado […], unilateralmente, anular os seus efeitos através de um ato legislativo oponível aos textos comunitários*» (cf. o já citado acórdão do TJUE *Costa/ENEL*, proc. 6/64).

Além disso, em ponto algum do artigo 83.º ou dos considerandos relativos ao regime sancionatório se abre espaço para a consideração autónoma da dimensão da empresa, pelo que o critério adotado pelo legislador nacional, de distinguir as pequenas e médias empresas para reservar o limite pecuniário máximo do RGPD para as grandes empresas, constitui em si mesmo uma violação do RGPD.

Importa, a este propósito, recordar que é muito pontual a relevância reconhecida no articulado do RGPD às pequenas e médias empresas, ao contrário do que sucedia na proposta inicial de regulamentação, porque se concluiu, no seio das instituições da União, que o impacto sobre os dados pessoais decorrente das condutas dos responsáveis pelos tratamentos de dados pessoais (e subcontratantes) não depende do número de trabalhadores que integram essas organizações, mas antes da natureza da atividade desenvolvida (categorias de dados tratados, volume de dados tratados, categorias de titulares dos dados objeto de tratamento, etc.). Nessa medida, a elevação a critério delimitador das molduras sancionatórias da dimensão da empresa contraria o RGPD e a *ratio* que lhe está subjacente.

À mesma conclusão se chega em relação à diferenciação das molduras sancionatórias para as pessoas singulares. Mais uma vez, em ponto nenhum do artigo 83.º do RGPD se distingue o regime em função de a infração ser cometida por pessoa coletiva ou por pessoa singular. Somente no considerando 150 se estatui que a fixação em concreto (pela autoridade de controlo) de coimas a pessoas que não sejam empresas – o que abrange ainda as pessoas coletivas de natureza não empresarial, de direito privado ou público – deve ter em conta o nível geral de rendimentos no Estado-Membro, bem como a situação económica da pessoa em questão. Portanto, o RGPD, mesmo no considerando, apenas admite que os limites máximos pecuniários sejam afastados em concreto, na ponderação levada a cabo pela autoridade de controlo. Aliás, no considerando 148, admite-se que «se o montante da coima suscetível de ser imposta constituir um encargo desproporcionado para uma pessoa singular, pode ser feita uma repreensão em vez de ser aplicada a coima», o que revela bem que o quadro de sanções pecuniárias em que a autoridade de controlo (no caso português, a CNPD) se move tem sempre de ser o previsto no n.º 4 e 5 do artigo 83.º, independentemente da natureza de pessoa coletiva ou singular do infrator.

Com os fundamentos acima expostos, a CNPD entende que a definição de limites máximos pecuniários inferiores aos limites máximos pecuniários estabelecidos no RGPD viola este ato legislativo da União Europeia e o princípio do primado do direito da União consagrado no Tratado.

b. O mesmo raciocínio tem de valer para a fixação de limites mínimos, uma vez que o RGPD não deixa espaço ao legislador nacional para definir quadro sancionatório diferente do que está estabelecido nos n.ºs 4 e 5 do artigo 83.º do RGPD.

Quando determina que «A violação das disposições a seguir enumeradas *está sujeita*, em conformidade com o n.º 2, *a coimas até* ...», o RGPD esgota o poder legislativo dos Estados-Membros quanto à definição do quadro sancionatório em relação às infrações previstas naqueles números. Admitindo apenas esse poder, nos termos do artigo 84.º do RGPD, quanto à definição de sanções penais para a violação do RGPD ou para sancionar com coima as infrações a disposições do RGPD não sancionadas no artigo 83.º.

De resto, os mínimos, tal como estão fixados na Proposta de Lei, suscitariam sempre reservas, desde logo pelo facto de, quanto às pessoas singulares, se prever um limite mínimo inferior ao previsto hoje na LPDP. Quando se tem presente que o RGPD pretende

reforçar a proteção dos dados pessoais, definindo um quadro sancionatório particularmente pesado, não pode deixar de se concluir pelo caráter desproporcionado e nada efetivo de uma norma legal que fixa um limite mínimo inferior ao limite mínimo fixado na lei nacional de há vinte anos, portanto, em violação do estatuído no RGPD (cf. n.º 1 do artigo 83.º).

c. Aliás, o facto de no RGPD só se referir o valor máximo da coima permite deduzir que o regime sancionatório assim fixado segue um modelo sancionatório similar ao do regime da concorrência, fixado no Regulamento (CE) n.º 1/2003, do Conselho de 16 de dezembro de 2002 (cf. artigo 23.º), e que inspirou o modelo consagrado no regime nacional de concorrência aprovado na Lei n.º 12/2012, de 8 de maio (cf. artigo 69.º). Neste regime, o valor máximo da coima apresenta-se como um teto ou limiar inultrapassável no processo concreto de determinação da coima, processo esse que toma por referência um «montante de base», a partir do qual se aplicam os diferentes critérios ou fatores de atenuação e agravamento.

Na verdade, o facto de o RGPD ter definido apenas os máximos das coimas aponta no sentido de que os mesmos não atuam como «[…] limite máximo de uma medida legal da sanção, mas [antes como] um limiar inultrapassável numa operação de determinação da sanção que não se orienta por ele»[28]. E que na aplicação em concreto do artigo 83.º a autoridade de controlo só pode (e deve) lançar mão dos critérios definidos no n.º 2 do mesmo artigo, para determinar o montante concreto da coima a aplicar, sem portanto parecer que possa atender a outros critérios que a lei nacional fixe.

Para obviar a eventuais juízos de inconstitucionalidade decorrentes da violação do princípio da determinação legal da coima (por caber à autoridade administrativa de controlo um muito amplo poder discricionário na definição concreta da coima), admite-se reconhecer neste máximo fixado pelo RGPD um verdadeiro máximo de uma medida legal de sanção, com efetiva função orientadora no processo de determinação concreta da coima[29], a que se juntam os critérios do n.º 2 do artigo 83.º, depreendendo-se dos n.ºs 4 e 5 do mesmo artigo

---

[28] JOSÉ LOBO MOUTINHO, «Legislador português. Precisa-se – Algumas notas sobre o regime sancionatório no Regulamento Geral sobre a Protecção de Dados (Regulamento (UE) 2016/679)», in Forum *de Proteção de Dados*, n.º 4, janeiro/2017, Edição CNPD, p. 40- (p. 53).

[29] Nesse sentido, LOBO MOUTINHO, ob. cit., pp. 53-55 e jurisprudência alemã aí citada.

que esse mínimo é 0. Esta solução permitiria ao aplicador da norma (autoridade de controlo ou tribunal) determinar um valor entre o máximo e o mínimo, como ponto de partida para o cálculo da coima.

4.2. Critérios de determinação da medida da coima

A Proposta de Lei assume no artigo 39.º três critérios para a determinação em concreto da medida da coima, além dos estabelecidos no n.º 2 do artigo 83.º do RGPD. Como se referiu, o legislador europeu não parece deixar espaço para que os Estados-Membros venham definir outros critérios de ponderação em relação às infrações previstas nos n.ºs 4 e 5 do artigo 83.º. Apenas ao abrigo do artigo 84.º, portanto para as infrações não sancionadas no RGPD, é que será possível ao legislador nacional adicionar critérios, desde que garantam sanções que sejam efetivas, proporcionadas e dissuasivas.

É certo que a alínea *k)* do n.º 2 do artigo 83.º do RGPD admite a ponderação de outros fatores agravantes ou atenuantes aplicáveis às circunstâncias de facto, como os benefícios económicos obtidos ou as perdas evitadas por via da infração. A dúvida que prevalece é se a escolha dos fatores não deve ser feita apenas no caso concreto, pela entidade (administrativa ou judicial) que aplicar a norma em concreto, e já não pelo legislador nacional de cada Estado-Membro. Afigura-se, portanto, que o disposto no artigo 39.º da Proposta ou os critérios do Regime Geral das Contraordenações não poderão relevar no âmbito das infrações elencadas no artigo 83.º do RGPD.

De todo o modo, e para a hipótese de o legislador nacional pretender manter o disposto no artigo 39.º para eventuais novas sanções, sempre se assinala que o critério previsto na alínea *a)* do n.º 1 do artigo 39.º da Proposta parece confundir dois aspetos distintos, um pertinente, outro irrelevante.

Na verdade, impõe-se a consideração da situação económica do agente, no caso de pessoa singular, ou o volume de negócios e o balanço anual, no caso de pessoa coletiva. A consideração da situação económica do infrator, também prevista no artigo 45.º do Regime Geral das Contraordenações, vem especificada no considerando 150 do RGPD, embora somente para as pessoas que não tenham natureza empresarial. Importa, contudo, notar aqui que o volume de negócios e o balanço anual de uma pessoa coletiva não retrata

necessariamente a situação económica da empresa, pelo que se estaria por esta via a definir um regime diferente para as pessoas coletivas e as pessoas singulares, em prejuízo das primeiras num aspeto de regime que não parece justificar especial diferenciação à luz dos princípios da igualdade e da justiça.

Por outro lado, a Proposta de Lei parece querer limitar-se nesta alínea às pessoas coletivas de natureza empresarial (ao reportar-se ao volume de negócios), o que se estranha por deixar de fora do critério da situação económica as pessoas coletivas privadas de fins não lucrativos. Ora, não se vê motivo pertinente para não ponderar a situação económica de tais organizações quando se esteja a fixar o montante da coima, concluindo-se também aqui pela violação dos princípios da igualdade e da justiça.

Cabe também assinalar que o critério definido na alínea *b)* do n.º 1 do artigo 39.º está já abrangido pelo critério estabelecido na alínea *a)* do n.º 2 do artigo 83.º do RGPD, quando manda tomar em conta a duração da infração, pelo que a sua autonomização neste artigo 39.º, como se correspondesse a um critério distinto, constitui uma repetição desnecessária e que só gera confusão.

Inadmissível, em face do RGPD, é a referência, na alínea *c)* do n.º 1 do mesmo artigo 39.º, à dimensão da entidade, tendo em conta o número de trabalhadores e a natureza dos serviços prestados. Este é, como se disse supra, um critério não aceite pelo RGPD, pela irrelevância da dimensão da empresa quando é certo que uma empresa com um ou dois trabalhadores pode afetar de modo particularmente intenso as dimensões fundamentais das pessoas – por exemplo, uma empresa que disponibilize uma aplicação informática (*app*) através da qual sejam recolhidos dados sensíveis partilhados com terceiros e até transferidos para território exterior ao da União. Sendo certo que no âmbito do respetivo procedimento legislativo europeu esse critério foi inicialmente equacionado, para a final não ficar acolhido no texto do articulado, com pontualíssimas exceções. Donde se conclui que a imposição da sua ponderação contradiz o RGPD e deve por isso ser eliminada. Como já se referiu, o único número a que a autoridade de controlo deve dar particular atenção é, no caso concreto, ao dos titulares de dados pessoais afetados pela violação, esse, sim, previsto na alínea *a)* do n.º 2 do artigo 83.º, do RGPD.

4.3. A tipificação dos ilícitos contraordenacionais

Constata-se ainda que na Proposta de Lei se faz um esforço de tipificação dos ilícitos contraordenacionais. Todavia, considerando a jurisprudência do TJUE referida supra em II.2, a CNPD entende que o RGPD não deixa margem aos Estados-Membros para introduzir alterações ao regime sancionatório previsto nos n.ºs 4 e 5 do artigo 83.º. Com os mesmos fundamentos, não deve o legislador nacional repetir as normas do RGPD.

Nessa medida, a CNPD recomenda a eliminação do n.º 1 do artigo 37.º, com exceção da alínea *e)* e da alínea *l),* relativa às obrigações que os Estados-Membros podem definir no âmbito das matérias abrangidas pelos artigos 85.º e seguintes do RGPD, bem como da alínea *u)* do n.º 1 do artigo 38.º da Proposta.

De todo o modo, sempre se dirá que algumas das disposições previstas no n.º 1 dos artigo 37.º e 38.º da Proposta de Lei violam o RGPD, como sucede com a alínea *h)* do artigo 37.º. Nela, a propósito da não prestação de informação nos termos impostos pelos artigos 13.º e 14.º do RGPD, distingue-se a informação relevante da não relevante (cuja omissão originaria contraordenação grave), distinção essa que não é consagrada nem reconhecida no artigo 83.º do RGPD.

Na verdade, na alínea *b)* do n.º 5 deste último artigo, sanciona-se como contraordenação muito grave a violação dos direitos dos titulares dos dados nos termos dos artigos 12. a 22º, não se distinguindo, nem se deixando espaço para distinguir em função dos elementos informativos omitidos. Consequentemente sempre teria de ser eliminada a alínea *b)* do n.º 1 do artigo 38.º da Proposta.

Acresce que, onde a Proposta de Lei podia ter previsto autonomamente comportamentos sancionáveis, limitou-se a qualificar como contraordenação muito grave «A violação das regras previstas no capítulo VI da presente lei».

Com efeito, na alínea *l)* do n.º 1 do artigo 37.º, há uma total ausência de especificação das condutas que no âmbito do capítulo VI da presente lei justificam a qualificação como contraordenação grave, em violação do princípio da tipicidade dos ilícitos.

De entre os diferentes artigos previstos nesse capítulo, só se consegue encontrar obrigações suficientemente densificadas cuja violação pode originar uma sanção nos

seguintes artigos (alguns dos quais apenas após alteração da sua redação como se sublinha ao longo deste parecer):

i. No artigo 24.º, apenas o disposto no n.º 6;
ii. No artigo 25.º, apenas o n.º 2;
iii. O artigo 27.º;
iv. No artigo 28.º, nos n.ºs 4, 5, 7 e 8;
v. No n.º 6 do artigo 28.º (ou no novo artigo que venha regular os tratamentos de dados biométricos), depois de serem especificados os limites do tratamento.

Resulta ainda da alínea *k)* do n.º 1 do artigo 37.º e do artigo 52.º da Proposta de Lei que uma mesma conduta (o incumprimento de ordens ou proibições da CNPD) é sancionada como contraordenação e como crime. Por consideração do princípio *ne bis in idem*, importaria corrigir o disposto na alínea *k)* do n.º 1 do artigo 37.º. Com efeito, reconhecendo o RGPD aos Estados-Membros autonomia para definir sanções com outra natureza para as infrações previstas no artigo 83.º, pode o legislador nacional prever como crime as infrações previstas na alínea *e)* do n.º 5 e no n.º 6 do artigo 83.º, opção seguida na presente Proposta de Lei. O que deverá evitar-se é qualificar a mesma conduta, sem qualquer distinção, como crime e contraordenação.

Assim, apenas fará sentido manter-se como contraordenação a recusa de colaboração com a CNPD. Simplesmente, como essa infração vem qualificada como contraordenação grave (cf. artigo 31.º do RGPD e alínea *a)* do n.º 4 do artigo 83.º do RGPD), o legislador nacional não a pode elevar a contraordenação muito grave.

4.4. Outros aspetos do regime contraordenacional

Importa sublinhar que o **artigo 45.º** da Proposta de Lei, quando determina a aplicação subsidiária do Regime Geral das Contraordenações «Em tudo o que não esteja previsto na presente lei em matéria contraordenacional (…)», tem de ser revisto, por forma a salvaguardar o disposto no RGPD. Assim, recomenda-se a seguinte redação para a parte inicial do artigo 45.º: *Em tudo o que não esteja previsto no RGPD e na presente lei em matéria contraordenacional (…).*

Note-se ainda que, como o Regime Geral das Contraordenações se aplica subsidiariamente, e tendo em conta o disposto no artigo 8.º deste Regime, é imprescindível prever na Proposta de Lei que, nesta matéria contraordenacional, a negligência é sempre sancionável. Esta previsão que aqui se recomenda não contraria o artigo 83.º do RGPD, porque na própria alínea *b)* do n.º 2 deste artigo se impõe ter em consideração o caráter intencional ou negligente da infração.

4.5. Tutela jurisdicional

Por último, ainda no contexto da atividade da autoridade de controlo, a CNPD gostaria de chamar a atenção para os artigos 34.º e 36.º da Proposta.

O **artigo 34.º** (tutela jurisdicional) prevê, no seu n.º 2: «[A]s ações propostas contra a CNPD são da competência dos tribunais administrativos». De acordo com o n.º 1 deste artigo, a propositura de ações por qualquer pessoa contra decisões da CNPD abrange expressamente as *de natureza contraordenacional*.

Estranha-se a razão pela qual o legislador parece defender (com este inciso) uma regressão no caminho ensaiado com a substancial especialização dos chamados "tribunais de competência especializada" que conhecem de matérias determinadas. Sem prejuízo da necessidade de proceder a ponderações periódicas sobre a efetividade de alterações passadas, o afastamento das matérias contraordenacionais daquela que era, desde 2011[30], a sua "sede natural", em matéria de competência jurisdicional, não apresenta, à primeira vista, qualquer elemento apreciativo face ao paradigma que presentemente se conhece. Com efeito, vigorava (e vigora), desde então, a competência especializada do «tribunal da concorrência, regulação e supervisão [para] conhecer das questões relativas do recurso, revisão e execução das decisões, despachos e demais medidas em processo de contraordenação legalmente suscetíveis de impugnação […] das demais entidades

[30] Cfr. artigo 2.º da Lei n.º 46/2011, de 24 de junho, que adita o artigo 89.º-B à Lei n.º 3/99, de 13 de janeiro. A competência deste tribunal vem hoje prevista no artigo 112.º da Lei n.º 62/2013, de 26 de agosto, sucessivamente alterada, em último pela Lei Orgânica n.º 4/2017, de 25 de agosto (Lei da Organização do Sistema Judiciário).

administrativas independentes com funções de regulação e supervisão»[31], onde se inseria a CNPD.

Tal como vêm redigidos os n.ºs 1 e 2 do artigo 34.º da Proposta de Lei sob análise, não pode deixar de se concluir que é pretendida uma alteração da situação atual, conferindo aos tribunais administrativos competência para julgar as «ações propostas contra as decisões, nomeadamente de natureza contraordenacional […] da CNPD».

Se, por um lado, atenta a especificidade da matéria sobre a qual se pronunciarão os tribunais administrativos e reconhecida que é a experiência, já não despicienda, do tribunal da concorrência, regulação e supervisão naquele âmbito, nos suscita a maior das dúvidas proceder a uma tão sensível alteração, por outro lado, não podem deixar de existir consequências formais de tal opção. Se o legislador pretender, efetivamente, prosseguir com esta modificação, haverá que prever a correspetiva alteração formal ao artigo 112.º, n.º 1, alínea *g),* da Lei da Organização do Sistema Judiciário.

Na hipótese contrária, e na esteira do defendido pela CNPD, considera-se que o n.º 2 do artigo 34.º deverá espelhar o previsto na Lei da Organização do Sistema Judiciário, mantendo a distinção dos tribunais competentes para apreciar respetivamente as ações de natureza administrativa e as de natureza contraordenacional. Para tanto, a mera remissão para aquela lei será suficiente para que se possa saber, a cada momento e perante questões de índole administrativa ou contraordenacional (ou, até, cível, se for o caso), a que tribunal compete a resolução dos litígios que venham a opor a CNPD a qualquer pessoa singular ou coletiva.

Nesse sentido, propõe-se a seguinte redação para o n.º 2 do artigo 34.º sobre a tutela jurisdicional:

2- A competência para conhecer das ações propostas contra a CNPD é dos tribunais administrativos, com exceção das ações de impugnação das deliberações sancionatórias, cuja competência jurisdicional se afere nos termos da Lei n.º 62/2013, de 26 de agosto.

Quanto ao **artigo 36.º** (Legitimidade da CNPD), que mantém o regime atualmente em vigor, há que notar que o legislador optou por abandonar a formulação do artigo 22.º, n.º 6, da LPDP, o que equivale a afastar a representação da CNPD em juízo por parte do Ministério

[31] Cfr. Artigo 112.º, n.º 1, alínea *g),* da Lei da Organização do Sistema Judiciário.

Público. Daqui depreende-se, o que se aceita e acolhe, a possibilidade de exercício pleno da capacidade judiciária conferida à CNPD, ainda que reconduzida, nesta sede legal, às matérias específicas do Regulamento Geral sobre a Proteção de Dados e da lei que o executa.

Este é um aspeto essencial no contexto de tutela dos direitos fundamentais, em particular atendendo ao nível de especialização e de tecnicidade que as matérias de proteção de dados comportam e à experiência e *expertise* que a CNPD detém.

Nesse sentido, a faculdade de levar as violações do regulamento ao conhecimento das autoridades judiciais e de intentar ações – opção admitida pelo RGPD no n.º 5 do artigo 58.º[32] – permitirá uma intervenção direta da autoridade de controlo nacional nos processos em que ela possa vir a intervir, independentemente da qualidade em que o venha a fazer, prescindindo-se da representação em juízo pelo Ministério Público.

5. As sanções penais

Aspeto de menor acerto é o da moldura das penas previstas para os crimes constantes da **Secção III da Proposta de Lei**. Com efeito, detetam-se situações pouco coadunáveis com os critérios de efetividade, proporcionalidade e dissuasão que o considerando 152 postula e o artigo 84.º do RGPD prescreve como norteadoras das restantes «regras relativas às outras sanções aplicáveis em caso de violação do disposto no (…) RGPD».

Também aqui, apesar do espaço de conformação ser bastante mais amplo para o legislador nacional, o regulamento não deixou à sorte de cada Estado-Membro a determinação plena e livre de eventuais sanções adicionais às que se inscrevem no RGPD. Não se disputa que o regime português assegure «garantias processuais adequadas em conformidade com os princípios gerais do direito da União e a Carta, incluindo a proteção jurídica eficaz e um processo equitativo» (cfr. considerando 148 do RGPD), mas já não se compreende como podem ter-se por efetivas, proporcionais e dissuasoras molduras penais que, inclusive, se reduzem relativamente ao que existia na LPDP.

Nota-se, positivamente, o facto de todos os crimes no elenco desta secção serem agora públicos, atendendo à eliminação do n.º 3 do artigo 44.º da LPDP, agora transposto para o

[32] Ver Considerando 129 do RGPD.

artigo 47.º da Proposta de Lei. Nele é também positivo o agravamento previsto no n.º 2 para o acesso indevido aos dados pessoais previstos nos artigos 9.º e 10.º do RGPD.

Igualmente positiva é a previsão autónoma do crime de desvio de dados, devidamente densificado no artigo 48.º da Proposta.

Já quanto ao que vem previsto para a violação do dever de sigilo (**artigo 51.º** da Proposta de Lei), em matéria de molduras penais, não se compreende a aparente regressão que se nota. No n.º 1 do artigo 51.º da Proposta de Lei passa a prever-se uma moldura para a pena de prisão de até um ano e para a pena de multa de até 120 dias relativamente a «Quem, obrigado a sigilo profissional nos termos da lei, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou em parte dados pessoais…». Comparando com idêntico preceito da LPDP, observa-se que o agente responsável pela mesma conduta era punido «com prisão até dois anos ou multa até 240 dias». Admite-se que o legislador tenha querido graduar as violações do n.º 1 e do n.º 2 de forma diferente, ao contrário do que acontecia na LPDP. Contudo, face à gravidade da conduta que aqui está em causa e tendo em conta o bem jurídico em risco, dificilmente se pode admitir que a conduta do n.º 1 do artigo 51.º possa ser revista para limites inferiores, podendo e devendo o legislador, se é essa a sua intenção, agravar as demais hipóteses previstas no n.º 2 daquele inciso.

Como nota genérica quanto às molduras previstas e atenta a complexificação conhecida e a que se espera ainda venha a ocorrer nos domínios da violação das normas, potenciada por meios tecnológicos cada vez mais intrusivos e capazes de ações disruptivas e atentatórias do direito à proteção de dados pessoais e, conexamente, do direito à reserva da intimidade da vida privada, ambos constitucionalmente previstos, propõe-se uma reponderação das mesmas por parte do legislador, no sentido de um eventual agravamento generalizado, ainda que limitado pelos critérios constitucionais e doutrinários relevantes. Tudo isto porque, de acordo com o n.º 1 do artigo 118.º do Código Penal, «O procedimento criminal extingue-se, por efeito de prescrição, logo que sobre a prática do crime tiverem decorrido os seguintes prazos: (…) c) Cinco anos, quando se tratar de crimes puníveis com pena de prisão cujo limite máximo for igual ou superior a um ano, mas inferior a cinco anos; d) Dois anos, nos casos restantes.».

Ora, a crescente especialização que esta matéria reclama da investigação criminal, associada ao grau de sofisticação que se começa a observar nas práticas criminais ligadas

à violação da proteção de dados pessoais, reclamam crescentemente verificações forenses de grande magnitude, por vezes muitíssimo prolongadas, pela extensão das violações e pelo número de titulares de dados envolvidos, não raras vezes de âmbito transnacional. Se é certo que o critério da conveniência da investigação não pode ditar, sem mais, a proporcionalidade das molduras penais, é, por outro lado, imprescindível garantir que as ditas molduras, associadas aos prazos prescricionais existentes se compatibilizem por forma a assegurar que estas práticas criminais são efetivamente punidas.

Percebe-se que o legislador tenha querido reservar para as violações ligadas aos dados previstos nos artigos 9.º e 10.º do RGPD molduras agravadas (cfr. artigos 46.º, n.º 2; 47.º, n.º 2 e 48.º, n.º 2, todos da Proposta de Lei), mas é fundamental perceber, também aqui, as alterações trazidas por este instrumento jurídico europeu, nomeadamente quanto ao catálogo de dados tidos por categorias especiais ou dados sensíveis, que é agora menor do que o que existia na LPDP, fruto da extirpação do conceito de vida privada do conjunto dos dados pessoais especialmente protegidos.

Finalmente, ainda quanto às molduras penais e à sua proporcionalidade, sobretudo em face do prescrito no artigo 84.º, n.º 1, *in fine*, do RGPD, é notório o desfasamento entre a capacidade dissuasora das coimas, com limites máximos que chegam e podem mesmo superar os dez ou os vinte milhões de euros, consoante se aplique o n.º 4 ou o n.º 5 do artigo 83.º do RGPD e as sanções criminais que têm como máximo pecuniário 120.000,00 (cento e vinte mil euros)[33]. Sem prejuízo de se reconhecerem as diferenças estruturais que distinguem a lógica dogmática das contraordenações e aquela que orienta as sanções criminais, tal não desmerece o argumento que defendemos de uma revisão, à luz das ditas efetividade, proporcionalidade e dissuasão, das molduras mais baixas assinaladas.

Uma última nota quanto ao regime sancionatório de direito penal. No **artigo 56.º**, n.º 2, da Proposta de Lei, prevê-se a sanção acessória de publicitar na Internet a condenação. Considerando que em causa pode estar a publicitação de dados pessoais (quando o infrator seja pessoa singular) e que a publicação *on-line* implica a divulgação global da informação e a sua perpetuação, esta sanção tem um intolerável impacto condicionador da vida das

[33] Cfr. artigo 47.º do Código Penal.

pessoas, transformando a pena numa sanção perpétua, o que se afigura inadmissível no nosso quadro constitucional.

A CNPD recomenda, por isso, a eliminação do n.º 2 do artigo 56.º da Proposta de Lei.

6. Matérias de regulação facultativa pelo legislador nacional

6.1. Tratamento de dados pessoais de saúde

O artigo 29.º da Proposta, sob a epígrafe *Tratamento de categorias especiais de dados pessoais,* refere-se unicamente a tratamentos de dados pessoais de saúde e só para impor o dever de sigilo a quem tenha legitimidade para os efetuar no âmbito das alíneas *h)* e *i)* do n.º 2 do artigo 9.º do RGPD.

Importa clarificar que esta norma não pode ser entendida no sentido de que qualquer das categorias de pessoas nela referida está legitimada a tratar dados pessoais de saúde e daí decorra o alargamento dos fundamentos de licitude. É que a legitimidade para aceder a dados de saúde dentro de uma organização depende da efetiva e demonstrada necessidade de acesso a essa informação, não apenas em concretização do princípio da proporcionalidade, como também por razões de segurança da informação e de proteção dos dados. Os termos amplos em que se refere, em abstrato, a possibilidade de acesso indiferenciada a todos os que de alguma forma trabalham ou colaboram dentro de uma organização, quando em causa estão dados especialmente sensíveis como são os dados de saúde, está, pois, em objetiva contradição com os princípios de proteção de dados pessoais e, em especial, com as alíneas *c)* e *f)* do n.º 1 do artigo 5.º do RGPD.

Aliás, não se alcança que os titulares de órgãos como o conselho de administração de um hospital tenham necessidade de conhecer dados pessoais identificados de saúde dos utentes do mesmo, ou que, sem mais, se justifique o acesso por trabalhadores administrativos aos ficheiros clínicos. O mesmo se diga quanto aos estudantes, os quais não realizam nem têm necessidade de realizar qualquer operação sobre dados pessoais. Sendo certo que, quanto maior for o leque de pessoas que acedem a dados de saúde, maiores são os riscos para a segurança, integridade e confidencialidade desses dados.

De resto, a grande generalidade dos profissionais de saúde já estão sujeitos ao dever de segredo, seja por forças das normas deontológicas emanadas das respetivas ordens profissionais, seja por força de contrato.

O mesmo sucede no n.º 3 do artigo 29.º, onde se admite que os titulares de órgãos e trabalhadores acedam a dados pessoais de saúde no contexto do acompanhamento, financiamento e fiscalização da atividade de prestação de cuidados de saúde. Nota-se que as atividades aqui descritas não implicam, nem devem implicar por regra o acesso a dados relativos a pessoas identificadas ou identificáveis, bastando o acesso a informação anonimizada. Quem toma decisões de financiamento não tem, em circunstância alguma, que conhecer a identidade dos titulares dos dados pessoais. Aliás, essa seria uma forma de contornar proibições legais de acesso a dados de saúde e dados genéticos por parte de laboratórios farmacêuticos ou de outras empresas cujo objeto direto não seja o de realizar diagnóstico ou prestar cuidados de saúde.

E mesmo no âmbito da fiscalização da atividade de prestação de cuidados de saúde, essa fiscalização pode ser concretizada por recurso a informação anonimizada ou codificada, não sendo por regra, necessário o conhecimento da identidade dos titulares da informação de saúde.

Por conseguinte, a CNPD recomenda a clarificação do disposto neste artigo, de modo a salvaguardar o princípio da proporcionalidade no acesso à informação, impondo medidas técnicas e organizativas, designadamente perfis de acesso, que garantam o princípio conhecido por *need to know*. Recomenda ainda a eliminação da referência a categorias de pessoas que não podem aceder a dados pessoais de saúde, sob pena de violação dos princípios e regras da segurança da informação e dos próprios deveres deontológicos a que os profissionais de saúde estão obrigados.

Considerando agora o **artigo 30.º** da Proposta, a CNPD tem as maiores reservas quanto à conformidade do seu teor com o RGPD e a CRP. Ali se prevê a possibilidade de criação de bases de dados ou registos centralizados de saúde, especificando-se que estarão assentes em plataformas únicas. Esta norma surge sem qualquer enquadramento justificativo, designadamente na exposição de motivos, que permita compreender a razão de ser da sua previsão.

Este artigo não define os aspetos essenciais do tratamento de dados para que possa ser tida como legitimadora do tratamento: desde logo, não define quem é ou pode ser responsável por tais bases de dados, nem as finalidades das mesmas. O teor aberto da norma permitiria a qualquer entidade, pública ou privada, ou pessoa singular criar uma base de dados de saúde centralizada, o que não pode ser o resultado pretendido pelo legislador nacional, por contrariar a proteção específica e reforçada exigida pelo n.º 1 do artigo 9.º do RGPD para os dados de saúde.

A estas objeções acresce ainda o risco que a centralização de informação clínica sempre importa: o evidente valor económico dos dados de saúde (de grande utilidade para laboratórios farmacêuticos e para seguradoras, por exemplo) é potenciado exponencialmente com a centralização dos mesmos (pela amplitude e maior facilidade de relacionamento da informação), sendo correspondentemente acompanhado pelo aumento do risco de violação dos dados pessoais. A este propósito assinale-se que não são apenas os requisitos de segurança e de inviolabilidade previstos no RGPD que estas bases de dados têm de respeitar, mas sim todos os requisitos previstos no RGPD.

É que o risco para os direitos e liberdades dos cidadãos da existência de um tratamento com estas características é suscetível de causar danos com tal intensidade, em especial no que respeita à possibilidade de dar origem a discriminação, a prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, ou a quaisquer outros prejuízos importantes de natureza económica ou social, que não podem ser tolerados. Ademais, sublinha-se que a informação de saúde abrange as informações sobre a pessoa recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação[34], o que é suscetível de incluir outros dados pessoais especialmente protegidos, como sejam dados que revelem a origem racial ou étnica, as convicções religiosas ou filosóficas bem como dados genéticos ou dados relativos à vida sexual ou à orientação sexual.

A probabilidade e a gravidade dos riscos para os direitos e liberdades dos cidadãos que um tal tratamento de dados pessoais acarretaria impõe uma cuidada ponderação e a realização de um estudo de impacto, bem como uma alargada discussão pública.

[34] Cf. referido na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho

Assim, considerando o teor aberto da norma que prevê a possibilidade de criação de registos ou bases de dados de saúde centralizadas, em termos que implicam um risco de restrição insuportável do direito à proteção desses dados e a outros direitos fundamentais, e portanto constituindo um condicionamento ou restrição não justificado e desnecessário daquele direito, a CNPD considera que o artigo 30.º não cumpre os princípios de proteção de dados, não respeita a proteção conferida pelo artigo 9.º do RGPD e não apresenta a densidade normativa exigível a uma norma restritiva de direitos, liberdades e garantias, para além de entender que não está demonstrada a proporcionalidade de tal restrição, nos termos do nº 2 do artigo 18.º da CRP. Com estes fundamentos, a CNPD recomenda a eliminação do artigo 30.º da Proposta.

6.2. Tratamento de dados de pessoas falecidas

No artigo 17.º da Proposta prevê-se a extensão do regime previsto no RGPD ao tratamento de dados pessoais sensíveis das pessoas falecidas, *i.e.,* os dados pessoais elencados no artigo 9.º do RGPD. A solução aqui encontrada não contraria o RGPD – o qual, embora aplicando-se diretamente apenas aos tratamentos de dados pessoais de pessoas vivas, admite no considerando 27 que os Estados-Membros apliquem o regime aos dados de pessoas falecidas –, e acompanha a proteção da personalidade após a morte assegurada pelo Código Civil português (n.º 1 do artigo 71.º). Todavia, a proteção limitada aos dados pessoais elencados no artigo 9.º do RGPD deixa, em grande medida, desprotegida a proteção dos direitos de personalidade das pessoas falecidas, por naquele não caberem, por exemplo, os dados relativos à imagem ou à vida privada.

Por essa razão, sob pena de uma contradição insanável entre a presente Proposta de Lei e o regime do Código Civil quanto à proteção dos direitos de personalidade de pessoas falecidas, recomenda-se a especificação no n.º 1 do artigo 17.º dos dados sujeitos a sigilo, designadamente dos relativos às comunicações, bem como à identidade, à imagem e à intimidade da vida privada.

Importa ainda notar a incongruência da redação da parte final do n.º 1 do artigo 17.º.

Após determinar-se a proteção dos dados pessoais das pessoas falecidas que se integrem nas categorias previstas no n.º 1 do artigo 9.º do RGPD, ressalvam-se os casos previstos no

n.º 2 do mesmo artigo. Se as situações previstas no n.º 2 do artigo 9.º do RGPD não se aplicarem aos dados das pessoas falecidas isso só pode significar que o seu tratamento está sempre proibido. Admitindo não ser essa a intenção subjacente a esta previsão, a CNPD recomenda que na parte final do n.º 1 do artigo 17.º da Proposta, em vez de «ressalvados os casos previstos no n.º 2 do mesmo artigo», se prescreva *em conformidade com o previsto no n.º 2 do mesmo artigo*.

Questão diversa, que não pode deixar de se assinalar, prende-se com o reconhecimento, no n.º 2 do artigo 17.º, aos herdeiros da legitimidade para o exercício dos direitos previstos no RGPD.

Notar-se-á, desde logo, que o Código Civil reconheceu legitimidade a familiares e herdeiros do falecido em relação aos vários direitos de personalidade, mas não em relação ao direito à reserva da intimidade da vida privada – esta solução deve-se provavelmente ao facto de se poder presumir que a vontade dos familiares e herdeiros é coincidente com a da pessoa falecida quanto à defesa do seu bom nome e da sua imagem, mas já a mesma presunção não poder ser afirmada quanto à vida privada deste. Na verdade, a vida privada do falecido é muitas vezes desconhecida dos familiares sobrevivos, não se podendo presumir que este quisesse que os seus familiares ou herdeiros acedessem a informação relativa à sua vida íntima, à sua saúde, à sua orientação sexual, etc.

Repare-se que, na terminologia da proteção de dados, o *direito de acesso*, bem como o *direito de retificação* e o *direito ao apagamento* são direitos intrínsecos do titular dos dados e diferem, não podendo por isso com eles ser confundidos, em relação a outras posições jurídicas subjetivas, designadamente, ao *acesso por terceiros,* à *obrigação de exatidão dos dados pessoais* (alínea *d)* do n.º 1 do artigo 5.º do RGPD) ou à obrigação de *eliminação da informação* (alínea *e)* do n.º 1 do artigo 5.º do RGPD).

Assim, se se compreende o reconhecimento a certas categorias de terceiros de legitimidade para garantir a defesa da honra e da reputação do falecido, tais direitos, já estão ponderadamente reconhecidos no Código Civil (cf., por exemplo, artigo 71.º, n.º 2, e 79.º, n.º 2), pelo que não é necessária a reiteração dessas faculdades na presente Proposta de Lei, sob pena de gerar insegurança jurídica, sem que com isso se adite qualquer efeito jurídico novo.

Acresce que o exercício, pelos herdeiros do falecido, do *direito de acesso* (titulado pelo falecido) aos dados pessoais é uma solução que permite às seguradoras, em especial no âmbito dos seguros de vida, acederem por via indireta a dados de saúde do falecido, nos casos em que este não tenha consentido especificamente. Com o que está o legislador a permitir um resultado que, ao menos aparentemente, parece ter querido vedar no contexto do acesso a dados pessoais constantes de documentos administrativos (cf. artigo 6.º, n.º 5, da Lei n.º 26/2016, de 22 de agosto).

Por todas as razões invocadas, a CNPD recomenda a eliminação do n.º 2 do artigo 17.º.

6.3. Videovigilância

Como se sublinhou supra, em II.3., a vida privada não está classificada pelo RGPD como um dado especialmente protegido, pelo que as condições que legitimam o seu tratamento – quanto às dimensões que vão para lá das tuteladas no n.º 1 do artigo 9.º do RGPD – têm de ser encontradas no artigo 6.º do RGPD. Um dos tratamentos de dados pessoais que tem agora de ser enquadrado neste artigo é o decorrente da utilização de sistemas de videovigilância, precisamente pelo impacto que tem na vida privada das pessoas.

Neste contexto, importa, antes de mais, avaliar em que medida pode o Estado português definir regras legais específicas sobre videovigilância, no contexto do RGPD. Ora, na ordem jurídica portuguesa reconhece-se hoje, no n.º 2 do artigo 1.º da Lei n.º 34/2013, de 16 de maio, que a atividade de segurança privada tem uma função subsidiária e complementar das forças e serviços de segurança pública do Estado. Enquanto tal, a instalação e utilização de sistemas de videovigilância desenvolvido no quadro desse diploma legal com a finalidade de garantia da segurança de pessoas e bens é percecionada pelo legislador como um tratamento de dados pessoais realizado no exercício de uma atividade complementar e conexa ao exercício da função de interesse público de segurança, razão por que é até obrigatória por lei no âmbito de certas atividades privadas (cf. artigo 8.º daquela lei). E o artigo n.º 2 do artigo 6.º reconhece aos Estados-Membros poder legislativo para disciplinar especificamente os tratamentos necessários que se revelem necessários à garantia daquele interesse público. Para além das situações abrangidas pela Lei n.º 34/2013, de 16 de maio, e das demais situações em que leis especiais impõem o dever de utilizar sistemas de

videovigilância por razões de interesse público, é ainda possível enquadrar a utilização de tais sistemas ao abrigo do Código do Trabalho (cf. n.ºs 1 e 2 do artigo 88.º do RGPD).

Nessa perspetiva, reconhece-se ser legítima e de grande pertinência a consagração na presente Proposta de Lei, no **artigo 19.º**, de condições e critérios para a delimitação do âmbito dos tratamentos de dados decorrentes dos sistemas de videovigilância, tendo em conta o significativo impacto que o mesmo é suscetível de ter na esfera jurídica dos cidadãos e que os tratamentos deixam de estar sujeitos a controlo prévio da CNPD passando a recair sobre quem quer utilizar tais sistemas a responsabilidade de avaliar se cumpre os princípios e regras de proteção de dados pessoais.

Todavia, não basta remeter para os requisitos previstos no artigo 31.º da Lei n.º 34/2013, de 16 de maio, sendo imprescindível que se especifique no n.º 1 do artigo 19.º que o tratamento de dados pessoais decorrente da utilização de sistemas de videovigilância tem de respeitar os princípios e regras definidas no RGPD.

Independentemente dos casos previstos em lei, pode ainda ser lícito realizar tratamentos de dados pessoais resultantes da utilização de sistemas de videovigilância ou da utilização de outros dispositivos que permitam o processamento de dados pessoais, designadamente de imagem e som[35], ao abrigo da alínea *f)* do n.º 1 do artigo 6.º do RGPD, desde que respeitadas as condições aí previstas e observando as restantes obrigações determinadas no Regulamento.

No que diz respeito aos limites aos tratamentos de dados decorrentes da utilização de sistemas de videovigilância ou de outros dispositivos, fixados no n.º 2 do artigo 19.º da Proposta, enquanto concretização da ponderação dos diferentes interesses e direitos em jogo, à luz do princípio da proporcionalidade, eles devem valer, não apenas para os tratamentos que assentam em previsão legal, mas também para os que se fundamentam num interesse legítimo do responsável ou de terceiro. Na realidade, considerando que os referidos sistemas envolvem um risco substancial para a liberdade e a vida privada das pessoas, a imposição legal de limites ao tratamento não elimina toda a possibilidade de o

[35] Recorda-se que são cada vez mais as utilizações de dispositivos móveis que permitem a captação de imagem, som, etc., integrados em automóveis, óculos, capacetes, com a finalidade aparente de proteção de pessoas e bens, e que recolhem dados pessoais na via pública e noutros locais destinados a ser utilizados com reserva.

realizar, sendo por isso, nessa medida, ainda aceitável esta norma legal em face da jurisprudência do TJUE.

Com efeito, o Acórdão Breyer[36] admite uma regulação nacional desde que esta não reduza o alcance do fundamento de legitimidade baseado na prossecução do interesse legítimo do responsável, isto é, desde que o Estado-Membro não exclua *de forma categórica e generalizada a possibilidade de algumas categorias de dados pessoais serem tratadas sem permitir uma ponderação dos direitos e interesses opostos em causa num caso específico* (cf. ponto 62).

Todavia, o n.º 2 do artigo 19.º deve ainda ser revisto de modo a servir de norma de conduta efetivamente orientadora e proporcionada para estes tratamentos de dados. Assim, a CNPD recomenda que na alínea *a)* seja definida uma medida máxima de captação da via pública para cobrir os acessos ao imóvel, para reduzir a incerteza jurídica e a arbitrariedade (*v.g.,* 30 cm). Do mesmo modo, na alínea *c)* a referência a áreas onde deva ser respeitada a privacidade constitui uma fórmula demasiado vaga, já que à partida a privacidade dos clientes e trabalhadores deve ser respeitada onde quer que se encontrem; recomenda-se, por isso, a sua substituição por *áreas de descanso ou lazer de clientes, bem como áreas destinadas a uso reservado dos clientes, designadamente (…),* destacando a tutela da privacidade dos trabalhadores na alínea *d).* Nesta alínea, deve, na perspetiva da CNPD, ser proibida a incidência sobre *o acesso e o interior das áreas de descanso ou de lazer dos trabalhadores, bem como das áreas destinadas a uso reservado pelos mesmos, designadamente (…).*

Entende ainda a CNPD que a captação de som deve ser por regra proibida, admitindo-se apenas durante o período em que os estabelecimentos onde se instalem os sistemas de videovigilância não estejam abertos ao público ou em funcionamento.

A este propósito, a CNPD não pode deixar de lamentar o facto de a Proposta não ter disciplinado a utilização de tecnologia distinta, designadamente de câmaras de vídeo ou de outros dispositivos acoplados a veículos aéreos não tripulados (*drones*), considerando o impacto que a sua utilização pode ter na vida privada e na liberdade das pessoas. Importante seria, desde logo, diferenciar o regime em função da finalidade e do contexto da

[36]Proc. C-582/14, disponível emhttp://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=PT

sua utilização, designadamente no âmbito do exercício de atividades profissionais reguladas (v.g., jornalista), de atividades profissionais não reguladas, mas em que o impacto sobre a proteção de dados pode ser minimizado com relativa facilidade (*v.g.,* atividade artística), e no âmbito de atividades não profissionais.

6.4. Acesso a documentos administrativos

O artigo 86.º do RGPD reconhece aos Estados-Membros poder para definir os termos em que os dados pessoais que constem de documentos oficiais na posse de uma autoridade pública ou de um organismo público ou privado para a prossecução de atribuições de interesse público podem ser divulgados, a fim de conciliar o acesso do público a tais documentos com o direito à proteção dos dados pessoais nos termos do presente regulamento.

O Estado português tem, pois, o poder de conciliar o acesso do público a documentos oficiais com o direito à proteção de dados pessoais, mas somente *nos termos do presente regulamento*. Significa isto que o regime nacional tem de respeitar os princípios, condições de licitude e, sobretudo, os direitos dos titulares previstos no RGPD.

A Proposta de Lei, nesta matéria integra um artigo relativo ao acesso a documentos oficiais (**artigo 26.º**), onde determina que o acesso a documentos administrativos que contenham dados pessoais se rege pelo disposto na Lei n.º 26/2016, de 22 de agosto – lei de acesso aos documentos administrativos (LADA). A própria LADA ressalva o regime jurídico de proteção de dados pessoais, no n.º 3 do artigo 1.º, quanto ao acesso aos documentos, e no n.º 1 do artigo 10.º e na alínea *c)* do artigo 20.º, no que diz respeito à divulgação de documentos na Internet e à reutilização de documentos. Ora a remissão da Proposta de Lei para a LADA e a ressalva do regime de proteção de dados, obriga o intérprete a voltar ao RGPD, numa lógica circular, não se conseguindo alcançar o exato regime do acesso a documentos administrativos que contenham dados pessoais (os quais, nos termos da alínea *b)* do artigo 3.º da LADA, correspondem ao conceito do artigo 4.º do RGPD).

O que é ainda dificultado pelo facto de no n.º 4 do artigo 1.º da LADA se ressalvarem uma série de regimes especiais, entre os quais alguns relativos a base de dados que não estão

sujeitas ao RGPD, mas antes à Diretiva 2016/680, o que torna ainda mais duvidoso o alcance da remissão para a LADA.

Sobretudo quando se considera que o regime de acesso aos documentos nominativos da LADA não garante os direitos dos titulares dos dados nos termos do RGPD, mesmo assentando que a tutela desses direitos tem de ser conciliada com a tutela do direito de acesso aos documentos administrativos.

Na verdade, o RGPD veio reforçar o direito de informação, nos termos dos artigos 7.º, 13.º e 14.º, sem que tenha correspondência na LADA. Desnecessário seria aqui lembrar a importância do direito de informação para a relevância jurídica do consentimento (cf. n.º 11 do artigo 4.º do RGPD).

Por outro lado, o acesso aos dados pessoais nos termos da alínea *b)* do n.º 5 do artigo 6.º da LADA assenta numa condição (o interesse direto, pessoal e constitucionalmente protegido) que não coincide com as condições do RGPD, e mesmo admitindo que o facto de os dados pessoais constarem de documentos administrativos poder justificar a redução da proteção dos seus titulares, essa justificação tem de ter lugar por razões que se prendem com o exercício específico da atividade pública e não simplesmente pelo facto de os dados pessoais estarem na posse de entidades públicas. De outro modo, a lei nacional comporta uma diferenciação de regime do acesso a dados pessoais que contraria o princípio da igualdade. É tipicamente o que sucede com os dados pessoais de saúde, cujo regime de acesso é distinto consoante se aplique o RGPD ou a LADA[37].

Um outro aspeto que é essencial prende-se com as garantias de não reutilização dos documentos que contêm dados pessoais e de não reversibilidade da anonimização – o RGPD contém regras orientadoras das medidas a adotar para cumprir o princípio da minimização dos dados, o que não sucede com a LADA.

Finalmente, a ausência de poderes inspetivos e corretivos da entidade competente para acompanhar o acesso aos documentos administrativos que contenham dados pessoais desprotege os titulares dos dados em termos que não são, em rigor, compatíveis com o RGPD.

---

[37] Basta tomar o exemplo dos interesses vitais do próprio titular, que, quando o mesmo esteja incapaz de consentir, pode justificar o acesso por terceiros, hipótese não acautelada na alínea b) do n.º 5 do artigo 6.º por não ser um interesse pessoal e direto do terceiro.

Em face disto, apenas uma de duas soluções pode assegurar que a conciliação entre os dois direitos espelhada na LADA seja feita nos termos do RGPD. Ou se considera que as ressalvas do regime jurídico de proteção de dados pessoais expressas na LADA implicam a sujeição do acesso (e das restantes operações de tratamento de dados pessoais) aos documentos administrativos com dados pessoais ao RGPD, caso em que o disposto no artigo 26.º não tem qualquer utilidade, devendo por isso ser eliminado, ou se é forçado a concluir que esta simples remissão para a lei de acesso aos documentos administrativos não cumpre os limites fixados no artigo 86.º do RGPD, pois a conciliação entre o direito de acesso pelo público a documentos administrativos e o direito à proteção dos dados pessoais não está em conformidade com o RGPD.

Ainda relacionado com a divulgação de dados pessoais, a redação do **artigo 27.º** da Proposta de Lei é indecifrável. Se o que se pretende é garantir o princípio da minimização dos dados pessoais no âmbito da contratação pública, então o critério não será o da suficiente *identificação do contraente público* (que corresponde a uma entidade pública e portanto de natureza coletiva) mas antes o da identificação do cocontraente e respetivos representantes. Deve ainda assegurar-se que, sendo necessária no âmbito deste tipo de procedimentos informação sobre os colaboradores dos candidatos ou concorrentes, a mesma seja dada sob forma agregada (sem a respetiva identificação), só se justificando a identificação dos titulares após a adjudicação, para o efeito de comprovar a correção das informações prestadas.

6.5 Publicação em jornal oficial

O **artigo 25.º** da Proposta insere-se no âmbito do regime de acesso do público a documentos oficiais, previsto no artigo 86.º do RGPD, o qual atribui ao Estado-Membro a função de conciliar aquele regime com o direito à proteção de dados pessoais.

Assim, neste artigo, o legislador nacional dispõe sobre algumas condições específicas de tratamento de dados pessoais publicados em jornais oficiais, o que se deve destacar pela positiva.

Todavia, a CNPD não poderia deixar de referir a redação do n.º 4 deste artigo, pois ela é reveladora de algum equívoco nos conceitos, contradizendo o previsto no artigo 17.º do RGPD.

Vejamos. O conceito de desindexação é distinto daquele de "*delisting*", o qual permite que uma pesquisa efetuada num motor de busca, a partir de um nome de uma pessoa singular, não retorne na lista de resultados as ligações (aos *websites* onde a informação está publicada) que o titular dos dados tenha solicitado para suprimir. Se a busca for feita através de outra chave de pesquisa que não o nome do titular, a lista de resultados apresentada permitirá então, através de ligação disponibilizada, aceder à informação que esteja publicada. A grande diferença é que deixa de ser possível a agregação massiva de informação em torno de uma pessoa através da pesquisa pelo seu nome. Este é o direito ao apagamento ou direito de eliminação (de determinadas ligações - *links*), reconhecido pelo TJUE no Acórdão *Google Spain*[38], ainda à luz do quadro legal da Diretiva de Proteção de Dados de 1995, e agora consagrado no novo regime jurídico do RGPD, como «direito a ser esquecido» pelos motores de busca.

Situação completamente diferente é a do processo de desindexação ou de não-indexação a um motor de busca. Trata-se aqui de indexação de páginas (*webpages*) e não de indexação de «dados pessoais». É decisão prévia da entidade que gere ou administra um sítio da Internet se pretende indexar o seu *website* (ou parte dele, só algumas páginas escolhidas) a motores de busca. Se optar por não indexar, pesquisas feitas no motor de busca não apontarão para esse sítio da Internet. Se optar pela indexação, poderá ainda escolher quais as páginas que pretende indexar ao motor de busca e as pesquisas apenas retornarão resultados dessas páginas.

Essa escolha criteriosa poderá, por exemplo, permitir que a informação disponível no sítio da Internet de uma autarquia, sobre o turismo, o património, a agenda cultural, a atividade política, disponibilização de formulários para requerimentos, etc., esteja indexada aos motores de busca, surgindo na lista de resultados quando se pesquisa o nome do concelho

---

38 http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30dda5f416897cd042ffb918c2f6bd5a55cd.e34KaxiLc3qMb40Rch0SaxyNbNv0?text=&docid=152065&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=258643

ou uma área temática local, enquanto páginas do sítio da Internet da autarquia relativas a decisões da câmara municipal sobre atribuições de licenças a pessoas singulares, processos disciplinares ou outro tipo de dados pessoais não sejam retornadas nas pesquisas pelo motor de busca, independentemente de se pesquisar pelo nome do indivíduo ou pela data da sessão camarária. Essa informação apenas estaria disponível através do acesso direto ao sítio da Internet da autarquia e não através de um motor de busca externo.

Daqui se conclui que o direito ao apagamento de dados pessoais publicados em jornal oficial não se pode realizar «através da desindexação desses dados pessoais em motores de busca».

Não seria possível dar exequibilidade ao pedido de um titular para desindexar os seus dados pessoais de um motor de busca; quanto muito, seria desindexada a página onde constassem esses dados pessoais, bem como toda a restante informação – pessoal ou não – que estivesse contida nessa página.

Duvida-se que seja esse o caminho pretendido pelo legislador. Além disso, o direito ao apagamento (de algumas ligações dos motores de busca) tem de ser exercido junto do responsável pelo tratamento do motor de busca; a desindexação de um motor de busca, não sendo um direito legalmente reconhecido, só pode ser efetuada pelo "gestor/administrador/responsável do sítio da Internet, o que neste caso seria o do jornal oficial. Ora o legislador nacional, no n.º 5 do artigo 25.º, determina que o responsável pelo tratamento de dados publicados no jornal oficial é «a entidade que manda proceder à publicação», a qual não terá muito provavelmente esse poder de decisão (como seria o caso, por exemplo, de publicações no Diário da República Eletrónico).

Não se trata, pois, de efetivar o exercício do direito ao apagamento através da desindexação de motores de busca, pelo que esta disposição deveria ser eliminada. Caso o legislador nacional pretenda determinar que as páginas dos jornais oficiais que contenham dados pessoais não sejam indexáveis a motores de busca, sugere-se a seguinte redação do n.º 5 do artigo 25.º:

4 – anterior n.º 5

5 – As páginas eletrónicas de jornal oficial que contenham dados pessoais não são indexadas a motores de busca.

6.6. Relações laborais

Também no âmbito das relações laborais o RGPD deixou espaço aos Estados-Membros para regular os tratamentos de dados pessoais dos trabalhadores. Porém, isso não significa uma extensa liberdade legislativa, antes obrigando a adaptação da legislação nacional ao novo modelo de supervisão administrativa que o RGPD consagra. Uma das consequências desse novo modelo é o fim do controlo administrativo prévio por parte da autoridade nacional, pelo que a simples remissão para o Código do Trabalho, tal como consta do n.º 1 do **artigo 28.º** da Proposta de Lei (mesmo que lido em conjunto com o n.º 2 do artigo 62.º da Proposta), não se afigura uma solução coerente com o RGPD ou pelo menos suficientemente clarificadora. Basta pensar que com tal remissão se abrange o disposto nos artigos 20.º e seguintes do Código do Trabalho, designadamente na parte em que se prevê a intervenção prévia da CNPD.

Assim, sugere-se que o n.º 1 do artigo 28.º da Proposta seja revisto, determinando-se que o empregador pode tratar os dados pessoais dos seus trabalhadores *para as finalidades definidas e com os limites definidos no Código do Trabalho (…)*, em vez de «nos termos definidos no Código do Trabalho […]».

Mas o artigo 28.º suscita ainda outras reservas.

No n.º 2 deste artigo especifica-se que o disposto no n.º 1 «[…] abrange igualmente o tratamento efetuado por subcontratante ou contabilista certificado em nome do empregador para fins de gestão das relações laborais […]». Ora, a referência específica à legitimidade de subcontratantes para tratarem dados pessoais é, à luz do RGPD, incompreensível. Um subcontratante processa dados pessoais *em nome e por conta* do responsável pelo tratamento (aqui, o empregador), pelo que a legitimidade para esse processamento decorre exclusivamente do contrato ao abrigo do qual essa relação de subcontratação se constitui (e do qual decorre, por imposição do RGPD, a obrigação de confidencialidade), não sendo necessário que a lei nacional venha prever tal possibilidade.

Mais estranha ainda é a autonomização do tratamento realizado por «contabilista certificado em nome do empregador, para fins de gestão das relações laborais». Desde logo, os contabilistas só podem processar dados pessoais dos trabalhadores de uma determinada entidade na qualidade de subcontratantes – *i.e.,* em nome e por conta do empregador – pelo que não se alcança a necessidade de autonomizar esta específica atividade profissional.

Mas, mais importante, é a finalidade aqui delimitada: «para fins de gestão das relações laborais». Desconhece-se que a profissão de contabilista abarque toda a gestão das relações laborais, bastando pensar nos procedimentos disciplinares ou na medicina do trabalho para perceber que há todo um conjunto de dados pessoais que estes, no exercício da sua profissão, não processam, nem podem em caso algum processar.

Por fim, ainda quanto ao n.º 2 do artigo 28.º, condiciona-se o tratamento de dados pelos subcontratantes e contabilistas certificados à celebração de um contrato de prestação de serviços e à sujeição a iguais garantias de sigilo. Importa esclarecer que o contrato de prestação de serviços não se confunde com o contrato ou ato jurídico que formalize a subcontratação regulada no artigo 28.º do RGPD. Este último artigo impõe cláusulas específicas de proteção de dados, pelo que da celebração do contrato de prestação de serviço, *per se*, nenhuma garantia decorre na perspetiva da proteção de dados pessoais.

Concluindo-se assim que o n.º 2 do artigo 28.º da Proposta nada acrescenta de relevante ao disposto no artigo 28.º do RGPD, antes contrariando ou prejudicando o alcance do aí previsto, a CNPD recomenda a sua eliminação.

No que diz respeito ao n.º 3 do artigo 28.º, a CNPD admite que a redação decorra de um qualquer lapso que torna, na realidade, o preceito incompreensível. Pretende-se, talvez, clarificar que o consentimento do trabalhador não releva, por regra, como condição de licitude de tratamentos dos dados pessoais pelo empregador, precisamente porque a natureza não paritária da relação laboral não permite assegurar a liberdade da manifestação de vontade do trabalhador, requisito imprescindível de relevância jurídica do consentimento (cf. n.º 11 do artigo 4.º e considerandos 42 e 43 do RGPD). Por essa razão, o GT29[39] entende que apenas quando do tratamento resulta uma vantagem jurídica ou material para o trabalhador é que o seu consentimento pode relevar, sendo essa circunstância a única exceção. Tal como está redigida, a alínea *a)* do n.º 3 do artigo 28.º da Proposta restringe excessivamente a relevância do consentimento do trabalhador, com isso eliminando qualquer margem de livre arbítrio dos trabalhadores mesmo quando há condições para a sua manifestação. Por essa razão, a CNPD recomenda que a alínea *a)* seja revista,

[39] Diretrizes sobre o consentimento no RGPD, revistas e aprovadas em 10 de abril de 2018, disponíveis em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

passando a constar dela *Se do tratamento não resultar uma vantagem jurídica ou económica para o trabalhador*.

Quanto à alínea *b),* o aí estatuído parece querer concretizar o disposto no n.º 4 do artigo 7.º do RGPD. Na verdade, o consentimento constitui uma condição de licitude autónoma em relação ao contrato, de acordo com o artigo 6.º do RGPD, já que, quando os dados são necessários para a celebração ou execução do contrato, uma manifestação de vontade no sentido de autorizar o tratamento dos mesmos dados não pode formar-se livremente; assim, apenas quanto aos dados que não sejam necessários à execução do contrato é que o consentimento pode relevar. A intenção do legislador nacional parece ser a de clarificar o sentido do n.º 4 do artigo 7.º no contexto das relações laborais. Uma vez que a norma tem por objeto as relações laborais, onde o RGPD deixa espaço para o legislador nacional, admite-se que esta especificação, reiterando parte do estatuído no n.º 4 do artigo 7.º, não degrada o valor da norma do RGPD.

Finalmente, o artigo 28.º, nos n.ºs 7 e 8, ocupa-se ainda da «transferência de dados pessoais dos trabalhadores entre empresas que se encontrem em relação de domínio ou de grupo, ou mantenham estruturas organizativas comuns», em termos que não suscitam reservas à CNPD, tendo em conta o disposto no n.º 2 do artigo 88.º do RGPD.

De todo o modo, sempre se assinala que os termos redutores em que a norma está expressa poderão abranger a transferência internacional de dados para entidades subcontratantes, quando estas estejam *em relação de domínio ou de grupo ou mantenham estruturas organizativas comuns*, o que acontece frequentemente. Ora, desde que os requisitos da subcontratação bem como os relativos a transferências internacionais estejam cumpridos, nos termos do RGPD, não será possível limitar à partida a transferência para subcontratantes. A este propósito, veja-se o parecer 2/2017 do GT29, de 8 de junho de 2017, sobre o tratamento de dados no local de trabalho[40].

Questão diferente é a regulada no **n.º 6 do artigo 28.º.** Aqui se legitima o tratamento de dados biométricos dos trabalhadores se a finalidade for a de controlar a assiduidade ou o acesso às instalações do empregador. Recorda-se que o n.º 1 do artigo 9.º do RGPD

[40] WP 249, disponível em http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

alargou as categorias de dados especialmente protegidos (dados sensíveis), aí introduzindo os dados biométricos que permitam a identificação inequívoca dos titulares dos dados. Se se compreende a opção de enquadrar legalmente este tipo de tratamento de dados, considerando o disposto na parte final do n.º 2 do artigo 88.º do RGPD, deve porém alertar-se para a imprescindibilidade de regular, condicionando ou limitando, o tratamento, porque a simples afirmação pela lei nacional da sua admissibilidade não permite a sua realização em conformidade com o RGPD.

A CNPD faz notar que o interesse do empregador em proteger a informação que existe ou circula no âmbito da atividade da organização poderá justificar a utilização de biometria para controlo de acesso, não apenas às instalações (controlo de acesso físico), mas também aos dispositivos eletrónicos (controlo de acesso lógico), para autenticação do utilizador. Assim, recomenda-se que na parte final da norma seja aditada a referência a controlo de acessos a sistemas e aplicações informáticos.

Além disso, o tratamento de dados biométricos comporta um tal grau de complexidade técnica que exige a definição criteriosa de regras e limites para a sua conceção e realização.

A lei tem, pois, que impor, desde logo, que o sistema biométrico não permita a reversibilidade do dado biométrico (para prevenir o risco de descodificação e de reprodução).

Tem também de proibir o registo e o armazenamento da imagem da característica biométrica (*v.g.,* representação digitalizada das impressões digitais, da iris, da geometria da mão ou da geometria facial), apenas admitindo uma representação digital (*template*).

Considerando os riscos decorrentes do relacionamento de informação pessoal e o princípio da minimização dos dados consagrado na alínea *c)* do n.º 1 do artigo 5.º do RGPD, deve ainda limitar-se o tratamento à recolha e utilização de um único dado biométrico por trabalhador.

Tudo isto deve ficar definido neste artigo, ou em artigo autónomo dedicado ao tratamento de dados biométricos, podendo remeter-se para regulamento administrativo a definição de outros aspetos do tratamento de dados, como seja a ponderação das taxas de falsas aceitações ou falsas rejeições admissíveis (como forma de garantir a adequação do

tratamento à finalidade visada, nos termos da alínea *c)* do n.º 1 do artigo 5.º do RGPD) e as formas admissíveis de armazenamento dos dados biométricos[41].

A CNPD entende ser essencial que a lei afaste ainda a possibilidade de relacionamento deste tipo de sistemas de informação com outras tecnologias, como por exemplo a interconexão com sistemas de videovigilância.

6.7. Tratamentos de dados de saúde por seguradoras

Não pode a CNPD deixar de assinalar o facto de o RGPD, no seu artigo 9.º, não legitimar diretamente o tratamento de dados de saúde no âmbito dos contratos de seguro, aspeto que a Proposta de Lei não acautelou apesar dos alertas emitidos pelo setor da atividade seguradora. Sendo certo que a consequência desta ausência de disciplina legal é o dever de eliminação dos dados de saúde tratados pelas seguradoras.

Com efeito, o contrato por si só não é condição de licitude para tratar dados sensíveis, e a alínea *b)* do n.º 2 daquele artigo limita a intervenção do legislador nacional às matérias de legislação laboral, de segurança social e de proteção social. Deste modo, apenas se poderia enquadrar aqui os seguros de saúde, na medida em que se possa considerá-los ainda como uma forma de proteção social. No mais, sobraria ainda a hipótese de o legislador, nos termos da alínea *g)* do mesmo número, considerar de interesse público importante o tratamento de dados de saúde na atividade seguradora. Ora, se se consegue acompanhar que no âmbito dos seguros obrigatórios é já reconhecido o interesse público importante, já o mesmo não acontece relativamente aos restantes seguros, designadamente os seguros de vida. Note-se que ainda que se possa reconhecer à atividade seguradora algum interesse público (enquanto atividade sujeita a regulação pública), muito dificilmente é suscetível de ser um interesse público qualificado, como exige aquela alínea *g).*

Assim, a CNPD entende que para os seguros que não sejam obrigatórios ou de saúde, apenas o n.º 4 do artigo 9.º poderá servir para legitimar os Estados-Membros a prever em lei novas condições do tratamento.

---

[41] Para uma perceção mais completa das questões que este tipo de tratamentos suscita, apesar de se tratar de um documento datado (2004) e portanto potencialmente desatualizado, pode ver-se a Deliberação da CNPD relativa aos *Princípios sobre a utilização de dados biométricos no âmbito de controlo de acessos e de assiduidade*, acessível em https://www.cnpd.pt/bin/orientacoes/PRINCIPIOS-BIOM-assiduidade-acesso.pdf

A seguir-se qualquer dos caminhos aqui apontados, é imperioso que a lei nacional preveja não apenas a possibilidade de efetuar o tratamento de dados de saúde, mas também o respetivo regime do mesmo, designadamente, os limites a que necessariamente tem de estar sujeito e as medidas de segurança e de mitigação do impacto sobre os direitos dos titulares dos dados – o que, na perspetiva da CNPD, terá mais sentido ser concretizado na legislação que regula este setor de atividade.

7. Disposições finais ou transitórias

O texto da Proposta de Lei padece de alguns lapsos jurídicos que convém corrigir, e que se refletem não só na exposição de motivos como no próprio articulado.

Para além de se afirmar, na exposição de motivos, que «o RGPD se torna eficaz» a 25 de maio de 2018 e no n.º 2 do artigo 62.º estabelece-se que «Todas as normas que prevejam autorizações ou notificações de tratamentos de dados pessoais à CNPD […] deixam de vigorar à data de entrada em vigor do RGPD». Ora, o RGPD é claríssimo a estatuir no artigo 99.º que entra em vigor no 20.º dia após a data da sua publicação (tendo sido publicado em 4 de maio de 2016) e que é aplicável a partir de 25 de maio de 2018. Ou seja, o legislador europeu assegurou um período de transição de dois anos para que os Estados-Membros, as entidades administrativas e as diferentes organizações que tratam ou processam dados pessoais se preparassem devidamente para o novo quadro jurídico.

Independentemente da dificuldade que se possa sentir em fazer corresponder aos conceitos firmados no ordenamento jurídico português algumas soluções jurídicas do direito da União Europeia (como seja a diferenciação entre vigência e aplicação de um diploma legal), não pode pretender-se, muito menos afirmar-se, que o Regulamento não se encontra já em vigor e portanto a produzir efeitos jurídicos sobre os Estados-Membros da União desde 2016. Desde logo, produz sobre estes o dever de tomar as medidas necessárias para assegurar a plena aplicação do RGPD a partir de 25 de maio de 2018 e, no mínimo, a não adotar medidas que sejam suscetíveis de comprometer a sua aplicação efetiva[42].

[42] Cf. Acórdão *Wallonie* do TJUE (C-129/96), n.ºs 44 e 45, ainda que a propósito do período de transposição de uma diretiva, mas os argumentos aí refletidos são, por um argumento de maioria de razão, válidos para os regulamentos europeus.

Esta precisão jurídica – a aplicabilidade do RGPD ter sido adiada durante dois anos – não pode, pois, ser ignorada na presente Proposta de Lei, exigindo-se rigor jurídico na redação das disposições contidas numa Proposta de Lei desta natureza.

Acresce que esta imprecisão jurídica tem consequências práticas relevantes. Especificamente, o disposto no n.º 2 do artigo 62.º da Proposta de Lei, ao determinar que as normas que preveem autorizações e notificações à CNPD deixam de vigorar na data de 25 de maio de 2016, tem um resultado absurdo. Ou seja, um diploma legal em vigor, na melhor das hipóteses, em maio de 2018 determina retroativamente que as normas que sustêm as autorizações já emitidas pela CNPD deixam de vigorar desde maio de 2016, retirando com isso base legal às decisões da CNPD. Note-se que são as mesmas normas que serviram e servem de base ao sancionamento dos responsáveis que realizam tratamentos de dados sem prévia notificação. Não pode ser esse o resultado pretendido, pelo que a CNPD considera imperiosa a revisão do n.º 2 do artigo 62.º, na parte final, passando a dispor *deixam de vigorar na data de aplicação do RGPD*.

Para além da observação feita supra, em II.2, sobre o artigo 61.º, importa ainda deixar aqui duas últimas notas quanto às disposições finais e transitórias, especificamente em relação ao **artigo 63.º** da Proposta. Em primeiro lugar, a Lei n.º 67/98, de 26 de outubro, foi alterada pela Lei n.º 103/2015, de 24 de agosto, devendo por isso ser assim referenciada. Em segundo lugar, esta lei não pode ser revogada por este diploma enquanto não for transposta a Diretiva (UE) 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Na verdade, até à aprovação da lei que transponha a Diretiva 2016/680, os tratamentos de dados pessoais realizados para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais têm de respeitar o direito à proteção de dados pessoais consagrado no artigo 35.º da CRP e no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, pelo que se considera imprescindível salvaguardar a sua sujeição ao atual regime legal de proteção de dados pessoais, consagrado na LPDP.

De resto, afigura-se útil uma norma que determine que todas as remissões para a LPDP se consideram feitas para o RGPD.

IV. Conclusões

1. Com os fundamentos acima expostos, a CNPD conclui que várias disposições da Proposta de Lei não respeitam o direito da União Europeia, na medida em que incidem sobre matérias em relação às quais o RGPD não conferiu ao Estados-Membros autonomia para legislar, uma vezes replicando as normas do RGPD, outras contrariando mesmo o regime previsto no RGPD.

   Por essa razão, a CNPD recomenda a eliminação das seguintes disposições:

   i. Norma sobre o âmbito de aplicação: artigo 2.º;
   ii. Normas relativas à CNPD: n.ºs 3 e 4 do artigo 4.º, alíneas *d), e)* e *g)* do n.º 1 do artigo 6.º, n.º 1 do artigo 7.º, artigo 8.º (propondo-se nova redação para os artigos 7.º e 8.º);
   iii. Normas relativas ao encarregado de proteção de dados: artigo 9.º (com proposta de nova redação), artigo 11.º, n.ºs 3 e 4 do artigo 12.º e artigo 13.º;
   iv. Normas sobre acreditação e certificação: n.ºs 2 e 3 do artigo 14.º;
   v. Normas sobre direitos dos titulares: os artigos 18.º e 20.º;
   vi. Normas sobre prazos de conservação: artigo 21.º (sobre os prazos de conservação, com exceção do n.º 2, que deve ser revisto)
   vii. Transferências internacionais: artigo 22.º
   viii. Disposições finais e transitórias: o n.º 2 do artigo 61.º.

2. A CNPD recomenda ainda a eliminação do regime excecional previsto nos artigos 23.º, 44.º e 54.º da Proposta para os tratamentos de dados realizados por entidades públicas. Esse regime excecional consiste, por um lado, na previsão de que os tratamentos realizados por entidades públicas, só por serem por elas realizados, podem prosseguir finalidades diferentes das que justificaram a recolha dos dados, o que traduz a negação do princípio da finalidade, em violação da alínea b) do n.º 1 do artigo 5.º do RGPD.

   Por outo lado, excecionam-se ainda as entidades públicas da aplicação de sanções em caso de violação do RGPD, o que viola o princípio da igualdade e fragiliza a tutela dos direitos fundamentais dos cidadãos no contexto de tratamentos de dados pessoais realizados por entidades públicas, quando é certo que estes podem ser tão ou mais intensamente intrusivos da privacidade e da liberdade dos cidadãos, do que os levados a

cabo por entidades privadas, e que não existem razões que justifiquem esta solução diferenciada, quando nas últimas duas décadas o regime sancionatório na lei de proteção de dados era o mesmo para entidades públicas e privadas.

3. Nas matérias em que o RGPD encarrega os Estados-Membros de definir, por via legislativa, aspetos do regime de proteção de dados, destaca-se que a Proposta de Lei assume um teor vago e aberto, não logrando prever regras específicas para os aspetos do regime sobre que incide.
   i. Assim sucede com o artigo 24.º quanto aos tratamentos de dados para fins de liberdade de expressão e de informação, onde se justificava diferenciar a liberdade de informação e a liberdade de imprensa, por um lado, da liberdade de expressão, designadamente para fins académicos, artísticos ou literários, por outro – para neste último grupo de casos se estabelecer um regime específico que concretize os princípios da proteção de dados, já que em causa não está, como no primeiro, uma atividade profissional regulada.

   ii. Do mesmo modo, no artigo 31.º, os tratamentos de dados para fins de arquivo de interesse público, fins de investigação científica ou histórica ou fins estatísticos não são objeto de definição de regras específicas, considerando-se por isso que deve ser eliminado, pela sua inutilidade, o disposto no n.ºs 1 e 3 daquele artigo.
   No que diz respeito à derrogação do exercício de direitos genericamente afirmada no n.º 2 do artigo 31.º, a sugere a sua alteração (ou a regulação da matéria em sede própria), tendo em conta que apenas quanto ao tratamento com fins de arquivo de interesse público, de investigação histórica e fins estatísticos se justifica afastar o exercício do direito de oposição, não havendo por regra razão para afastar os restantes direitos de acesso e retificação, previstos no n.º 1 do artigo 35.º da CRP, nem o direito de limitação.
   A CNPD recomenda também a revisão do n.º 4 do artigo 31.º, de modo a cumprir o princípio da finalidade e os requisitos do consentimento previstos no RGPD, sob pena de se ter aquela norma por desconforme com o RGPD.

   iii. A CNPD propõe ainda a introdução de um artigo que assegure o cumprimento de dever de audiência no âmbito dos procedimentos de cooperação com

autoridades de controlo de outros Estados-Membros e de coerência perante o Comité, por força do modelo de balcão único, bem como a previsão de causas de suspensão do procedimento diretamente decorrentes da concertação plurinacional.

4. No que diz respeito ao regime das contraordenações, os limites máximos das coimas definidos nos n.ºs 4 e 5 do artigo 83.º do RGPD não podem ser afastados pelos Estados-Membros da União, nem estes podem prever limites mínimos.
   i. Assim, a CNPD entende dever eliminar-se o n.º 2 dos artigos 37.º e 38.º, onde se prevê uma moldura sancionatória diferente da prevista no RGPD, e diferenciada em função da dimensão das empresas e da natureza coletiva ou singular dos sujeitos que realizem tratamentos de dados (fatores que o legislador europeu não considerou na definição da moldura sancionatória), em violação clara do RGPD e do primado do direto da União.
   ii. A CNPD recomenda igualmente a eliminação do artigo 39.º da Proposta, por repetir ou aditar critérios de ponderação, quando o RGPD, no n.º 2 do artigo 83.º, fechou ao legislador nacional tal possibilidade em relação às infrações previstas no RGPD, remetendo somente para o aplicador em concreto da norma – a autoridade nacional ou o tribunal – a descoberta de outros critérios.
   iii. O RGPD não deixa margem aos Estados-Membros para introduzir alterações ao elenco das infrações previsto nos n.ºs 4 e 5 do artigo 83.º, pelo que a CNPD sugere a eliminação do n.º 1 do artigo 37.º da Proposta, com exceção da alínea *e)* e da alínea *l),* relativa às obrigações que os Estados-Membros podem definir no âmbito das matérias abrangidas pelos artigos 85.º e seguintes do RGPD, bem como da alínea *u)* do n.º 1 do artigo 38.º da Proposta.
   iv. Recomenda-se também a tipificação de infrações relativas às obrigações abrangidas genericamente na alínea *l)* do n.º 1 do artigo 37.º da Proposta, que são as previstas no n.º 6 do artigo 24.º, no n.º 2 do artigo 25.º, no artigo 27.º, nos n.ºs 4, 5, 7 e 8 do artigo 28.º e no n.º 6 do artigo 28.º (após reformulação nos termos propostos pela CNPD).

v. A CNPD aconselha ainda a revisão da redação do artigo 45.º, quanto à aplicação subsidiária do Regime Geral das Contraordenações, para que se ressalve também o previsto no RGPD, e a introdução de uma disposição que preveja que, nas contraordenações, a negligência é sempre sancionável.

vi. A CNPD recomenda ainda que o n.º 2 do artigo 34.º da Proposta seja alterado, por forma a salvaguardar a competência especializada em matéria de contraordenações do tribunal da concorrência, regulação e supervisão.

5. Em relação às sanções penais previstas na Secção III da Proposta de Lei, a CNPD entende deverem ser revistas as molduras penais. Desde logo, a moldura definida no artigo 51.º da Proposta, uma vez que representa uma regressão em relação ao regime sancionatório penal atualmente previsto na LPDP, mas também as previstas nos artigos 46.º, 47.º e 48.º, que não parecem corresponder a sanções efetivas, proporcionais e dissuasoras como impõe o artigo 84.º do RGPD. Para além do notório desfasamento entre a capacidade dissuasora das coimas, com limites máximos que chegam e podem mesmo superar os dez ou os vinte milhões de euros, e as sanções criminais que têm como máximo pecuniário cento e vinte mil euros.

   A CNPD recomenda também a eliminação do n.º 2 do artigo 56.º da Proposta de Lei, por prever uma sanção acessória de publicitação na Internet da aplicação de sanção penal, o que significar transformar a pena numa sanção perpétua.

6. Nas matérias em que o RGPD deixa espaço para a disciplina legislativa nacional, a CNPD recomenda a alteração nos seguintes termos.

   i. A clarificação do disposto no artigo 29.º sobre tratamentos de dados de saúde, de modo a salvaguardar o princípio da proporcionalidade no acesso à informação, impondo a adoção de medidas técnicas e organizativas, designadamente perfis de acesso; considera ainda dever eliminar-se a referência a categorias de pessoas que não podem, em qualquer caso, aceder a dados pessoais de saúde.

ii. A CNPD entende ser inadmissível o previsto no artigo 30.º da Proposta, pelo teor vago e aberto com que admite a criação de registos ou bases de dados de saúde centralizadas, sem a densidade normativa exigível a uma norma restritiva de direitos, liberdades e garantias e suscetível de proporcionar a avaliação da proporcionalidade de tal restrição, em violação direta dos princípios de proteção de dados.

iii. Em relação ao artigo 17.º da Proposta, onde se prevê a extensão do regime previsto no RGPD ao tratamento de dados pessoais sensíveis das pessoas falecidas, a CNPD recomenda que no n.º 1 sejam aditados os dados sujeitos a sigilo, designadamente os relativos às comunicações, bem como os dados referentes à identidade, à imagem e à intimidade da vida privada. Recomenda-se também a correção da incongruência da redação da parte final do n.º 1 do artigo 17.º, e a eliminação do n.º 2 do artigo 17.º, em coerência com a tutela assegurada pelo Código Civil e com os direitos previstos no RGPD.

iv. No que diz respeito ao regime da videovigilância, previsto no artigo 19.º da Proposta, para além de sugestões para tornar mais exata a redação do n.º 1, a CNPD propõe a revisão dos limites fixados no n.º 2, no sentido de clarificar os tratamentos que ficam proibidos por traduzirem uma restrição desproporcionada dos direitos fundamentais dos titulares dos dados.

A este propósito, a CNPD lamenta o facto de a Proposta não ter disciplinado a utilização de câmaras de vídeo ou de outros dispositivos acoplados a veículos aéreos não tripulados (*drones*).

v. Quanto à conciliação do acesso e divulgação de documentos administrativos que contenham dados pessoais com o regime previsto no RGPD, a CNPD entende que o artigo 26.º da Proposta nada acrescenta desse ponto de vista, devendo por isso ser eliminado. De facto, ou se considera que as ressalvas do regime jurídico de proteção de dados pessoais expressas na lei de acesso aos documentos administrativos implicam a sujeição do acesso e das demais operações de tratamento de dados pessoais ao RGPD, caso em que o disposto no artigo 26.º não tem qualquer utilidade, ou se é forçado a concluir que a simples remissão para a lei de acesso aos documentos administrativos não cumpre os limites fixados no artigo 86.º do RGPD,

por nesse diploma legal não estarem concretizadas garantias essenciais da proteção dos dados.

Também o texto do artigo 27.º da Proposta de Lei deve ser revisto, para que se cumpra, como se julga ser a intenção, o princípio da minimização dos dados pessoais no âmbito da contratação pública.

Propõe-se ainda a revisão do n.º 4 do artigo 25.º, relativa à publicação de dados pessoais em jornais oficiais, pelo equívoco em que assenta quanto a conceitos técnicos, de modo a prevenir a contradição do previsto no artigo 17.º do RGPD.

vi. Sobre os tratamentos de dados nas relações laborais, a CNPD propõe a revisão do n.º 1 do artigo 28.º, para o tornar mais preciso, bem como da alínea *a)* do n.º 3, sob pena de se contradizer o RGPD quanto à relevância do consentimento.

Propõe ainda a eliminação do n.º 2 do mesmo artigo.

Quanto ao disposto nos n.ºs 7 e 8 do artigo 28.º, tal como se encontra redigidos, adverte para o risco que daí decorre de limitação de transferências para subcontratantes em violação do RGPD, quando os pressupostos neste previstos estejam preenchidos.

No que diz respeito ao tratamento de dados biométricos, previsto no n.º 6 do artigo 28.º. considera a CNPD ser imprescindível a definição legal do regime deste tratamento, porque a simples afirmação pela lei nacional da sua admissibilidade não garante a sua realização em conformidade com o RGPD. Recomenda-se ainda que se afaste a possibilidade de relacionamento deste tipo de sistemas de informação com outras tecnologias, como por exemplo a interconexão com sistemas de videovigilância.

vii. A CNPD assinala ainda a ausência no RGPD de fundamento direto de licitude dos tratamentos de dados de saúde no âmbito dos contratos de seguros e a necessidade de definição de um regime legal específico sobre esse tratamento, advertindo desde já que não é suficiente a mera previsão legal do tratamento.

7. No âmbito das disposições finais ou transitórias, além da eliminação do n.º 2 do artigo 61.º, entende a CNPD dever ser revisto o n.º 2 do artigo 62.º, na parte final, tendo em conta que o RGPD já está em vigor desde 2016.

A CNPD alerta ainda para a circunstância de o artigo 63.º não poder dispor sobre a revogação da LDPD, enquanto não for transposta a Diretiva (UE) 2016/680, relativa a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.

Finalmente, a CNPD recomenda a introdução de uma disposição no sentido de que todas as remissões para a LPDP se consideram feitas para o RGPD.

Lisboa, 2 de maio de 2018

Filipa Calvão (Presidente)