CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2025/26

I. PEDIDO

1. O Senhor Secretário de Estado da Presidência do Conselho de Ministros solicitou à Comissão Nacional de Proteção de Dados (CNPD) a emissão de parecer sobre o "Projeto de proposta de lei que autoriza o Governo a transpor a Diretiva (UE) 202212555, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União - PCM - (Reg. PL 298/XXIV 12024).".

2. O pedido formulado e o presente parecer enquadram-se nas atribuições e competências da CNPD, enquanto entidade administrativa independente com poderes de autoridade para o controlo dos tratamentos de dados pessoais, conferidos pela alínea c) do n.º 1 do artigo 57.º, conjugada com a alínea b) do n.º 3 do artigo 58.º e com o n.º 4 do artigo 36.º, todos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados - RGPD), em conjugação com o disposto no artigo 3.º, no n.º 2 do artigo 4.º e da alínea a) do n.º 1 do artigo 6.º, todos da Lei n.º 58/2019, de 8 de agosto, que executa na ordem jurídica interna o RGPD.

II. ANÁLISE

3. O presente pedido de pronúncia tem por objeto essencial a transposição da Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro, destinada a garantir um elevado nível comum de cibersegurança em toda a União Europeia.

4. Nesse mister, propõe-se, ainda, a execução na ordem jurídica interna das obrigações decorrentes do Regulamento (UE) 2019/881, do Parlamento Europeu e do Conselho, de 17 de abril, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança), implementando um quadro nacional de certificação da cibersegurança; nem como se procede à nona alteração da Lei de Segurança Interna, aprovada pela Lei n.º 53/2008, de 29 de agosto, alterada pela Lei n.º 59/2015, de 24 de junho, pelo Decreto-Lei n.º 49/2017, de 24 de maio, pelas Leis n.ºs 21/2019, de 25 de fevereiro e 73/2021, de 12 de novembro, pelo Decreto-Lei n.º 122/2021, de 30 de dezembro, pela Lei n.º 24/2022, de 16 de dezembro e pelos Decretos-Leis n.ºs 41/2023, de 2 de junho e n.º 99-A/2023, de 27 de outubro, à segunda alteração da Lei do Cibercrime, aprovada pela Lei n.º 109/2009, 15 de setembro, alterada pela Lei n.º 79/2021, de 24 de novembro e à também segunda alteração à Lei das Comunicações Eletrónicas, aprovada pela Lei n.º 16/2022, de 16 de agosto, alterada pelo Decreto-Lei n.º 114/2024, de 20 de dezembro.

A. CONSIDERAÇÕES GERAIS AO PROJETO.

5. A CNPD considera particularmente importante a atenção prestada à Diretiva proposta a transposição, partilhando a intenção inspiradora desse documento, no sentido de procurar assegurar salvaguardas em relação aos riscos de segurança que a digitalização vem convocando, bem como, na mesma seara, o reforço dos direitos fundamentais dos cidadãos que a eles se encontram expostos.

6. Nessa medida, as previsões constantes na Diretiva de reforço das medidas de segurança e avaliação desses riscos, bem como a sua supervisão e eficácia prática apresentam-se como elementos concretizadores positivos da tutela dos direitos fundamentais dos cidadãos, onde se encontra, também, o direito à proteção de dados pessoais, matriz fundamental que também a justifica.

7. O mesmo serve para dizer que as exigências de combate à ciberciminalidade e o reforço das medidas aumentadas de cibersegurança não poderão prescindir de ter como destinatário principal dos seus desideratos os direitos subjetivos dos cidadãos e a sua autodeterminação pessoal e informacional.

8. Daqui resulta, igualmente, que qualquer bloco legislativo que venha a ser ponderado nesta matéria não deverá perder de vista a legislação de proteção de dados pessoais que a antecede e que deverá ajudar a garantir, e não o inverso, *ie.*, que na prossecução unilateral ou sublinhada de certos fins securitários se possa, indiretamente, abafar ou obstar o que de certo modo o impulsionou, como seja, uma potencial limitação ou desrespeito ao direito à proteção de dados.

9. Deverá, pois, ser cuidado o labor legislativo na ponderação de equilíbrio entre valores, interesses e direitos, e qualquer limitação não poderá deixar de considerar o que sumamente se prescreve no artigo 52.º da Carta dos Direitos Fundamentais da União Europeia no tocante a eventuais restrições de direitos fundamentais, tendo presente que o direito à proteção dos dados pessoais se encontra previsto no artigo 8.º do mesmo Diploma.

10. Prescreve este artigo 52.º, no seu n.º 1, que *"1. Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros."*

11. Tem sido doutrina do Tribunal de Justiça da União Europeia (TJUE), na clarificação aplicativa da(s) norma(s) restritiva(s) que licitamente permita uma ingerência limitativa desses direitos, que a base legal que a preveja deverá definir claramente o âmbito dessa limitação, em confronto dialético, e ser suficientemente clara e precisa

nesse juízo de proporcionalidade estrita, especificando ela mesma o alcance da restrição ao exercício do direito garantido[1].

12. Para que tal possa ser reputado justificado na satisfação desse requisito, a legislação deverá não só recortar o âmbito e aplicação da restrição em causa, como, também, como reverso consequencial da restrição, estabelecer um conjunto de garantias nucleares, de modo a compartimentar imperativamente a abrangência da limitação, evitando assim possibilidades de abuso.

13. Na verdade, se a limitação é a exceção, nem por isso o direito se pode ver amputado geneticamente, pelo que haverá, dito douto modo, de operar-se uma delimitação positiva e negativa daquele, assim se conferindo a sua identidade especial, e se autorizando o juízo racional valorativo de *proportio*, a ratear através desses elementos.

14. Ainda nesta linha, não deverá qualquer diploma sobre esta matéria afetar a aplicação das regras previstas no RGPD e demais legislação de proteção de dados, com quem deve dialogar, bem como deverá ser garantido o respeito pelos poderes e atribuições das autoridades de controlo sobre essas matérias, procurando uma desejável e harmónica cooperação, com espaços claros de ocupação, no sentido de, a fim, partilhar o que é um propósito comum[2]. Felicita-se, neste ponto, o cuidado legislativo de prever no artigo 1.º do Regime Jurídico da Cibersegurança, nas alíneas c) e d), a aplicabilidade da legislação de proteção de dados pessoais de forma expressa.

15. A comunhão a que se alude pode ser lida, desde logo, observando o disposto no artigo 5.º n.º 1 do RGPD, que ergue a segurança como um dos princípios essenciais relativos ao tratamento de dados, e que vem confirmada no artigo 32.º do RGPD, que melhor o desenvolve, demonstrando a importância de que as prossecuções relativas à cibersegurança se ergam a essenciais aos direitos e garantias dos cidadãos, à sua reserva e informação pessoal, bem como à sua privacidade[3].

---

[1] Veja-se, a propósito o Acórdão do TJUE, C-419/14, parágrafo 81.

[2] No Considerando 14 da Diretiva pode ler-se, impressivamente, que: "O direito da União em matéria de proteção de dados e o direito da União em matéria de privacidade são aplicáveis a qualquer tratamento de dados pessoais realizado ao abrigo da presente diretiva. Em especial, a presente diretiva não prejudica o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (8) e a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho (9). Por conseguinte, a presente diretiva não deverá afetar, nomeadamente, as funções e os poderes das autoridades competentes para controlar o cumprimento do direito da União em matéria de proteção de dados e do direito da União em matéria de privacidade aplicáveis."

[3] Veja-se, a propósito o conteúdo do considerando 143 da Diretiva: A presente diretiva respeita os direitos fundamentais e observa os princípios reconhecidos na Carta, nomeadamente o direito ao respeito pela vida privada e pelo caráter privado das comunicações, o direito à proteção de dados pessoais, a liberdade de empresa, o direito de propriedade, o direito à ação e a um tribunal imparcial, a presunção de inocência e os direitos de defesa. O direito a um recurso efetivo estende-se aos destinatários dos serviços prestados por entidades essenciais e importantes. A presente diretiva deverá ser aplicada de acordo com esses direitos e princípios.

16. É, pois, a esta luz que serão analisados os pontos referente a proteção de dados desta Proposta de Lei, partindo, por conseguinte, do pressuposto estruturante da Diretiva da sua plena efetividade, e que as questões relacionadas com a cibersegurança só poderão obter resposta satisfatória numa escolha de regime que as confirme e garanta, apenas se justificando qualquer restrição na medida em que funcionalmente as melhor possa servir, nomeadamente observando princípios estritos de necessidade e proporcionalidade, em respeito aos núcleos fundamentais do direitos pessoais, que são os seus conceitos chave autorizantes.

17. Isto considerando,

B. ANÁLISE NA ESPECIALIDADE: QUANTO AO ARTIGO 10.º DA PROPOSTA.

18. Sob epígrafe "Tratamento de dados pessoais", este artigo assim dispõe:

"Artigo 10.º

Tratamento de dados pessoais

1 - As entidades que integram o quadro institucional da segurança do ciberespaço, nos termos do artigo 15.º, tratam dados pessoais na medida do estritamente necessário para assegurar o cumprimento de obrigações legais e a prossecução de missões de interesse público ou de autoridade pública em que estão investidos, nos termos do disposto nas alíneas c) ou e) do n.º 1 e no n.º 3 do artigo 6.º do RGPD e em conformidade com o presente decreto-lei e demais legislação nacional aplicável.

2 - As entidades que integram o quadro institucional da segurança do ciberespaço podem ainda tratar dados pessoais para a prossecução de um interesse legítimo das entidades essenciais e importantes, tal como referido na alínea f), n.º 1 do artigo 6.º do RGPD.

3 - Sem prejuízo do disposto no artigo 29.º da Lei n.º 58/2019, de 8 de agosto, as entidades que integram o quadro institucional da segurança do ciberespaço podem proceder ao tratamento de categorias especiais de dados pessoais para, na medida do estritamente necessário:

4 - Evitar a consumação de uma ciberameaça significativa para a segurança das redes e sistemas de informação;

5 - *Responder eficazmente a um incidente de cibersegurança ".*

19. A remissão realizada para o artigo 15.º especifica quais as entidades que preenchem o plural quadro institucional da segurança do ciberespaço, a saber, o CSSC (na qualidade de órgão consultivo do Primeiro-Ministro no domínio da cibersegurança), o CNSC, (*inter alia*, na qualidade de autoridade nacional de

cibersegurança e de certificação de cibersegurança), assim como, na qualidade de autoridades nacionais setoriais ou especiais de cibersegurança, o GNS, a ANACOM, a ASF, a CMVM, o Banco de Portugal, a Comissão de Avaliação de Segurança no Ciberespaço, a Polícia Judiciária, o SIS, o Serviço de Informações Estratégicas de Defesa e o Comando de Operações de Ciberdefesa.

20. À luz do que se deixou expendido na parte A., *supra*, o inciso indicativo ou declarativo feito constar no número do artigo em análise afigura-se, a ver da CNPD, como insuficiente face à legislação de proteção de dados pessoais.

21. Como vem sendo afirmado por esta Comissão, a mera inclusão de cláusula genérica sobre cumprimento da legislação pertinente ou a mera referência ao tratamento de dados ou ao cumprimento das regras em vigor não se afigura capaz de preencher ou satisfazer os ditames – imperativos - que a matéria de proteção de dados reclama.

22. Não se ignora que, considerando o objeto essencial do projeto *sub iudice* e das atividades que se visam impor, haverá lugar a tratamento de dados pessoais e, eventualmente, a adequações mais ou menos evidentes com outros interesses em juízo.

23. Mas cumpre recordar que assumindo a dimensão jurídica de direitos fundamentais, os dados pessoais e sua proteção formam parte cimeira desse património nuclear de direitos e liberdades na qual assenta a vivência de uma sociedade democrática, com as consequências que tal dignidade reclama, enquanto uma das suas manifestações.

24. Como matéria jusfundamental, a proteção de dados pessoais goza, também, da consagração de um conjunto de princípios próprios, que emergem na dependência axiológica daquele núcleo essencial, no sentido de lhes confirmar eficiência, e impõe-se de forma juridicamente vinculativa, e diretamente, a todos os Estados-Membros, como é o caso, desde logo, do RGPD e suas normas.

25. Tal servirá para dizer que, quando o Legislador declara que os núcleos conformadores e as condições executantes das normas que pretende construir cumprirão a matéria prevista no RGPD e sua Lei de Execução, nada está a acrescentar para além do natural pressuposto do seu exercício legislativo, já que, sob pena de ilicitude, outra solução não poderia conceber-se.

26. Daqui decorrerá que, quando o Legislador se encontre perante regulação que implique o tratamento de dados pessoais, a obrigação que sobre si impende será a de, perante o caso ou tratamento(s) concreto(s) que vêm implicados, estabelecer o regime particular das suas condições que, por um lado, demandam a concretização das regras previstas nos diplomas imperativos que os regulam, e que, por outro lado, consistam na

consubstanciação ou subsunção do regime de proteção previsto na Constituição da República Portuguesa e na Legislação Europeia e nacional que enformam essa matéria.

27. Apenas se desenhando os sujeitos, fundamentos, fins e o *modus* como os tratamentos serão executados e operacionalizados, em específico, é que se permitirá concluir que são cumpridas aquelas determinações e princípios, o que terá de decorrer de um juízo valorativo de cada tratamento proposto, ponderação essa que, natural e logicamente, decorrem da prévia ontologia e desenho do tratamento que, depois, merecerá -ou não- essa adequada qualificação.

28. Se nenhum dos termos do tratamento estiver definido, nada se poderá concluir, nem nenhum juízo de proporcionalidade poderá ser concretizado.

29. Dever-se-á, portanto, de cada vez que um específico tratamento de dados pessoais seja previsto por emanar de conteúdos normativos, regular-se, nesse mesmo documento, e com pelo menos a mesma dignidade, os imperativos concretos capazes de enformar os respetivos tratamentos em causa e que concretizam esses mesmos princípios e seu regime.

30. O regime concreto de tratamento de dados, tudo convocando, não é aspeto subsidiário ou secundário ou meramente prático, antes sendo onde esses direitos fundamentais se realizam e se endereçam aos cidadãos.

31. Na sua ausência, não é, pois, possível a esta Comissão pronunciar-se sobre o seu valor ou desvalor, o que sacrifica as atribuições, intenções e fins do Legislador quando prevê o parecer prévio deste tipo de matérias a esta autoridade, o que não é desejável.

32. Isto posto, deve evitar-se a vaga alusão a tratamentos de dados pessoais *"(…) na medida do estritamente necessário para assegurar o cumprimento de obrigações legais e a prossecução de missões de interesse público ou de autoridade pública em que estão investidos (…)",* uma vez que queda verdadeiramente indefinido que dados se pretendem tratar, o que justifica aquele tratamento em particular, para que fins e em que termos[4], elementos imprescindíveis ao enunciado um harmónico de necessidade e proporcionalidade que o Legislador diz pretender.

33. Em geral, sempre que perante um tratamento de dados chamado a cumprir o RGPD, haverá de se particularizar, também, o período de conservação dos dados, a sua eliminação, e a ontologia de dados e registos

[4] Repare-se que a noção de dados pessoais definida no RGPD é amplíssima, e nem todos os elementos caracterizadores são suscetíveis de significar os mesmos graus de intrusão: Entende-se por dados pessoais "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou *social dessa pessoa singular."*

a ser concebida e sua eventual forma de partilha, nomeadamente as medidas técnicas e organizativas a deverem ser aplicadas aos tratamentos[5], que também constituem aspetos materiais inafastáveis na proteção de dados.

34. A ausência destes elementos conformadores impossibilita qualquer avaliação propedêutica de garantia dos direitos dos cidadãos, constituindo omissões a reparar, desde logo na concretização do princípio da menor intrusão na esfera dos titulares dos dados.

35. Não é indiferente, também, o fundamento de licitude de que se pretende lançar mão em vista a esses tratamentos, *i.e.*, *"…nos termos do disposto nas alíneas c) ou e) do n.º 1 e no n.º 3 do artigo 6.º do RGPD"*.

36. Para que um tratamento de dados pessoais possa ocorrer licitamente, este terá de encontrar estribo em alguma das enunciações taxativas previstas no artigo 6.º n.º 1 do RGPD: "*a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.*"

37. Ainda que o Legislador Europeu se tenha expressado pela possibilidade cumulativa de fundamentos, estes não têm a mesma natureza e, bem assim, partilham os mesmos efeitos, nem sempre comungando, pela sua razão de ser, as mesmas exigências.

38. A alínea c) remete para a necessidade de certo tratamento em vista *ao cumprimento de uma obrigação legal a que o responsável pelo tratamento esteja sujeito.* Nos termos do número 3 do mesmo artigo, acrescenta-se, ainda, que a obrigação a que se alude haverá de decorrer do direito da União, ou do direito do Estado-Membro.

39. Tal inciso dirige-se, no essencial, aos responsáveis pelo tratamento, e na medida em que, enquanto tal, sejam destinatários diretos de comandos normativos imperativos que, em vista à necessidade de lhes darem cumprimento, se vejam, nessa mesma medida, na obrigação de proceder ao tratamento de dados pessoais com

[5] Sobre esta matéria, pode ver-se a Diretriz 2023/1 desta Comissão.

cabimento nesse comando[6], não constituindo, por isso, numa interpretação amplíssima, uma base autorizante à promoção de tratamentos de dados próprios[7].

40. Ainda que se admita que, em essência, este fundamento não afaste os intervenientes públicos, inexiste no projeto razão que permita concluir pela sua necessidade ou aferir desse juízo.

41. Coisa diferente, todavia, é o fundamento assente no previsto na alínea e) daquele artigo 6.º, na medida em que ali se prevê: *e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento.*

42. Ao contrário do previsto na alínea c), neste caso, o fundamento não resultará de obrigações legais específicas que incidam sobre o responsável pelo tratamento, mas antes assenta numa *causa/*autorização necessária ao cumprimento de certas atribuições ou competências atribuídas por Lei a certo Ente, em vista a prossecução de tarefas de interesse público e de *publica potestas em* que está investido, devendo, em contrapartida, ser identificado claramente o interesse público em jogo e a autoridade pública particular que branda o fundamento, e quais as prossecuções, com esses tratamentos, que esta procura servir.

43. Também aqui, o RGPD mantém a exigência de que o fundamento esteja definido pelo direito da União ou pelo direito do Estado-Membro, mas vai mais longe, como contraponto da mais ampla autorização: *"no que respeita ao tratamento referido no n.º1, alínea e), deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento."*

44. Este fundamento deve ainda, impressivamente, *"(…)prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas relativas a outras situações específicas de tratamento em conformidade com o capítulo IX. O direito da União ou do Estado-Membro deve responder a um objetivo de interesse público e ser proporcional ao objetivo legítimo prosseguido."*

45. Do que se é capaz de retirar da proposta, tais elementos parecem encontrar-se, também, omissos.

[6] Veja-se o caso, por exemplo, da obrigatoriedade de certas instituições de denunciar transações suspeitas ao abrigo da legislação contra o branqueamento de capitais, ou o cumprimento de normas de direito laboral, por parte das entidades empregadoras.

[7] Que só poderia assentar numa conceção de que todos, de certa forma, somos destinatários de obrigações legais, em maior ou menor medida, o que diluiria completamente a utilidade e eficácia do fundamento em sede hermenêutica de proteção de dados pessoais.

46. Do quadro institucional da segurança do ciberespaço e respetivas atribuições, parece declarar-se na Proposta, também, o acolhimento mormente no fundamento acabado de analisar, devendo, porém, procurar clarificar-se este importante ponto, em confronto com o que se deixou supra quanto ao outro fundamento também invocado, uma vez que, como se tentou demonstrar, não são intercambiáveis e acarretam configurações distintas.

47. É que, como se disse, não só o fundamento do tratamento se afigura determinante para aferir o tratamento lícito, como, também, exige o regime próprio que o haverá de praticar e, até, recortes específicos no tocante aos direitos dos titulares dos dados (veja-se, a propósito, o prescrito no artigo 21.º, sob epígrafe direito de oposição).

48. Resulta ainda deste correr que parece existir confusão entre o constante no número 1 do artigo 10.º do Projeto e o seu número 2, onde se afirma que *"2 - As entidades que integram o quadro institucional da segurança do ciberespaço podem ainda tratar dados pessoais para a prossecução de um interesse legítimo das entidades essenciais e importantes, tal como referido na alínea f), n.º 1 do artigo 6.º do RGPD.*

49. Sobre este ponto, ainda que se admita menos feliz a tradução portuguesa do RGPD deste preceito, o artigo 6.º n.º 1 *in fine* não permite grandes dificuldades interpretativas, afastando essa solução quando perante tratamentos de dados efetuados por autoridades públicas na prossecução das suas atribuições e competências, dirigindo-o apenas a responsáveis pelo tratamento do setor privado: *"O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica*[8]*,."*

50. O n.º 3 do mesmo artigo prescreve, ainda, *que "Sem prejuízo do disposto no artigo 29.º da Lei n.º 58/2019, de 8 de agosto, as entidades que integram o quadro institucional da segurança do ciberespaço podem proceder ao tratamento de categorias especiais de dados pessoais para, na medida do estritamente necessário: a) Evitar a consumação de uma ciberameaça significativa para a segurança das redes e sistemas de informação; b) Responder eficazmente a um incidente de cibersegurança. "*

51. Não obstante o endereçamento ao regime previsto na Lei n.º 58/2019 no tocante aos "Tratamentos de dados de saúde e dados genéticos", este inciso pretende erigir permissão genérica para o tratamento de categorias especiais de dados por parte das Entidades que integram o quadro institucional da segurança do ciberespaço, preenchendo, destarte, aquelas categorias de dados sujeitos a uma especial proteção pelo Legislador Europeu, acolhidos no artigo 9.º do RGPD.

[8] Na versão inglesa, mais claramente: "Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."

52. Deverá ter-se presente o tratamento de tais dados é, em regra, proibido, apenas podendo ser realizado no espartilhado conjunto de exceções previstas no n.º 2 e 3.º daquele artigo.

53. Daqui resulta que "*1 - É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.*"

54. Da Proposta em análise desconhece-se, desde logo, a que categorias especiais de dados pretende o Legislador fazer referência. Se é verdade que pela referida remissão à Lei n.º 58/2018 se dirige aos ditames que dizem respeito a dados de saúde ou genéticos, a proibição ou restrição do Legislador Europeu é mais ampla e, considerando as exigências de juízo de proporcionalidade ou concordância prática a realizar em concreto e em função dos fins, essas categorias não são, também, idênticas. Poder-se-á reputar, por exemplo e em abstrato, existir *necessidade* de alguma ou alguma dessas categorias, e não necessariamente doutras.

55. Rematando, se um tratamento de dados genericamente exige que se determinam quais os dados a tratar, a avaliar na estrita medida dos fins de que são serventia, só assim de admitindo uma restrição à sua subjetividade fundamental, por maioria de razão estes requisitos e juízos deverão ser ainda mais exigentes quando perante dados especialmente protegidos que, pela sua natureza, exigirão cuidados adicionais.

56. Ademais, como se já notou, apenas podem ser tratados quando caibam numa das circunstâncias taxativas previstas nos números 2 e 3 daquela parcela legislativa.

57. Compulsadas as razões ali expostas, não é evidente o acolhimento numa dessas causas excecionais.

58. Convirá, a este propósito, deixar algumas observações, que se conjugam, *mutatis mutandis*, com o que já se referiu aquando da análise sobre o fundamento de licitude do tratamento dos dados pessoais pelas entidades indicadas, nomeadamente o previsto no artigo 6.º, n.º 1, alínea e) do RGPD.

59. O artigo 9.º n.º 2, alínea g) declara que uma exceção à proibição poderá ocorrer *"g) Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;"*

60. O tratamento deverá, assim, nesses casos, ser proporcional ao objetivo visado, objetivo esse que consistirá em interesse público importante, respeitando ainda o direito à autodeterminação, e terá, sempre, de ser

acompanhado de "medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses dos titulares dos dados".

61. Ainda que pareça existir uma sobreposição ao tratamento de dados pessoais assente no artigo 6.º n.º 1, alínea e), na medida em que este último também regula um tratamento assente em interesse público, não é indiferente o acrescento do adjetivo "importante".

62. Face à especial proteção dos dados abrangidos pelo artigo 9.º, apenas os interesse públicos considerados de particular importância podem cair no âmbito desta norma. Tal reflete, na verdade, a natureza particular dos dados em causa, face aos riscos – maiores – associados ao seu tratamento, cuja intrusão é igualmente reforçada na Legislação Constitucional nacional.

63. Não bastará, assim, alegar que um tratamento de dados sensíveis é necessário ao exercício de interesses públicos, ou declarar a sua eficácia ou utilidade de facto – haverá antes de mais, que bem recortar qual o interesse público em causa, capaz de consubstanciar um interesse especialmente importante e, também, que demonstrar, clara e evidentemente, a importância e dignidade desse excecional tratamento, e a sua imprescindibilidade para a prossecução desses interesses.

64. Tal exigirá, como também se já lavrou aqui, quer uma delimitação positiva (os benefícios desse tratamento em função do importante interesse), quer negativa (as consequências sacrificiais desse interesse, pelo seu não tratamento), bem como uma perspetiva quantitativa face aos sujeitos potencialmente afetados, expressando-se o juízo de proporcionalidade que o Legislador realizou, nas circunstâncias concretas, específicas, para que prevê cedência.

65. O Legislador deverá, ainda, prever medidas adequadas de salvaguarda dos direitos fundamentais e dos interesses dos titulares dos dados, a aferir em concreto, definindo o seu conjunto de direitos, seja em sede informacional, seja em sede da garantia do seu exercício e, bem assim, do controlo, conhecimento e domínio que sobre eles devem ter, afastando-se qualquer possibilidade de tratamentos "ocultos".

66. Em súmula, deve, como se disse, ser respeitada a essência do direito a restringir ou limitar, não se podendo diluir à imperceção a ligação ontológica entre o direito e o seu titular, ou autorizar em branco tratamentos de todos os dados que lhes pertençam, a escolher indefinida e discricionariamente por quem os pretenda tratar, como ocorre na circunstância, presente, de não se definirem as categorias de dados sensíveis a tratar – não é essa a intencionalidade prática prevista no regime europeu e nacional respeitante à proteção de dados pessoais.

67. Acrescerá, ainda, uma especificação do regime a adotar nesses tratamentos, atentando às exigências previstas no RGPD, desde logo no que toca ao prazo de conservação dos dados.

68. Em conclusão, sugere-se a clarificação de cumprimento destes requisitos, em conjugação – por relação direta -, com o que supra se já expendeu.

C. QUANTO AO CONSTANTE NOS ARTIGOS 23.º E 79.º DA PROPOSTA.

69. O artigo 23.º do documento em juízo, sob epígrafe "Cooperação entre autoridades nacionais" refere que *"O CNCS, o Secretário-Geral do Sistema de Segurança Interna e as autoridades nacionais setoriais de cibersegurança, no exercício das suas atribuições e competências ao abrigo do presente decreto-lei, atuam em cooperação estreita com: a) A Comissão Nacional de Proteção de Dados, sempre que estejam em causa incidentes que tenham dado origem à violação de dados pessoais, nos termos do artigo 79.º;"*

70. No seu número 7, fez-se constar que *"As autoridades referidas neste artigo devem responder aos pedidos de informação no prazo de 5 dias após a data em que as informações tiverem sido solicitadas, salvo motivo devidamente justificado. "*

71. O indicado artigo 79.º, sob o título "Violação de dados pessoais" apresenta o seguinte conteúdo *"1 - Sempre que a autoridade de cibersegurança competente obtiver um grau razoável de certeza, no decurso de uma ação de supervisão ou da imposição de medida de execução, de que a infração das obrigações estabelecidas nos artigos 27.º a 29.º e dos artigos 40.º a 43.º por parte de uma entidade essencial ou importante pode implicar uma violação de dados pessoais, nos termos do artigo 4.º, ponto 12, do RGPD, a qual deve ser notificada nos termos do artigo 33.º do mesmo RGPD, aquela autoridade deve, sem demora injustificada, informar a CNPD. 2 - No caso de a CNPD aplicar uma coima, nos termos do artigo 58.º, n.º 2, alínea i) do RGPD e restante direito nacional aplicável, a autoridade competente fica impedida de aplicar uma coima em resultado da prática da mesma infração nos termos do presente decreto-lei, sem prejuízo do disposto no número seguinte. 3- A autoridade de cibersegurança competente pode impor as medidas de execução, previstas no artigo 56.º, n.º 1, alíneas a) a h), às entidades essenciais e importantes cuja violação das obrigações decorrentes do presente decreto-lei resulte num incidente de violação de dados pessoais. "*

72. Deixou-se, no capítulo preliminar deste documento, um conjunto de considerações que importará ora recuperar, como seja, o facto da matéria de cibersegurança e de proteção de dados pessoais deverem apresentar fins comuns, bem como a aplicabilidade desejavelmente harmónica dos seus ditames a favor desses fins, reservando-se, para tanto, as competências e atribuições das autoridades de controlo de proteção de dados intactos, tudo como resulta, desde logo, da Diretiva a executar.

CNPD
Comissão Nacional
de Proteção de Dados

73. Em vista a tais desideratos, o RGPD atribui um conjunto alargado de competências exclusivas às autoridades de proteção de dados pessoais – no caso português a CNPD -, nomeadamente nos seus artigos 56.º a 58.º do RGPD, bem como na demais legislação nacional relacionada com a proteção de dados pessoais, seja por via da sua Lei de Execução, seja nos diplomas avulsos que suscitam matéria relacionada com dados pessoais.

74. Um dos objetos onde se prescreve regime particular e se desenha a competência concreta desta Comissão é, precisamente, o relacionado com as violações de dados pessoais – *e .g.*, veja-se o previsto nos artigos 32.º a 34.º do RGPD, e o respetivo regime sancionatório previsto nos artigos 83.º e 84.º do mesmo Diploma, bem como os incisos que preenchem os artigos 37.º a 45.º da Lei n.º 58/2019.

75. Partindo do pressuposto da reserva total das competências desta Comissão quanto à proteção de dados pessoais como, de resto, parecer inspirar da Diretiva, crê-se que a harmonização respeitante, ora ao dever de colaboração, ora às esferas de intervenção de cada ator público deverá também ser clarificada, sob pena de sobreposições competenciais indesejáveis, ou de difíceis diálogos que possam comprometer a eficácia do escopo essencial de ambas os campos, potencialmente sacrificando, a final, o que se procura reforçar.

76. Desde logo, se se atentar à exegese do artigo 23.º da Proposta, parece endereçar-se a "cooperação estreita" com a CNPD apenas nos casos em que estejam em causa "violação de dados pessoais", o que parece constituir um universo reduzido se se reputar as questões que podem ser levantadas na prossecução de fins de cibersegurança. Veja-se, em articulação, sempre a julgar em concreto, dos já endereçados princípios plasmados no artigo 5.º do RGPD, o conjunto de direitos dos artigos 12.º a 23.º, as competências e atribuições desta Autoridade e os trâmites processuais a encetar, e os regimes preventivos e/ou sancionatórios a levar à sua efetivação.

77. Seria desejável estabelecer-se regime concreto de como se haverá de proceder a essa cooperação, atentos, ademais, os princípios de legalidade e competências dos Entes Públicos, bem como o *due process* que daí possa resultar e que se afigura como elemento essencial na referência ao conjunto garantístico dos atores envolvidos, seja na perspetiva dos atos suscetíveis de serem praticados, seja no respeito pelos direitos dos cidadãos.

78. Depois, se é verdade, que o artigo 8.º da Lei n.º 58/2019 refere um "dever de colaboração" – que resulta, também, da hermenêutica geral da natureza e funções desta Comissão -, essa prerrogativa endereça-se em sentido contrário, *i.e.*, que as outras Entidades, públicas ou privadas, devam cooperar com a CNPD em vista à prossecução das tarefas, muitas exclusivas, que a Lei lhe impõe.

79. Parece proceder-se, na Proposta, a uma relativa inversão, na medida em que, ainda que se reconheça a competência em sede de violação de dados à CNPD, se exige, no 23.º, n.º 7, que esta responda a solicitações das autoridades de cibersegurança no prazo de 5 dias. Ademais, se se ler este inciso em conjugação com o

previsto no artigo 79.º nº 1 e do dever de notificação que aí se encontra ínsito, pode concluir-se por poder existir contradição, devendo, pois, procurar clarificar-se quais as entidades sobre quem recai esse dever

80. O que se pretenderá criar, aparentemente, será um novo mecanismo de comunicação de violação de dados pessoais, por via do conhecimento da autoridade de cibersegurança competente, regime que não se afigura reprodutivo do previsto no artigo 33.º do RGPD, pelo que se exigiria a sua -também nova - representação.

81. Se, repita-se, se entende que se pretende uma conjugação das esferas de cada uma das autoridades, deverá o Legislador cuidar de estabelecer, com cautela, qual o regime objetivo e subjetivo a empreender *in casu*, em harmonização adjetiva e substantiva que pertencem à esfera dos intervenientes.

82. Note-se, ainda neste devir, o que vêm prescrito no artigo 79.º nºs 2 e 3 da Proposta*: "2- No caso de a CNPD aplicar uma coima, nos termos do artigo 58.º, n.º 2, alínea i) do RGPD e restante direito nacional aplicável, a autoridade de cibersegurança competente fica impedida de aplicar uma coima em resultado da prática da mesma infração nos termos do presente decreto-lei, sem prejuízo do disposto no número seguinte. 3- A autoridade de cibersegurança competente pode impor as medidas de execução, previstas no artigo 56.º, n.º 1, alíneas a) a h), às entidades essenciais e importantes cuja violação das obrigações decorrentes do presente decreto-lei resulte num incidente de violação de dados pessoais."*

83. Se o Legislador excecionou a possibilidade de *ne bis in idem,* as observações que se acabaram de deixar também encontram aqui reflexo.

84. Isto é, da arquitetura que se forjou deste artigo, face a explanada competência da CNPD, não parece evitar-se que possam existir processos simultâneos ou concorrenciais, suscetíveis de conduzir a destinos diferentes, ou que na sua apreciação não exista comunicabilidade ou comunhão de factos, antes se centrando naquilo que, a final, pode ou não constituir uma decisão autónoma da Autoridade de proteção de dados, mas que, na verdade, poderá partir de diferentes factos constitutivos ou mecanismos processuais diversos ou, até, divergentes – as devidas sanções haverão de resultar da subsunção de certos factos a normas, racionalmente fundada; em respeito pelos princípios derivantes do processo equitativo, as sanções não consubstanciam um "ato" em si próprio ou por si só, que permitam justificar ou consumir certos factos concretos, desligadas dos juízos e direitos que as fundamentam.

85. Rematando, deverá reputar-se o estabelecimento de uma base legal compreensiva onde se preveja a cooperação e troca de informação relevante, mais do que um relativo ou unilateral "dever de cooperação", ainda mais se se partilhar a ideia de que, nestas matérias, a proteção de dados pessoais poderá intervir de forma mais ampla do que os casos de violação de dados.

86. De resto, a autoridade de cibersegurança parecer reservar para si, ainda, assim, a possibilidade de imposição das medidas de execução previstas no artigo 56.º n.º1 alínea a) a h) da Proposta, que assim diz: "*a) Advertências sobre infrações dos deveres decorrentes do presente decreto-lei e do respetivo regime regulamentar aplicável; b) Ordens ou instruções vinculativas com vista à adoção de medidas necessárias para prevenir, impedir ou corrigir um incidente, determinando os prazos para a sua execução e respetiva informação; c) Ordens ou instruções vinculativas com vista à correção de deficiências ou infrações ao presente decreto-lei; d) Ordens ou instruções vinculativas com vista ao cumprimento do disposto no artigo 26.º e seguintes ou, quando se trate de uma entidade pública do disposto no artigo 33.º, ou ainda com vista ao cumprimento do disposto nos artigos 40.º e seguintes; e) Ordens para que as entidades em causa informem as pessoas singulares ou coletivas a quem prestam serviços ou que realizam atividades potencialmente afetadas por ciberameaça significativa da natureza desta, bem como de quaisquer medidas de proteção ou corretivas que possam ser adotadas em resposta a essa ciberameaça; f) Ordens para que a entidade em causa aplique, num prazo razoável, as recomendações formuladas em resultado de uma auditoria de segurança; g) Designação de um supervisor com funções adequadamente circunscritas, durante um período limitado, para supervisionar o cumprimento das obrigações previstas nos artigos 26.º e seguintes, e previstas nos artigos 40.º e seguintes, pela entidade em causa; h) Ordens para que entidade em causa publicite os aspetos das infrações ao presente decreto-lei de uma forma específica; "*

87. Com isto também se quer dizer que alguns dos elementos aí constantes constituem não só competências que esta Comissão pode dispor no âmbito de violação de dados pessoais, como, também, são elementos que podem ser determinantes para considerar se deverá ou não aplicar-se a certo agente uma coima, já que as violações de dados assentam, também, num conceito amplo de violação de regras de segurança e das medidas que possam ou não ter sido implementadas pelo responsável, em sede de proteção de dados pessoais.

88. Em conclusão, também aqui crê esta Comissão que estes aspetos devem ser repensados numa perspetiva sistemática, e clarificadas as coordenações interinstitucionais e orgânico-processuais capazes de levar à prática a intenção legislativa, o que reforça o que se disse quanto à proximidade das diferentes ações e disciplinas, que impõe, como reverso, cuidados acrescidos.

D. DA FALTA DE UM ESTUDO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS PESSOAIS

88. Finalmente, não poderá deixar-se de sublinhar, ainda, que a Proposta *sub iudice* não se encontra suportada num estudo de impacto sobre a proteção de dados pessoais o qual é, recorda-se, obrigatório nos termos nos termos conjugados dos artigos 18.º, n.º 4, da Lei n.º 43/2004, 7.º da Lei n.º 58/2019, e 35.º do RGPD.

89. Tal omissão também compromete uma avaliação segura e fundamentada em concreto quanto aos prováveis riscos decorrentes dos tratamentos de dados pessoais a realizar e, sobretudo, poderá prejudicará a decisão ponderada dos titulares do poder político-legislativo numa matéria em que a compreensão de tais riscos é essencial para concluir, no plano normo-material, quanto à concreta admissibilidade e condições de execução dos tratamentos de dados, especialmente nesta área da cibersegurança, avaliação que será também suscetível de ser enquadrada, por outra via e face a essa natureza, na eventual necessidade de avaliação de impacto prevista no artigo 35.º do RGPD.

III. CONCLUSÃO

91. Nos termos e com os fundamentos expostos a CNPD recomenda:

a) Reponderar o(s) fundamento(s) de licitude erigidos no artigo 10.º da Proposta, considerando o vertido nos pontos 32. a 47., todos deste documento, estabelecendo, consequentemente, o regime concreto que esse imponha, nos termos feitos constar nos pontos 20. a 31.;
b) Por conseguinte, eliminar o incisivo referente ao fundamento de licitude de tratamento com base no "interesse legítimo", conforme o exposto nos pontos 48. e 49.;
c) Repensar e/ou densificar, em relação com a) e sob pena de ilicitude, o tratamento de "categorias especiais de dados", conforme indicado nos pontos 50. a 68.;
d) Estabelecer regime concreto de harmonização legislativa, processual e de cooperação entre a autoridade de cibersegurança e a CNPD, em função das suas naturezas, atribuições e competências, como analisado no título "C".;
e) A realização de avaliação de impacto dados pessoais, seja por via da obrigatoriedade prevista nos termos conjugados dos artigos 18.º, n.º 4 da Lei 43/2004, 7.º da Lei 58/2019 e, atenta a natureza da matéria em causa, nos termos do artigo 35.º do RGPD.;

Lisboa, 27 de fevereiro de 2025

Assinado por: **JOSÉ CARLOS VEGAR ALVES VELHO**
Data: 2025.02.27 19:39:26+00'00'

José Vegar Velho (Vogal)