CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2021/52

I. Pedido

1. O 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 Decreto-Lei que «*regulamenta o regime jurídico da segurança do ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019*».

2. A CNPD emite parecer no âmbito das suas atribuições e competências enquanto autoridade 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, a alínea *b)* do n.º 3 do artigo 58.º e n.º 4 do artigo 36.º, todos do Regulamento (UE) 2016/679, de 27 de abril de 2016 – Regulamento Geral sobre a Proteção de Dados (doravante RGPD), em conjugação com o disposto no artigo 3.º, no n.º 2 do artigo 4.º e na 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. A Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, transpondo para o ordenamento jurídico nacional a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, remete para legislação complementar a definição dos requisitos de segurança das redes e sistemas de informação, bem como das regras de definição de incidentes. O presente Projeto de Decreto-Lei pretende regulamentar o referido regime, integrando ainda as disposições relativas à execução no mesmo ordenamento das obrigações em matéria de certificação da cibersegurança previstas no Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019.

4. Uma vez que o regime jurídico de proteção de dados contém algumas normas cuja *ratio* é comum ao regime jurídico da cibersegurança e, sobretudo, que têm em comum as entidades destinatárias, a perspetiva da CNPD, ao emitir o presente parecer, é a de que o presente Projeto deve procurar respeitar uma certa harmonização concetual para facilitar a aplicação pelas entidades daqueles regimes e corrigir algumas das dificuldades que a sua aplicação articulada tem suscitado. Quanto a este último ponto, a CNPD procurará aqui deixar alguns contributos gizados na sequência da sua experiência no âmbito de incidentes de segurança que afetam dados pessoais.

5. Assim, a CNPD começa por salientar que, entre as diferentes obrigações impostas pelo Projeto às entidades sujeitas ao regime da cibersegurança, importa ponderar a adoção de medidas no plano organizativo e relativas

aos recursos humanos. Na verdade, demonstrando a experiência que parte dos incidentes de segurança resultam de erro humano ou falha de organização, a CNPD recomenda que:

i. No artigo 7.º se especifique, além dos elementos aí elencados, que o plano de segurança integre também a descrição das medidas organizativas e, em particular, de formação dos recursos humanos;

ii. Na alínea *a)* do n.º 1 do artigo 8.º, se acrescente a descrição sumária de atividades de formação dos recursos humanos sobre as questões de segurança das redes e sistemas de informação.

6. No que diz respeito à análise de riscos, a experiência tem revelado ser importante que esta análise não seja compartimentada, antes abrangendo a rede e a totalidade do sistema de informação e, portanto, considerando todas as suas implicações também quanto aos dados pessoais. Assim, para prevenir uma visão parcelar dos riscos e a desconsideração das consequências sobre as pessoas a quem diz respeito a informação da introdução de medidas mitigadoras de certo risco, a CNPD recomenda que no artigo 10.º do Projeto, eventualmente, no n.º 2, se exija expressamente que a obrigação de realizar a análise dos riscos e de documentação dessa análise reflita uma visão de conjunto dos riscos.

7. Ainda no âmbito do mesmo artigo 10.º, não se alcança a razão por que, entre os fatores a considerar na análise dos riscos, não estão elencados outros fatores que não podem deixar de ser determinantes nessa avaliação. Desde logo, estranha-se a omissão da referência à sensibilidade ou criticidade da informação existente nos sistemas de informação, à existência de mecanismos fiáveis de rastreabilidade, bem como de recuperação e redundância, e ainda à adequação dos recursos humanos adstritos a cada função específica neste contexto. A CNPD considera, por isso, essencial a previsão expressa destes fatores no elenco do n.º 4 do artigo 10.º do Projeto.

8. No que diz respeito à notificação de incidentes, compreendendo que a obrigação de notificação ao Centro Nacional de Cibersegurança (CNCS) só nasça quando os incidentes tenham impacto relevante ou substancial (cf. artigo 10.º do Projeto), a CNPD entende que, no contexto de um regime que procura também promover a responsabilização ativa das entidades a ele sujeitas, se revela adequada e pertinente a previsão da obrigação de registo interno de todos os incidentes de segurança. Uma tal obrigação complementar permite não apenas a racionalização do juízo sobre a relevância ou substância do impacto, pela própria entidade, como também a verificação *ex post* desse juízo valorativo pela entidade administrativa competente. Essa obrigação será ainda relevante para efeito de identificar falhas na segurança da rede e do sistema de informação, ao permitir detetar a eventual recorrência dos incidentes.

9. Nesse sentido, a CNPD recomenda a introdução no capítulo IV, ou no Capítulo III, de uma norma que preveja a obrigação de registo interno dos incidentes de segurança.

10. Quanto ao regime das obrigações de notificação, assinala-se que o prazo previsto no n.º 1 do artigo 13.º do Projeto corre o risco de ser demasiado exíguo, pois que, com o prazo de duas horas para se realizar a notificação e dar prioridade à mitigação e resolução do incidente, a notificação pode traduzir-se numa mera formalidade vazia de conteúdo descritivo que permita a quem a recebe fazer uma avaliação ajustada do incidente. Tendo em conta que o legislador europeu, no contexto das violações de dados pessoais (ou seja, dos incidentes de segurança que afetam dados pessoais), definiu um prazo para o cumprimento da obrigação de notificação de 72 horas (cf. n.º 1 do artigo 33.º do RGPD), a CNPD toma a liberdade de sugerir que se repense o período de tempo fixado no n.º 1 do artigo 13.º do Projeto.

11. Em relação ao artigo 16.º do Projeto, a CNPD permite-se assinalar uma incongruência concetual. No n.º 2 do artigo 16.º, quando se pretende elencar os *efeitos* que os incidentes podem produzir, estão previstas também *causas* dos incidentes, como parece suceder com a «infeção por *malware*», a «intrusão» e a «tentativa de intrusão». E na mesma disposição, estranhamente, estão omissas consequências que o próprio artigo 4.º, ponto 2, da Diretiva (UE) 2016/1148 enuncia como consequências de incidentes de segurança, a saber, além da disponibilidade (indicada na alínea b) do n.º 2 do artigo 16.º do Projeto), a «autenticidade, a integridade e a confidencialidade».

12. Repare-se que esta observação não é meramente formal, já que, como se destacou no início do presente parecer, as entidades sujeitas ao regime aqui em análise estão também sujeitas, por regra, ao RGPD, o qual contém disposições relativas a incidentes de segurança e à obrigação de os notificar, importando, por razões de segurança e certeza na aplicação do Direito, que o legislador nacional não introduza diferenças, em relação à legislação da União Europeia, na caracterização dos incidentes e dos seus possíveis efeitos.

13. A CNPD recomenda, por isso, a revisão do n.º 2 do artigo 16.º do Projeto, a bem da clareza e da certeza jurídica num artigo que tem por epígrafe a «Taxonomia de incidentes e de efeitos».

14. Uma última nota para destacar que o presente diploma poderia ser uma oportunidade para densificar a obrigação de colaboração entre o GNSC e a CNPD, sumariamente prevista no n.º 8 do artigo 7.º da Lei n.º46/2018, de 13 de agosto, em especial tendo em conta o estatuído no considerando 63 da Diretiva (UE) 2016/1148. Com efeito, aí se refere o *dever de cooperar e trocar informações* entre as duas entidades quando ocorram incidentes de segurança com violação dos dados pessoais, o que a mera referência a «*atua em colaboração com*» constante daquele preceito legal não espelha suficientemente.

III. Conclusão

15. Com os fundamentos supra expostos e com o intuito descrito no ponto 4, a CNPD recomenda:

i. A adição, no contexto das obrigações previstas no artigo 7.º e na alínea *a)* do n.º 1 do artigo 8.º do Projeto, de medidas organizativas e, em particular, de formação dos recursos humanos sobre as questões de segurança das redes e sistemas de informação;

ii. A exigência expressa, no artigo 10.º do Projeto, eventualmente no n.º 2, de que a obrigação de realizar a análise dos riscos e de documentação dessa análise reflita uma visão de conjunto dos riscos;

iii. A previsão no n.º 4 do artigo 10.º dos seguintes fatores a considerar nessa análise dos riscos: sensibilidade ou criticidade da informação existente nos sistemas de informação, existência de mecanismos fiáveis de rastreabilidade, bem como de recuperação e redundância, e ainda adequação dos recursos humanos adstritos a cada função específica neste contexto;

iv. A introdução no capítulo IV ou no Capítulo III de uma norma que preveja a obrigação de registo interno dos incidentes de segurança;

v. A reponderação do período de tempo fixado no n.º 1 do artigo 13.º do Projeto para a execução do dever de notificação de incidentes de segurança;

vi. A revisão do n.º 2 do artigo 16.º do Projeto, a bem da clareza e da certeza jurídica num artigo que tem por epígrafe a «Taxonomia de incidentes e de efeitos», nos termos expostos supra nos pontos 11 e 12.

Lisboa, 4 de maio de 2021

Filipa Calvão (Presidente, que relatou)