COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

PARECER N.º 14 /2018

A Assembleia da República, através da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias, veio solicitar à Comissão Nacional de Protecção de Dados (CNPD) a emissão de parecer sobre a 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[1], relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

O pedido formulado visa cumprir as 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 (LPDP), sendo o parecer emitido no uso da competência fixada na alínea *a)* do n.º 1 do artigo 23.º da citada lei.

I. Da Proposta de Lei

Na Exposição de Motivos da proposta de lei afirma-se que *as redes e os sistemas de informação desempenham um papel vital na sociedade, sendo a sua resiliência e segurança essenciais para a prossecução de atividades económicas e societais*. Constata-se ainda que *a abrangência, frequência e impacto dos incidentes de segurança estão a aumentar, constituindo uma importante ameaça para o funcionamento das redes e dos sistemas de informação*.

Na proposta de lei, prevê-se a definição de uma Estratégia Nacional de Segurança do Ciberespaço, a ser aprovada por resolução do Conselho de Ministros, bem como a criação de um Conselho Superior de Segurança do Ciberespaço e respetiva composição e competências.

O Centro Nacional de Cibersegurança é a autoridade nacional competente, no contexto da aplicação da diretiva e, nessa medida, opera como ponto de contacto nacional para a cooperação internacional. Pela proposta de lei, adquire a natureza de Autoridade Nacional de

[1] JO L 194 de 19.7.2016, p.1-30

Cibersegurança, nele funcionando a equipa de resposta a incidentes de segurança informática nacional (CSIRT), cujas competências também estão definidas nesta proposta.

A proposta de lei estabelece obrigações genéricas para a administração pública e para os operadores de infraestruturas críticas, para os operadores de serviços essenciais e para os prestadores de serviços digitais, quanto à aplicação de medidas para prevenção e gestão do risco e quanto à notificação de incidentes ao Centro Nacional de Cibersegurança. Todavia, remete para legislação posterior complementar a definição de requisitos de segurança e de requisitos de notificação de incidentes, no prazo de 150 dias da entrada em vigor do diploma (cf. artigos 12.º,13.º e 31.º).

O Centro Nacional de Cibersegurança tem competências de fiscalização e sancionatórias, sendo que as infrações constituem contraordenações.

II. Da apreciação

A segurança das redes e dos sistemas de informação tem naturalmente uma especial relevância para a proteção de dados, sempre que estiver em causa o tratamento de dados pessoais. O âmbito desta diretiva e da proposta de lei que a transpõe é mais abrangente, pois diz respeito a qualquer tipo de informação, contudo, essa informação poderá comportar também informação de natureza pessoal.

Em conformidade com o artigo 2.º, n.º 7, alínea *a)* da proposta de lei aqui em análise, o *disposto na presente lei não prejudica o cumprimento da legislação aplicável em matéria de proteção de dados pessoais*. Esta é uma norma que se reveste de extrema importância, por duas ordens de razão: por um lado, porque a terminologia semelhante ('segurança', 'risco', 'incidente', 'notificação', 'medidas técnicas e organizativas') poderia trazer equívoco sobre o alcance e eventual concorrência das obrigações num e noutro contexto; por outro lado, porque as obrigações legais do novo regime de proteção de dados[2] em matéria de segurança da informação são bastante mais exigentes do que as comtempladas na diretiva em transposição, pelo que será necessário garantir que o nível de proteção será sempre o mais

[2] Regulamento (UE) 2016/679 – Regulamento Geral sobre a Proteção de Dados (RGPD) e Diretiva (UE) 2016/680, relativa ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais.

elevado. Por conseguinte, os responsáveis pelos tratamentos de dados pessoais e os subcontratantes terão de cumprir as disposições da legislação de proteção de dados pessoais.

Independentemente da observância dos preceitos quanto à segurança e quanto à notificação de violações de dados pessoais constante da legislação específica de proteção de dados, a Diretiva (UE) 2016/1148 diz expressamente que se aplica a legislação de proteção de dados aos tratamentos de dados pessoais efetuados no seu âmbito.

Aliás, o Considerando 72 explica que *a partilha de informações sobre os riscos e incidentes a nível do grupo de cooperação e da rede de CSIRT e o cumprimento dos requisitos de notificação de incidentes às autoridades nacionais competentes ou às CSIRT poderão requerer o tratamento de dados pessoais. Esse tratamento deverá cumprir o disposto na Diretiva 95/46/CE (...).* Esta menção à diretiva de proteção de dados deverá agora dar-se por feita aos novos atos legislativos de proteção de dados.

Assim, em linha com a diretiva em transposição, considera a CNPD que, por uma questão de clareza e segurança jurídica, deveria ser introduzida norma específica na proposta de lei que transpusesse o artigo 2.º, n.º 1, da Diretiva (UE) 2016/1148.

Ainda relativamente a outros aspetos de convergência com o regime de proteção de dados, sublinha-se que a Diretiva (UE) 2016/1148, no seu artigo 15.º, n.º 4, prevê que as autoridades competentes, neste caso, o Centro Nacional de Cibersegurança, *trabalhem em estreita colaboração* com as autoridades de proteção de dados, quando *tratarem de incidentes que tenham dado origem à violação de dados pessoais*.

Ora, esta disposição não vem transposta para o ordenamento jurídico interno no texto da proposta de lei aqui em apreciação. No entender da CNPD, essa é uma falha que deverá ser suprida no texto legislativo, pois uma cooperação entre as duas autoridades a este nível resultaria certamente numa aplicação mais eficaz do quadro legal aplicável. A esse propósito, o Considerando 63 reconhece que *os dados pessoais ficam em muitos casos comprometidos em consequência de incidentes*, pelo que as autoridades competentes e as autoridades de proteção de dados *deverão cooperar e trocar informações sobre todas as questões pertinentes para combater as eventuais violações de dados pessoais resultantes de incidentes.*

Deste modo, deverá ser aditada uma norma na proposta de lei, eventualmente no seu artigo 7.º (no qual já se prevê *articulação e estreita cooperação* com outras entidades), que determine a cooperação entre o Centro Nacional de Cibersegurança e a CNPD quando este tenha conhecimento de incidentes que tenham resultado em violação de dados pessoais.

Quanto ao âmbito de aplicação da proposta de lei, suscitam-se dúvidas sobre o alcance da alínea *e)* do n.º 1 do artigo 2.º, quando se estabelece que a lei se aplica *a quaisquer outras entidades que utilizem redes e sistemas de informação*, além de se aplicar à Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais. Todas as obrigações estão definidas em função destes últimos atores. Apenas o artigo 20.º, sobre notificação voluntária de incidentes, poderá abarcar outras entidades além das especificamente identificadas. Se assim for, talvez seja de restringir especificamente a aplicação da lei às entidades referidas na alínea *e)*, apenas para os efeitos do artigo 20.º, em vez de deixar a aplicabilidade da lei em aberto a quaisquer entidades sem objeto concreto.

Em relação às competências da equipa CSIRT, designada por «CERT.PT», elencadas no artigo 9.º da proposta de lei, chama-se a atenção para a competência prevista na alínea *b)* do artigo: *Monitorizar o ciberespaço*.

Com efeito, esta é uma competência demasiadamente vaga e abrangente, se não mesmo inexequível e desajustada neste contexto. Confrontando as atribuições das equipas CSIRT, previstas no Anexo I da diretiva, com o texto da proposta de lei, verifica-se haver grande coincidência, à exceção desta alínea *b)* do artigo 9.º. A competência correspondente na diretiva vem no n.º 2, alínea *a)*, i. do referido anexo e prescreve: *monitorizar os incidentes a nível nacional*.

Considera-se, por conseguinte, que deveria ser alterada a redação da alínea b) do artigo 9.º da proposta de lei, no sentido de substituir a monitorização do ciberespaço pela monitorização dos incidentes a nível nacional.

Ainda no quadro das obrigações e atribuições das CSIRT, listadas no Anexo I à diretiva, não poderá deixar de se notar que a proposta de lei apenas estabelece as competências das equipas, mas não as suas obrigações.

COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Por último, é de sublinhar o valor irrisório das coimas previstas, no âmbito do regime sancionatório definido nesta proposta de lei, em particular se se tiver em conta que *as redes e os sistemas de informação desempenham um papel vital na sociedade* (...) e que este *tipo de incidentes pode colocar em causa o regular funcionamento da sociedade, acarretar perigo para a vida humana, perdas de natureza financeira, bem como comprometer a confidencialidade, a integridade e a disponibilidade da informação das redes e dos sistemas da Administração Pública, dos operadores dos serviços essenciais e dos prestadores de serviços digitais*, como afirmado na Exposição de Motivos.

Embora se verifique não haver distinção entre o setor público e o setor privado, estando as entidades públicas igualmente sujeitas a sanções pecuniárias, afigura-se que a punição para uma infração muito grave balizada por uma coima máxima de 5 mil Euros[3] está longe de constituir uma sanção efetiva, proporcionada e dissuasiva, como exige o artigo 21.º da diretiva.

Além disso, na medida em que a segurança do tratamento de dados pessoais depende também da segurança de sistemas de informação e de redes, há uma relação evidente com o regime europeu de proteção de dados, que penaliza de modo bem mais severo o incumprimento de normas relativas às obrigações relativas à adoção de medidas de segurança adequadas.

III. Conclusão

Com os fundamentos acima expostos, considera a CNPD, em suma, o seguinte:

1. Deve ser clarificado o alcance da alínea *e)* do n.º 1 do artigo 2.º da proposta.

2. Deve ser introduzida norma específica quanto à aplicação da legislação de proteção de dados aos tratamentos de dados pessoais efetuados no âmbito da presente lei, em conformidade com o disposto no artigo 2.º, n.º 1, da diretiva em transposição.

[3] Valor que pode ser reduzido a metade em caso de negligência (cf. artigo 25.º da proposta de lei)

3. Deve ser aditada disposição que preveja a estreita colaboração entre o Centro Nacional de Cibersegurança e a CNPD quando aquele tratar incidentes que tenham dado origem à violação de dados pessoais, no cumprimento do artigo 15.º, n.º 4, da diretiva.

4. Deve ser alterado o texto da alínea *b)* do artigo 9.º da proposta, sobre as competências das equipas CSIRT, no sentido de substituir a competência da equipa CSIRT de *monitorizar o ciberespaço* pela monitorização de incidentes a nível nacional, conforme decorre do Anexo I à diretiva.

5. Devem ser ajustados os montantes das coimas previstas na proposta de lei, em cumprimento do artigo 21.º da diretiva, que determina deverem as sanções ser efetivas, dissuasivas e proporcionais, em particular tendo em conta o valor do bem a defender.

Lisboa, 17 de abril de 2018

Filipa Calvão (Presidente)