

PARECER/2023/67

I. Pedido

1. O Secretário de Estado da Administração Pública solicitou à Comissão Nacional de Proteção de Dados (CNPDP) emissão de parecer sobre dois projetos de Portaria que visam regulamentar aspetos da Lei n.º 104/2019, de 6 de setembro, que reformulou e ampliou o Sistema de Informação da Organização do Estado criado pela Lei n.º 57/2011, de 28 de novembro.

2. Assim, através do presente Parecer procede-se à análise, por um lado, do Projeto de Portaria que define o conteúdo, a estrutura, os prazos e a periodicidade de registo e atualização da informação no Sistema de Informação da Organização do Estado (SIOE), nos termos da Lei n.º 104/2019, de 6 de setembro (doravante "Projeto 1").

3. Por outro, do Projeto de Portaria que define as regras e os procedimentos especiais de segurança para acesso e tratamento de dados e para o funcionamento da plataforma de tramitação eletrónica no âmbito do Sistema de Informação da Organização do Estado (SIOE), nos termos da Lei n.º 104/2019, de 6 de setembro (de ora em diante "Projeto 2").

4. A CNPDP 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, conjugado 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, 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

5. A Lei n.º 104/2019, de 6 de setembro, reformulou e ampliou o Sistema de Informação da Organização do Estado (SIOE), criado pela Lei n.º 57/2011, de 28 de novembro, por sua vez alterada pela Lei n.º 66.º-B/2012, de 31 de dezembro, e integrou naquele Sistema os dados constantes da base de dados dos recursos humanos da Administração Pública (BDAP), bem como estabeleceu o regime de prestação de informação no SIOE sobre atividade dos empregadores públicos.

6. Os dois projetos de Portaria em análise visam corporizar o preceituado nos números 6 do artigo 4.º e 3 do artigo 6.º daquela Lei, na medida em que ali se estabelece que alguns aspetos técnicos e operacionais devem ser concretizados por meio de Portaria de regulamentação.

7. Aquela referida Lei estabelece nos números 1 e 3 do artigo 2.º o seu âmbito de aplicação, identificando um universo significativo de entidades públicas: órgãos de soberania e respetivos órgãos e serviços de apoio, incluindo Assembleia da República e Presidência da República; órgãos e serviços da administração direta, indireta e autónoma e demais entidades das regiões autónomas e das autarquias locais; às entidades intermunicipais, e às empresas do setor empresarial do Estado e dos setores empresariais regionais, municipais e intermunicipais; ao Banco de Portugal; entidades administrativas independentes e a outras entidades não financeiras e financeiras das administrações públicas em contas nacionais, às sociedades não financeiras e financeiras públicas, bem como as demais pessoas coletivas públicas e outras entidades que integram ou venham a integrar o setor público.

8. Ainda, preceitua no n.º 1 do artigo 4.º que o SIOE integra «informação estruturada, organizada, uniformizada e atualizada» relativa a:

- a. caracterização dos empregadores públicos, incluindo a sua atividade social, e dos respetivos trabalhadores;
- b. dados de identificação e demais dados pessoais dos trabalhadores ao serviço dos empregadores públicos, independentemente da natureza ou modalidade de vínculo laboral ou outro, e das pessoas em regime de prestação de serviço.

9. Por outro lado, vêm especificadas no mesmo artigo as finalidades visadas com o tratamento dos dados de identificação e demais dados do trabalhador no SIOE, das quais se destacam, para o que ora importa, as seguintes:

- a. Gerir, controlar, acompanhar e avaliar os movimentos dos trabalhadores, designadamente ocasionados pela reorganização, reestruturação, cisão, fusão e outras alterações estruturais ou funcionais dos empregadores públicos, bem como a mudança de local de trabalho, reafecção, mobilidade, cedência e outras vicissitudes contratuais dos trabalhadores;
- b. Gerir e controlar o sistema de créditos de horas e os acordos de cedência de interesse público no âmbito da atividade sindical;
- c. Garantir a troca de dados no âmbito da coordenação dos sistemas de segurança social.

10. Para cumprir aquelas finalidades, prevê-se que o SIOE possa constituir-se como plataforma de tramitação eletrónica de procedimentos administrativos, prestação e tomada de decisão, cuja estrutura e regras de funcionamento devem, nos termos do n.º 6 do mesmo artigo, ser reguladas por Portaria (número 5 do artigo 4.º).

11. É neste contexto que é apresentado para análise da CNPD o “Projeto 1”, que define o conteúdo, a estrutura, os prazos e a periodicidade de registo e atualização da informação no Sistema de Informação da Organização do Estado.

12. Em termos estruturais, o “Projeto 1” regula a estrutura e conteúdo da informação sobre os empregadores públicos (artigo 3.º), consagra regras sobre a forma de registo e atualização da informação (artigo 4.º), bem como especifica a informação a prestar pelo empregador público em determinados âmbitos concretos: informação sobre Identificação, caracterização e atividade social do empregador público; informação sobre Mapa de Pessoal; informação sobre o Quadro de Pessoal; informação sobre Fluxos de entradas e saídas de trabalhadores; informação sobre atividades de formação profissional dos trabalhadores; informação sobre atividades de segurança e saúde no trabalho; informação sobre acidentes de trabalho e doenças profissionais, informação sobre greves; e informação sobre prestadores de serviços (artigos 5.º a 13.º, respetivamente).

13. Por sua vez, tal como prescrito no n.º 3 do artigo 6.º da Lei n.º 104/2019, o “Projeto 2” define as regras e os procedimentos especiais de segurança para acesso e tratamento de dados e para o funcionamento da plataforma de tramitação eletrónica no âmbito do Sistema de Informação da Organização do Estado (SIOE), regula o modo como se efetua o acesso ao SIOE (artigo 2.º), explicita as competências da DGAEP enquanto entidade gestora do SIOE (artigo 3.º) e cuida de aspetos técnicos e de segurança dos sistemas e operações envolvidas.

14. Nomeadamente, identifica as funcionalidades da plataforma de tramitação eletrónica digital e estabelece regras para o funcionamento desta (artigo 16.º a 19.º).

15. Algumas das normas consagradas nos referidos projetos de Portaria suscitam à CNPD algumas reservas ou observações, que de seguida se explicitam.

16. Acresce que no “Projeto 2” prevê-se a existência de um mecanismo de acompanhamento e controlo do sistema de créditos sindicais e cedências de interesse público, no âmbito da atividade sindical, em articulação com as associações sindicais (alínea d) do artigo 16.º). No entanto, não fica claro se este mecanismo implica o tratamento de dados pessoais de trabalhadores ou se se trata apenas de informação agregada.

17. Vem preceituado no artigo 8.º do “Projeto 2” que “a autenticação dos utilizadores na plataforma eletrónica é efetuada com recurso a mecanismos de autenticação segura, designadamente através da utilização de Cartão de Cidadão ou Chave Móvel Digital, com possibilidade de recurso ao Sistema de Certificação de Atributos Profissionais (SCAP)”.

18. Tal disposição técnica é ambígua porquanto, embora defina um mecanismo robusto de autenticação, não concretiza, por um lado, se o SCAP será sempre utilizado para credenciar profissionalmente os trabalhadores na plataforma eletrónica, enquanto funcionários legítimos do organismo no qual exercem funções pelas quais devem ter acesso aos dados e, por outro, não concretiza, ainda, se nos casos em que não seja utilizado o SCAP, qual o mecanismo de verificação para estabelecer a identidade de cada utilizador em determinado organismo para autorizar ou revogar o acesso.

19. Ademais, embora o artigo 13.º do "Projeto 2" se determine que a plataforma eletrónica deve garantir a capacidade de controlar e limitar o acesso aos diversos recursos e de identificar os utilizadores através da associação do perfil às respetivas permissões, em como o seu ciclo de vida, a verdade é que não se encontra definido o modo como será contratualizada com os organismos públicos a responsabilidade para a manutenção da lista de utilizadores ativos atualizada.

20. Frise-se, ainda, que para efeitos de autenticação, são enviados dados do titular à plataforma que está a solicitá-la. No entanto, não vêm explicitados, no caso, quais os dados a transmitir para efeitos de autenticação no caso da plataforma eletrónica do SIOE.

21. No que respeita à possibilidade de utilização de mecanismos de autenticação individuais, tais como o Cartão de Cidadão (CC) e a Chave Móvel Digital (CMD) como instrumento para desempenhar os deveres profissionais, previstos no artigo 8.º, a CNPD reitera as reservas expendidas no Parecer/2023/9¹.

22. De facto, a utilização daqueles meios por parte dos trabalhadores para efeitos de identificação constitui uma operação de tratamento que, para que se afigure lícita, deve ser legitimada por, pelo menos um dos fundamentos de licitude previstos no artigo 6.º do RGPD.

23. Ora, uma leitura atenta do artigo 6.º do RGPD permite facilmente concluir que não existe qualquer norma legal que imponha, ou possibilite, que o empregador exija aos seus trabalhadores a utilização do seu CC ou CMD como instrumentos de trabalho (cf. Lei n.º 7/2007, de 5 de fevereiro, Decreto-Lei n.º 74/2014, Lei n.º 37/2014, de 26 de junho).

24. Desde logo, também não é possível enquadrar o tratamento dos dados pessoais na necessidade de cumprimento de uma obrigação jurídica, nem no interesse legítimo do responsável (cf. alíneas c) e f) e parte final do n.º 1 do artigo 6.º do RGPD].

¹ Disponível em www.cnpd.pt.

25. Recordar-se, a este respeito, o que foi dito no Parecer n.º 66/2017 da CNPD a propósito da Portaria n.º 73/2018, de 12 de março.

26. Nos termos conjugados da alínea a) do n.º 1 do artigo 6.º e da alínea 11) do artigo 4.º, ambos do RGPD, a validade do consentimento como fundamento de licitude do tratamento de dados depende do preenchimento de requisitos muito exigentes, que visam pautar os direitos, liberdades e garantias dos titulares de dados pessoais, isto é, deve constituir uma manifestação de vontade livre, específica, informada e inequívoca.

27. Tal implica que tem de ficar demonstrada a existência de condições de liberdade para a manifestação dessa vontade. Ora, a situação de dependência em que o trabalhador se encontra no contexto das relações laborais, não permite, à partida, a formação livre dessa vontade.

28. Por outro lado, a letra da lei é clara quando estabelece que o titular do CC só utiliza as suas funcionalidades de certificação eletrónica “[q]uando pretenda” (cf. n.º 5 do artigo 18.º da Lei n.º 7/2007, de 5 de fevereiro). Assim, para que a adesão a estes meios seja efetivamente livre, os responsáveis devem poder garantir ao trabalhador um meio alternativo que permita a autenticação do trabalhador sem recorrer aos dados constantes do seu documento pessoal de identificação.

29. Uma vez que a formação livre da vontade depende da existência de alternativa à utilização daqueles meios, porque qualquer deles supõe a utilização voluntária e livre pelos trabalhadores, se não for garantida uma alternativa à utilização daqueles meios, o tratamento de dados pessoais que resulte da utilização do CC ou da CMD para esses fins será ilícito.

30. Por essa razão deve a DGAEP garantir que disponibiliza mecanismos alternativos para a autenticação dos profissionais, sem que daí decorra qualquer ónus ou encargo para o trabalhador.

31. No que respeita às características do sistema e às medidas de segurança, estabelece-se no artigo 2.º do “Projeto 2” o acesso ao SIOE será realizado através da página eletrónica da Direção-Geral da Administração e do Emprego Público (DGAEP), que disponibiliza uma interface web para administração e gestão da aplicação e que a ligação da plataforma eletrónica à rede pública deve ser assegurada, no mínimo, por duas origens fisicamente independentes (artigo 6.º).

32. Estabelece-se, ainda, observa-se que a ligação da plataforma eletrónica à Internet deve ser protegida por um sistema de proteção de fronteira (firewall) e deve estar alojada num segmento da rede de produção devidamente protegido (artigo 10.º).

33. A CNPD entende que tais medidas devem ser robustecidas com outras que acautelem que o repositório dos dados do SIOE não fica também exposto na rede pública.

34. Nomeadamente, devem adotar-se as seguintes medidas, entre outras:

- a. Garantir que o sistema de armazenamento dos dados não está na mesma rede que a plataforma eletrónica;
- b. Usar uma firewall para filtrar o tráfego entre a rede da plataforma eletrónica e a rede privada onde está o repositório dos dados, permitindo apenas as portas e os protocolos necessários para a comunicação entre a aplicação e o repositório;
- c. Configurar um *reverse proxy* para intermediar as requisições da aplicação para o repositório, evitando a exposição direta do endereço de rede do repositório na rede pública;
- d. Adotar um protocolo seguro para a transmissão dos dados entre a aplicação e o repositório de dados;
- e. Introduzir uma autenticação forte para o acesso ao repositório de dados: senhas complexas, certificados digitais ou *tokens*, para evitar o acesso não autorizado ou fraudulento; e
- f. Aplicar uma criptografia dos dados armazenados, como o uso de algoritmos simétricos ou assimétricos, para evitar a leitura ou a cópia dos dados por terceiros em caso de invasão ou roubo.

35. Deve ter-se em consideração que, embora "Projeto 2" preveja mecanismos de controlo e registo de acessos (artigo 13.º), o mesmo é omissivo relativamente ao prazo de conservação de dados de arquivo, o que se revela uma desconformidade com o RGPD.

36. Assim, recomenda-se que sejam revistas e densificados na Portaria estes aspetos, em obediência ao preceituado na alínea e) do art.º 5.º do RGPD, quando prescreve que os dados são «conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades».

37. Refira-se, ainda, que não obstante no "Projeto 1" se estabeleça um período transitório tendo em vista garantir a capacitação dos empregadores públicos para o registo da informação prevista, e que até ao final desse período de adoção gradual do sistema, a DGAEP assegura a disponibilização de soluções eletrónicas para as entidades efetuarem o registo da informação (artigo 15º), não fica claro quais são essas soluções eletrónicas, sendo certo que tais referências parecem apontar para soluções de contingência por forma a haver o reporte da informação pretendida.

38. Sendo esse o caso, é necessário o estabelecimento de um plano de contingência que assegure as medidas técnicas e organizacionais adequadas para esse cenário.

39. No que respeita ao exercício dos direitos por parte dos titulares, o Projeto 2 explicita que os mesmos são exercidos mediante prova da identidade do titular, nos termos previstos do RGPD e demais legislação de proteção de dados em vigor, identificando a entidade junto da qual estes direitos devem ser exercidos e o modo para o seu exercício – via plataforma ou junto do empregador público ou DGAEP.

40. Por fim, não pode deixar de se referir que a Lei n.º 43/2004, de 18 de agosto, pela alteração introduzida pela Lei n.º 58/2019, de 8 de agosto, passou a determinar no n.º 4 do artigo 18.º que “os pedidos de parecer sobre disposições legais e regulamentares em preparação devem ser remetidos à CNPD pelo titular do órgão com poder legiferante ou regulamentar, instruídos com o respetivo estudo de impacto sobre a proteção de dados” pelo que futuros projetos que venham a ser apresentados à CNPD para emissão de parecer, deverão vir instruídos com o respetivo estudo de impacto.

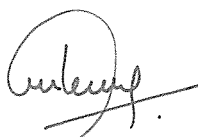
41. A omissão desse estudo de impacto compromete uma avaliação mais completa por parte da CNPD quanto aos prováveis riscos decorrentes dos tratamentos de dados pessoais.

III. Conclusão

42. Em consequência, a CNPD recomenda, entre outras medidas supra explicitadas, o seguinte:

- a. Sejam disponibilizados aos trabalhadores meios alternativos à autenticação através de Cartão de Cidadão e Chave Móvel Digital.
- b. Sejam robustecidas as características do sistema e às medidas de segurança, acomodando, entre outras, as medidas referidas no ponto 34.
- c. Sejam estabelecidos prazos de conservação dos dados de arquivo.

Lisboa, 6 de julho de 2023



Ana Paula Lourenço (Relatora)