PARECER/2022/72

I. Pedido

1. O Instituto da Segurança Social, I.P. (ISS, IP) veio solicitar à Comissão Nacional de Proteção de Dados (CNPD) a emissão de parecer sobre uma Convenção que visa determinar os termos e as condições de cooperação entre este Instituto, o Instituto de Segurança Social dos Açores, IP.RA, (ISSA, IP RA), o Instituto de Segurança Social da Madeira, IP-RAM (ISSM, IP RAM) e o Instituto de Informática, IP (II.IP) e a Caisse Nationale d'Assurance Vieillesse (CNAV), no que respeita ao intercâmbio eletrónico de informações sobre óbitos/existência de segurados, em conformidade com o Regulamento (CE) n.º 883/2004 do Parlamento Europeu e do Conselho, de 29 de abril de 2004, relativo à coordenação dos sistemas de segurança social e o Regulamento de aplicação (CE) n.º 987/2009 do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, que estabelece as modalidades de aplicação do Regulamento (CE) n.º 883/2004.

2. O pedido vem acompanhado da Avaliação de Impacto sobre a Proteção de Dados (AIPD).

3. O pedido formulado e o parecer ora emitido decorrem das atribuições e competências da CNPD, enquanto autoridade nacional de controlo dos tratamentos de dados pessoais, conferidos pela alínea c) do n.º 1 do artigo 57.º e pelo n.º 4 do artigo 36.º 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 na alínea a) do n.º 1 do artigo 6.º, todos da Lei n.º 58/2019, de 8 de agosto.

II. Análise

4. O Regulamento (CE) n.º 883/2004 do Parlamento Europeu e do Conselho, de 29 de abril de 2004, veio definir as regras de coordenação dos sistemas nacionais de segurança social, no âmbito da livre circulação de pessoas.

5. Por sua vez, o Regulamento de aplicação (CE) n.º 987/2009 do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, estabelece as modalidades de aplicação do Regulamento (CE) n.º 883/2004. Note-se que, ao abrigo dos poderes conferidos pelo artigo 71.º do Regulamento (CE) n.º 883/2004, a Comissão Administrativa para a Coordenação dos Sistemas de Segurança Social, fixou, através da Decisão n.º H5, de 18 de março de 2010, algumas regras para assegurar a cooperação entre as entidades nacionais competente quanto à troca de dados pessoais.

6. Nos termos dos Regulamentos supra citados, é permitido às diferentes instituições dos Estados-Membros da UE a troca de informações necessárias à verificação da existência das pessoas que preencham os pressupostos para serem titulares do direito a prestações, bem como ao cálculo e pagamento correto das prestações e à verificação da manutenção do direito a essas prestações.

7. A CNAV, enquanto responsável pelo regime jurídico francês de pensões dos trabalhadores por conta de outrem e dos trabalhadores independentes, deve verificar a existência das pessoas a quem são pagas as prestações. Acresce que os regimes de pensões obrigatórios delegaram na CNAV, operadora do Sistema Nacional de Gestão de Identificadores (SNGI), a missão de solicitar às instituições dos outros Estados-Membros da UE informação sobre se as pessoas cobertas pelos respetivos regimes, residentes nesses Estados, ainda se encontram vivas. Com efeito, o Decreto n.º 2018-390, de 24 de maio de 2018, prevê que o SNGI tem por objetivo verificar se os segurados ainda se encontram vivos.

8. Nos termos do artigo 104.º da Lei n.º 2020-1576 de 14 de dezembro de 2020 e do Decreto n.º 2021-390 de 2 de abril de 2021, relativo ao controlo da existência dos titulares de pensões de velhice e de outras pensões, residentes fora de França, os regimes de pensões obrigatórios franceses partilham a gestão da informação em matéria de provas de vida, a fim de tornar mais eficazes os controlos de existência das pessoas em causa.

9. Por sua vez, nos termos do n.º 1 do artigo L215 do Código de Segurança Social Francês, os Fundos de pensões e seguros de saúde no trabalho registam e verificam os dados necessários para determinar os direitos de pensões dos segurados do regime geral, liquidam e pagam as pensões decorrentes desses direitos.

10. Por outro lado, a Lei n.º 4/2007, de 16 de janeiro(Lei de Bases da Segurança Social), no artigo 25.º, relativo à relação com sistemas estrangeiros, dispõe que «O Estado promove a celebração de instrumentos de coordenação sobre segurança social com o objetivo de garantir a igualdade de tratamento aos beneficiários por ele abrangidos que exerçam atividade profissional ou residam no respetivo território relativamente aos direitos e obrigações, nos termos da legislação aplicável, bem como da proteção dos direitos adquiridos e em formação.»[1]

11. Assim, a presente Convenção vem regular a troca eletrónica de ficheiros informáticos com informação sobre óbitos/a existência de pessoas residentes em França, que recebem uma prestação do ISS,I.P., ISSM,IP-

[1] Veja-se em especial o Decreto-Lei n.º 187/2007, de 10 de maio, relativo ao regime jurídico de proteção na eventualidade de velhice e invalidez do regime geral de segurança social; o Decreto-Lei nº 322/90, 18/10, de outubro, relativo ao regime jurídico de proteção na eventualidade morte do regime geral de segurança social.

RAM e ISSA,IPRA, por um lado e, por outro, das pessoas residentes em Portugal e que recebem uma prestação da CNAV e dos regimes de pensão obrigatórios franceses.

12. A comunicação de dados pessoais configura um tratamento de dados pessoais, na aceção da alínea 2) do artigo 4.º do RGPD. O Anexo 1 da Convenção é dedicado à proteção de dados pessoais.

13. Da análise deste Anexo constata-se que o ponto 2 (responsabilidade das partes) refere que o país emissor dos dados é responsável pela transferência desses dados para o outro país. Recebidos os dados, o país é responsável pelas suas próprias atividades de tratamento. Ora, nos termos da alínea 7) do artigo 4.º do RGPD, o responsável pelo tratamento é a pessoa singular ou coletiva autoridade pública, a agência ou outro organismo que individualmente ou em conjunto com outras determina a finalidade e os meios de tratamento. Recomenda-se, assim, a reformulação deste inciso por forma a utilizar com precisão os termos empregues no RGPD2, por forma a indicar como responsável a parte outorgante portuguesa ou francesa, consoante o caso. O mesmo se aplica ao ponto 3, onde se referem os encarregados de proteção de dados (EPD) e as entidades de referência em matéria de informática e liberdades Tendo em conta que os responsáveis pelo tratamento de dados são entidades públicas, nos termos da alínea a) do n.º 1 do artigo 37.º do RGPD, sobre estas recai o dever de designar um EPD ou um delegado de proteção de dados, devendo, por isso, ser a referência a entidades de referência em matéria de informática e liberdade atualizada em conformidade com o conceito previsto no artigo 37.º do RGPD, na versão em língua francesa ("delegado de proteção de dados").

14. Refira-se ainda que no ponto 6. do Anexo 1 há um lapso na indicação dos artigos do RGPD onde estão previstos e regulados os direitos dos titulares dos dados, uma vez que o artigo 23.º do RGPD não prevê um direito. Nessa medida, a CNPD recomenda a revisão desse ponto 6., para passar a referir-se os direitos elencados nos artigos 15.º a 22.º do RGPD.

15. Os dados objeto de comunicação vêm referidos no Artigo 7.º da Convenção, compreendo dados de identificação (apelido de solteiro(a), apelido de casado(a), apelido utilizado, se for diferente dos apelidos anteriores, nome(s) próprio(s), data de nascimento, sexo, número secundário de inscrição no país (se utilizado pelo país), data e local de nascimento, filiação), data do óbito, endereço postal, código de identificação da situação- prova de vida e os números de identificação nacionais da pessoa em causa: número de Segurança Social (NIR) em França e número de Segurança Social (NISS) em ISS,I.P., ISSM,IP-RAM e ISSA,IPRA. Os dados objeto de tratamento são necessários e adequados à finalidade em causa em cumprimento do princípio da minimização dos dados previsto na alínea c) do n.º 1 do artigo 5.º do RGPD.

[2] Veja-se ainda a última parte do ponto 6.

16. Nos termos do n.º 2 do artigo 7.º da Convenção as modalidades de transmissão dos dados e a estrutura do ficheiro a utilizar para a troca dos mesmos são definidos no Anexo 2 – contrato de prestação de serviços. Aqui se refere que esta informação é enviada e recebida recorrendo a transferência de ficheiros de texto em formato pré-definido, cifrados com uma ferramenta de PGP3. Mais se especifica que a transferência de ficheiros é realizada através do protocolo FTP.

17. Importa assinalar que, este protocolo não é cifrado e, embora se recorra ao mecanismo do PGP, que fornece autenticação e privacidade criptográfica para comunicação de dados e, como as transferências são realizadas via rede privada s TESTA4, o risco seja relativamente baixo, a segurança das transmissões dos dados pode ser reforçada, através da utilização de um protocolo seguro ponto-a-ponto (por exemplo, sFTP/SSH). . Assim, a CNPD recomenda a reponderação das soluções encontradas no sentido de reforçar a segurança das transmissões dos ficheiros.

18. O ponto 6.2.3 da minuta do contrato de prestação de serviços (Anexo 2), respeitante a regras de rastreabilidade na gestão da troca de dados no II, I.P., dispõe que este organismo mantém um registo de envio de ficheiros com as respetivas instituições parceiras (emissor, data de entrada, data a ter em conta pela aplicação, etc.). No entanto não define o período de retenção pelo II, I.P., o qual se afigura dever ser análogo ao definido para a CNAV no ponto 6.2.1, portanto, de três anos. Recomenda-se, por isso, a previsão explícita do período de conservação do registo de envio dos ficheiros.

19. Note-se que no ponto 7.3 do Anexo 2se estabelece que «O acesso a este servidor é feito por filtragem de IP na rede privada e a ligação é feita através de login e palavra-passe». A este propósito, recomenda-se a utilização de credenciais fortes com passwords longas, únicas, complexas e com números, símbolos, letras maiúsculas e minúsculas. Importa também definir se a Área de Monitorização e Segurança da Informação (AMESI) irá proceder à recuperação do ficheiro de forma automática ou manual. Caso seja de forma manual, deve ser estabelecido um protocolo que assegure a confidencialidade da credencial atribuída de acesso aos ficheiros.

20. Sublinha-se que no contrato de prestação de serviço (Anexo 2) não está definido pelo II, I.P., onde ficam armazenados os ficheiros de pedidos enviados à CNAV e respetivas respostas, se os mesmos são retidos na forma cifrada com a ferramenta PGP e quem terá acesso ao repositório, tanto dos dados em uso como dos dados em arquivo, identificados na tabela do ponto 2.2.1.3 da AIPD. Embora estejam previstos e identificados os controlos de acessos lógicos aos dados, no âmbito das transferências, não se identificam os mesmos

[3] Para uma explicação simplificada deste conceito, pode ver-se https://pt.wikipedia.org/wiki/Pretty_Good_Privacy
[4] Cf. https://ec.europa.eu/isa2/solutions/testa_en/

controlos para os dados uma vez recuperados para o repositório de destino no II, I.P. Recomenda-se assim, a introdução de um novo ponto que contemple estes aspetos em falta.

21. Por último, importa referir que no ponto 11 do contrato de prestação de serviços (Anexo 2) vem descrito o processo de envio de dados em situações de natureza excecional. Uma das modalidades referidas é a utilização de uma ferramenta de transferência disponibilizado pela DSI da CNAV, utilizando o protocolo HTTPS. A CNPD relembra que este protocolo deverá estar assente na versão mais recente do TLS.

III. Conclusão

22. Nos termos e com os fundamentos acima expostos, a CNPD recomenda:

a) A reformulação do ponto 2 do Anexo 1, por forma a utilizar uma terminologia em conformidade com a do RGPD, em especial quanto ao conceito de responsável pelo tratamento;

b) A reponderação do ponto 4 do Anexo 2 de modo a garantir uma maior segurança na transferência de ficheiros;

c) A definição no ponto 6.2.3 do Anexo 2 do prazo de conservação pelo II,I.P. do registo de gestão de troca de dados com as instituições parceiras; e

d) A introdução de um inciso no Anexo 2 com as informações em falta identificadas supra, no ponto 20.

Lisboa,10 de agosto de 2022

Maria Cândida Guedes Oliveira (Relatora)