

PARECER/2021/112

I. Pedido

1. O Alto Comissariado para as Migrações, I.P (ACM), solicitou à Comissão Nacional de Proteção de Dados (CNPDP) a emissão de parecer sobre o projeto de Protocolo relativo à criação da Plataforma ConheSer+, da responsabilidade do ACM, do Serviço de Estrangeiros e Fronteiras (SEF) e do Instituto de Segurança Social, I.P. (ISS), em regime de corresponsabilidade.
2. A plataforma é uma ferramenta que interrelaciona a informação sobre refugiados residente nos sistemas das entidades signatárias, criando uma nova base de dados. A plataforma pretende facilitar a articulação das entidades por via da “operacionalização eficiente e em tempo real e o mapeamento desta população”, com o objetivo de estabelecer “um modo colaborativo de trabalho entre o SEF, o ACM e o ISS para que, agregando as valências dos três institutos públicos, o Estado Português possa assegurar um adequado acolhimento a refugiados no nosso país, ultrapassando as normais barreiras processuais em silos entre as entidades e dados inseridos em triplicado entre estas instituições” possibilitando, em suma, a “gestão integrada do processo de acolhimento”.
3. Pretende ainda “assegurar os indicadores da gestão de caso mediante o registo individual de requerentes e beneficiários de proteção Internacional (movimentos migratórios programados ou não programados), o registo do projeto de vida de cada [um] [...] e respetivo agregado familiar até à fase de autonomização [...] e ainda a identificação de movimentos secundários (abandonos, retomas e tomadas a cargo)”. A Plataforma possibilitará a produção de dados estatísticos, para monitorização, e de indicadores de “execução física e financeira dos protocolos ACM para gestão dos apoios [...] com as entidades de acolhimento”. Está prevista a “transferência de dados entre os responsáveis pelo tratamento e o Conselho Português para os Refugiados (CPR), a Santa Casa de Misericórdia de Lisboa (SCML), bem como entidades da sociedade civil (entidades de acolhimento)”.
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

i. Condição de licitude

5. O Protocolo em análise visa regular um sistema de informação, consubstanciado numa plataforma informática única de refugiados, para apoiar as entidades que têm por competência tramitar os processos de acolhimento e integração de pessoas a necessitar de proteção internacional.

6. Com efeito o SEF é a entidade responsável pelo registo e decisão sobre a aceitação da análise dos pedidos de proteção internacional, bem como, pela garantia de condições de acolhimento até à decisão de admissibilidade (cf. Lei n.º 27/2008, de 30 de junho, com as alterações introduzidas pela Lei n.º 26/2014, de 5 de maio), o ACM tem por competência a integração de estrangeiros residentes em Portugal (cf. alíneas c) e j) do n.º 2 do artigo 3.º do Decreto-Lei n.º 31/2014, de 27 de fevereiro, a Portaria n.º 203/2016, de 25 de julho, e ainda as Resoluções do Conselho de Ministros n.º 12-B/2015, de 20 de março, e n.º 103/2020, de 23 de novembro) e ao ISS compete suportar os encargos resultantes da atribuição das condições materiais de acolhimento aos requerentes de proteção internacional que entrem ou se encontrem em território nacional, desde a admissão do pedido até decisão final sobre o mesmo (cf. artigo 61.º, n.º 2 da Lei n.º 27/2008, de 30 de junho, alterada pela Lei n.º 26/2014, de 5 de maio).

7. A Resolução do Conselho de Ministros n.º 103/2020, de 23 de novembro, criou o Grupo Operativo Único, cuja formação restrita apenas integra estas três entidades, com funções de coordenação em matéria de acolhimento e integração de refugiados.

8. Nenhum dos diplomas ou regulamentos acima indicados prevê a criação do novo tratamento de dados pessoais da Plataforma ConheSer+. Apenas é referido que este tratamento está previsto na medida 25 do Simplex+2018. Ora, a medida referida afigura ser um ato de natureza política, que, por isso mesmo, necessita de intermediação legislativa para determinar a criação de um tratamento de dados pessoais e onde sempre se teria que prever garantias adequadas dos direitos fundamentais e interesses dos titulares dos dados.

9. Na verdade, os dados pessoais objeto de tratamento incluem dados de extrema sensibilidade, designadamente relativos a convicções religiosas e filosóficas, raça e etnia, saúde, pelo que, atenta a finalidade, teria de se encontrar condição de licitude na alínea b) ou na alínea g) do n.º 2 do artigo 9.º do RGPD. De facto, não basta que as entidades administrativas com competência legal para o tratamento de dados pessoais neste contexto decidam, por protocolo, criar uma nova plataforma e uma nova base de dados, centralizando a informação até aqui dispersa pelos sistemas de informação destas três entidades, invocando somente uma medida governamental, sem natureza legislativa ou, sequer, regulamentar. Sobretudo quando em causa estão

dados especiais, pois que aí a alínea e) do n.º 1 do artigo 6.º do RGPD é manifestamente insuficiente para fundamentar tal tratamento.

10. Sublinha-se que este é um tratamento de dados pessoais novo, que incide sobre um universo alargado de titulares de dados especialmente vulneráveis e relativo a um conjunto extenso de dados pessoais especialmente sensíveis, e que pela sua natureza implica riscos acrescidos para estes titulares, carecendo por isso de um específico e especialmente garantístico enquadramento legislativo.

11. Aliás, tanto a alínea b) como a alínea g) do n.º 2 do artigo 9.º do RGPD exigem que o tratamento tenha por base o direito da União ou do Estado-Membro. É essa previsão no direito português, e especificamente das garantias para acautelar os riscos acrescidos para os direitos dos titulares dos dados, que é omissa. Deste modo, não se encontra no RGPD fundamento de licitude para o tratamento de dados pessoais pretendido.

12. Sem prejuízo do que acaba de se concluir, a CNPD aprecia ainda as disposições constantes do Protocolo, destacando os aspetos de regime que devem ser revisitados.

ii. Responsabilidade conjunta

13. No n.º 2 da Cláusula Sexta do Protocolo afirma-se a responsabilidade conjunta dos três outorgantes, remetendo para um “Acordo de Responsabilidade Conjunta do Tratamento de Dados Pessoais”, doravante Acordo, que faz parte integrante do Protocolo.

14. Contudo, na Cláusula Terceira define-se, sob a epígrafe “Obrigações Específicas dos Outorgantes” que todas as entidades disponibilizam e recebem informação, remetendo-se para o Anexo F a discriminação dos dados pessoais a partilhar, acrescentando-se que ao ACM compete a “gestão da plataforma, assegurando o bom funcionamento da mesma e a atribuição de perfis”, e ao SEF cabe “garantir a segurança da informação e [d]o alojamento da Plataforma ConheSer+”.

15. Analisando o Acordo, com exceção das Cláusulas 6.ª e 9ª, que, respetivamente, determinam a existência de um endereço específico para ponto único de contacto e regulam a tramitação das comunicações relativas ao exercício dos direitos dos titulares, verifica-se que este se limita a imputar a cada parte o cumprimento das obrigações previstas no RGPD, o que não cumpre o disposto no artigo 26.º do RGPD. Recomenda-se, assim, a sua densificação.

iii. Avaliação de Impacto sobre a Proteção de Dados

16. O pedido veio acompanhado da Avaliação de Impacto sobre a Proteção de Dados (AIPD), em cumprimento do disposto no n.º 4 do artigo 18.º da Lei n.º 43/2004, alterada pela Lei n.º 58/2019, de 8 de agosto.

17. No ponto 4. da AIPD afirma-se que é efetuada uma "breve" análise de risco, na medida em que "ainda não se deu início à fase de desenvolvimento da aplicação informática". Percorrendo a AIPD isso mesmo é patente, não sendo possível verificar quais os efetivos riscos existentes e que medidas podem ser aptas a mitigar esses riscos. De todo modo, não pode a CNPD, nesta fase e com as informações disponibilizadas, pronunciar-se sobre a conformidade do tratamento de dados com o RGPD.

18. Assinala-se que não parece que o facto de não se ter iniciado o desenvolvimento da aplicação que irá dar suporte à Plataforma seja o único elemento que condiciona a análise de risco. Aliás, é também no momento da definição dos meios de tratamento que se deve, por aplicação dos princípios plasmados no artigo 25.º do RGPD, decidir as medidas aptas a proteger os direitos dos titulares.

19. A título de exemplo, refere-se a questão da subcontratação. Afirma-se a possibilidade de os responsáveis pelo tratamento poderem, sempre que se justifique, recorrer a subcontratantes, estando prevista a obrigação destes de implementação de todas as medidas técnicas e organizativas adequadas à proteção dos dados pessoais que lhes sejam transmitidos pelo responsável em questão, de modo a assegurarem a defesa dos direitos e interesses dos respetivos titulares, e sempre em cumprimento do disposto nos artigos 28.º e 29.º do RGPD.

20. Mas esta referência é genérica, limitando-se a repetir o previsto no n.º 1 do artigo 28.º do RGPD e a remeter para as disposições que regulam as subcontratações.

21. Na AIPD diz-se que "não foram ainda determinados quais os subcontratantes intervenientes neste processo. Logo que o seja feito, os mesmos assumirão tal posição devendo ser celebrado o contrato ou outro ato normativo com cada subcontratante, estabelecendo todos os aspetos estipulados no art. 28.º do RGPD, nomeadamente a duração, âmbito, finalidade, instruções de tratamento documentadas, autorização prévia onde um subcontratante está envolvido, fornecimento de qualquer documentação que comprove a conformidade com o RGPD, notificação imediata de qualquer violação de dados, bem como o definido no art. 29.º daquele Regulamento".

22. Ora, não estando indicado se existirão subcontratações e sobre que serviços incidirão, não é possível avaliar o risco daí decorrente. Pelo que a determinação da existência de subcontratações terá necessariamente de ser sujeita a nova avaliação de risco.

23. Já quanto à possibilidade de transferência de dados pessoais para fora da União Europeia, parece existir uma contradição entre a AIPD, onde é afirmado que não estão previstas, e o Acordo, uma vez que a Cláusula 11.ª, trata de "Transferências de dados para fora do Espaço Económico Europeu".

24. Pouco é referido sobre a tecnologia a utilizar para a implementação da plataforma, havendo apenas uma breve referência na secção que aborda *software malicioso*, onde é indicado que o acesso pode ser feito por redes menos seguras e que para tal os *browsers* serão atualizados.
25. Subentende-se, assim, que se trata de uma aplicação *web* acedida pelos utilizadores via *browser*. Nada se sabe, em rigor, da infraestrutura de comunicação, se em rede interna com acessos dedicados ou disponível na *internet*, nada é dito sobre a segurança do transporte da informação entre o cliente e a plataforma ConheSER+, nem dos meios usados na comunicação com as entidades externas.
26. Nada é referido relativamente à infraestrutura de segurança, designadamente se é existente e se previne acessos ilícitos e demais ataques.
27. Também quanto à interoperabilidade entre os sistemas é mencionado que as entidades pretendem que seja realizada através dos serviços de Interoperabilidade da Administração Pública, disponibilizados pela AMA, IP. Sobre esta matéria nada é detalhado e nenhum dos documentos remetidos acrescenta alguma informação sobre a matéria.
28. De igual modo, nada é indicado em relação à tecnologia usada para a base de dados gerida pela Plataforma, nem à infraestrutura que a implementa, nem à comunicação da componente aplicacional com o repositório de dados, nem à política de administração desse repositório e do controlo dos acessos, nem, com o rigor necessário, em relação à política de cópias de segurança.
29. Declara-se que, além dos acessos nominais à Plataforma ConheSER+, será disponibilizado o acesso via *web service*. Este possui como credenciais de autenticação um nome de utilizador e respetiva palavra passe, únicos a todas as invocações. Não está especificado qual o conjunto de operações que este *web service* disponibiliza nem quais as entidades capazes de o invocar. Da leitura dos documentos apenas se pode especular que poderá ser usado no carregamento automático de informação do SEF para a plataforma ConheSER+, no início da tramitação do processo, e no retorno de informação para os sistemas do SEF. Ademais, não se conhecem em detalhe essas operações automatizadas referidas nos anexos.
30. Ainda relativamente ao *web service*, não se sabe se as funcionalidades que disponibiliza ultrapassam as competências das diferentes entidades quando acedem à ConheSER+. Seria importante esclarecer se o *web service* terá capacidades que poderão ser invocadas pelos sistemas das entidades, contornando assim as limitações que a plataforma impõe no acesso direto dos utilizadores.
31. Nada é referido acerca da transferência de dados para as entidades externas, como seja, por exemplo, o Conselho Português para os Refugiados, a Santa Casa da Misericórdia de Lisboa e as diversas entidades de

acolhimento. Nada é indicado acerca dos dados que são enviados, nem sobre as medidas de segurança adotadas no transporte da informação, nem sobre a tecnologia utilizada. Tão pouco é referido como é espoletada a comunicação.

32. Na AIPD é identificado o risco de acesso ilegítimo que torna possíveis as operações de consulta, alteração ou apagamento. Como origens potenciais desse risco são apontadas a partilha de credenciais entre funcionários e o roubo de identidade, e como medida de mitigação propõem-se “que os utilizadores sejam devidamente e regularmente informados das boas práticas de higiene e segurança”, juntamente com a definição de palavras-passe fortes, bem como mecanismos para o bloqueio de sessão. Ora, atendendo à sensibilidade da informação tratada, as medidas indicadas são manifestamente insuficientes, impondo-se a utilização de mecanismos de autenticação multifator.

33. As referências aos registos de auditoria não estão suficientemente detalhadas. É indicado que as operações de acesso, criação e edição de registos, e de exportação de dados, serão alvo de *log*. Nada mais é referido relativo ao conteúdo desses registos de auditoria, para além de se mencionar que identificam o utilizador e a data/hora da alteração.

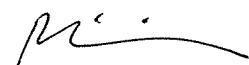
III. Conclusão

34. Com os fundamentos acima expostos entende a CNPD que o Protocolo incide sobre um tratamento de dados pessoais que não tem fundamento de licitude, não podendo, por isso, sob pena de violação do artigo 9.º do RGPD, ser realizado.

35. Não obstante, a CNPD assinala supra as disposições do Protocolo que carecem de reformulação e densificação e os aspetos do tratamento que carecem de avaliação e recomenda, especificamente, que:

- a. O Acordo de Responsabilidade Conjunta do Tratamento de Dados Pessoais seja objeto de revisão de modo a estabelecer as responsabilidades de cada responsável conjunto, em obediência ao artigo 26.º do RGPD;
- b. Sejam claramente definidos os meios de tratamento e efetuada nova AIPD, de modo que sejam previstas medidas mitigadoras aptas a garantir os direitos fundamentais e interesses dos titulares dos dados pessoais.

Lisboa, 26 de agosto de 2021



Filipa Calvão (Presidente que relatou)