PARECER/2020/37

I. Pedido

O Instituto da Segurança Social, I.P. (ISS), submeteu à Comissão Nacional de Proteção de Dados (doravante CNPD), para parecer, o Protocolo a ser outorgado com o Instituto de Informática, I.P., e com a Caixa Geral de Aposentações, I.P. (CGA), regendo *"os termos em que se verifica a cooperação, coordenação, troca de informação e procedimentos entre os serviços da CGA e as instituições de segurança social signatárias*".

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, 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 (doravante, Lei de Execução).

Importa para o efeito ter presente as finalidades do Protocolo, aqui se destacando, em especial, "*a concretização justa, rápida e eficaz das prestações de segurança social*", a simplificação o "*relacionamento dos cidadãos com a Administração*", e o objetivo de "*assegurar o controlo das obrigações contributivas, garantir a atribuição rigorosa das prestações sociais, bem como promover a eficácia na prevenção e combate à fraude e evasão contributiva*".

Para cumprir o estabelecido no Protocolo, o ISS e a CGA acordam em dotar os seus sistemas de informação das funcionalidades necessárias à partilha dos dados pessoais constantes de duas listas estruturadas que constituem os anexos I e II do referido Protocolo. Sendo o Instituto de Informática o responsável técnico pelos sistemas de informação do ISS e pela infraestrutura de comunicação de suporte aos referidos sistemas, e que "*assegura a construção, gestão e operação de sistemas aplicacionais e de infraestruturas tecnológicas nas áreas de tecnologias de informação e comunicação dos*

serviços e organismos dependentes do Ministério do Trabalho, Solidariedade e Segurança Social', é na qualidade de subcontratante do ISS que o mesmo é signatário deste protocolo.

A partilha dos dados entre os dois sistemas de informação ocorre da seguinte forma:

- Para a consulta de dados individualizados em situações singulares a CGA facultará o acesso ao seu portal da *Internet* a utilizadores do ISS selecionados e devidamente autorizados.
- Para as restantes consultas de dados entre os sistemas de informação da CGA e do ISS serão implementados *webservices*[1].

II. Apreciação

O Protocolo em apreço clarifica, na cláusula 6.º, a qualidade em que o ISS, a CGA e o Instituto de Informática intervêm no mesmo – respetivamente, responsáveis pelo tratamento (cf. alíneas *2)* e *7)* do artigo 4.º do RGPD) e subcontratante (cf. alínea *8)* do artigo 4.º do RGPD).

Analisados os dados objeto de tratamento elencados em anexo ao Protocolo, compreende-se que em causa estão também dados relativos à saúde de pessoas singulares, pelo que o tratamento incide sobre dados sensíveis especialmente protegidos nos termos do n.º 1 do artigo 9.º do RGPD. Na verdade, no anexo I do Protocolo estabelece-se que na "*Relação de dados a transmitir pela CGA*" se conta a "*designação da prestação (pensão de aposentação, velhice; invalidez; morte; preço de sangue; sobrevivência, subsídio mensal vitalício, bonificação por deficiência, etc…)*" e o "*tipo de incapacidade do subscritor*".

Tendo isso em conta e afigurando-se que o tratamento é realizado em grande escala, só pode concluir-se, em conformidade com a alínea *b)* do n.º 3 do artigo 35.º do RGPD, que o presente tratamento tem de ser precedido de uma avaliação de impacto sobre a proteção de dados. Essa avaliação pode ainda ser obrigatória caso se verifique, o que não foi

[1] Serviços disponibilizados via *web*.

possível aferir pela análise do Protocolo, os pressupostos previstos na alínea *a)* do n.º 3 do artigo 35.º do RGPD, como melhor se explica infra, no ponto 4.

A referida avaliação é particularmente pertinente para avaliar o risco para os direitos dos titulares dos dados e para determinar as medidas mitigadoras desse risco, em especial, medidas de segurança adequadas. Não obstante, no pedido não é mencionado que se tenha realizado a necessária avaliação de impacto, nem, em rigor, se vê refletida no clausulado do Protocolo as conclusões dessa avaliação e medidas que, nessa sede, tivessem sido definidas.

A CNPD recomenda, por isso, que essa avaliação seja ainda concretizada e que o texto do Protocolo seja densificado com a previsão de condições e regras adequadas a tutelar os direitos e interesses em crise.

Em especial, a CNPD destaca em seguida alguns aspetos omissos no clausulado do Protocolo ou que suscitam dúvidas quanto à adequação das soluções nele traçadas.

1. Começa-se por assinalar que na alínea *a)* do n.º 1 da cláusula 5.ª consta que o acesso aos dados armazenados nos sistemas de informação da CGA pode ser efetuado por funcionários do ISS devidamente selecionados e autorizados, através da "*consulta dos dados pessoais no portal da CGA na internet, por meio eletrónico e em tempo real*". O Protocolo remete na mesma cláusula e no mesmo número, para os anexos I e II, onde se identificam as categorias de dados pessoais comunicados entre as duas entidades.

Ora, da leitura do Protocolo não se afigura claro se esses dados são referentes à consulta dos dados pessoais no portal da CGA na *Internet*, ou se aos dados transmitidos pelas invocações aos *webservices*, ou até se se reportam a ambos os casos.

Aliás, o Protocolo não é explícito em relação aos conjuntos de dados pessoais que se tornam acessíveis ao funcionário da ISS, nem menciona as limitações ao conjunto de subscritores ou beneficiários de pensões ou prestações da CGA, cuja informação possa ser consultada através do referido portal.

Importa, por isso, também força do princípio da transparência vertido na alínea *a)* do n.º 1 do artigo 5.º do RGPD, que se defina com precisão os termos em que o tratamento de dados se concretiza, no caso, o acesso a dados pessoais por trabalhadores de entidade pública distinta daquela que os detém.

2. Em segundo lugar, no que concerne ainda à cláusula 5.ª, no n.º 2 refere-se que "*o ISS comunica à CGA a identificação das pessoas autorizadas a aceder à base de dados, tendo em vista a atribuição do nome de utilizador e as respetivas palavras-passe*". Neste ponto, o Protocolo não torna explícito o critério empregue na seleção desses funcionários, nem o universo de funcionários do ISS a credenciar para o acesso ao portal da CGA na *Internet*.

Os sistemas de informação da CGA e do ISS integram e tratam um universo alargado de dados pessoais, alguns dos quais correspondendo à categorias especiais de dados previstas no n.º 1 do artigo 9.º do RGPD (*v.g.*, relativos à saúde), pelo que se tem de prever e aplicar medidas técnicas e organizativas adequadas a garantir o cumprimento dos princípios da integridade e confidencialidade, consagrados na alínea *f)* do n.º 1 do artigo 5.º do RGPD, e como forma de garantir a própria auditabilidade do sistema e das operações de tratamento dos dados. .

3. Ainda no que diz respeito à cláusula 5.ª, mais concretamente no n.º 5, estatui-se que a "*comunicação eletrónica de dados entre sistemas pode ser efetuada através de circuito VPN entre o II e a CGA*".

Acontece que o Protocolo não determina expressamente que a comunicação dos dados pessoais entre o ISS e CGA deve ser sempre realizada através de canais seguros. Essa omissão afigura-se incompreensível, face aos princípios da integridade e confidencialidade, já aqui invocados, e dos quais decorre para o responsável pelo tratamento a obrigação de adotar as medidas técnicas ou organizativas adequadas a garantir a segurança do tratamento, nomeadamente a confidencialidade dos dados.

4. Importa também assinalar que no Protocolo não se encontra referência ao modo como a informação de um determinado subscritor ou beneficiário de pensões ou prestações da CGA, ou de um beneficiário do ISS se torna elegível para partilha entre as entidades em

causa. Aliás, não resulta do Protocolo se a seleção é casuística, manual e sujeita ao critério dos funcionários das partes signatárias, ou se redunda de aplicação sistemática e automatizada de um algoritmo nas bases de dados. E esse é um aspeto do tratamento que deveria estar explicitado e regulado no Protocolo, também porque os riscos e medidas mitigadoras dos riscos são de diferente natureza num caso e noutro.

Na primeira hipótese, a seleção deverá ser acompanhada de registos de auditoria de acesso rigorosos e definição de uma política de alarmística, como genericamente decorre dos princípios da integridade e da confidencialidade, e especificamente da alínea *d)* do n.º 1 do artigo 32.º do RGPD. Na segunda hipótese, a seleção, ao ser o resultado de procedimento sistemático e automatizado, implica a realização de uma avaliação de impacto sobre a proteção de dados, como decorre da alínea *a)* do n.º 3 do artigo 35.º do RGPD, a qual deveria ter acompanhado o presente pedido de parecer – caso tivesse sido elaborada, facto que a CNPD desconhece.

5. Finalmente, importa atender às regras de conservação dos dados pessoais. No n.º 7 da cláusula 5.ª convenciona-se que "*os dados transmitidos ao abrigo do Protocolo são conservados pelo prazo estritamente necessário ao cumprimento das finalidades nele previstas, sem prejuízo dos prazos legais estabelecidos*".

Acontece que o Protocolo não define intervalo temporal concreto, nem qualquer critério subjacente à delimitação temporal da conservação dos dados.

Sendo certo que a natureza dos tratamentos de dados pessoais realizados pelo ISS e pela CGA pressupõe o acompanhamento dos casos que se podem prolongar no tempo, deveria estar especificado o prazo para o apagamento dos dados, ou para a revisão periódica dos mesmos, garantindo-se assim que os sistemas de informação não conservem dados por período temporal superior ao justificado pelas finalidades prosseguidas, como impõe a alínea *e)* do n.º 1 do artigo 5.º do RGPD.

Acresce que também não se encontram regras sobre atualização dos dados conservados, que foram obtidos pelas invocações aos *webservices*, obrigação que decorre do princípio da exatidão vertido na alínea *d)* do n.º 1 do artigo 5.º do RGPD.

III. Conclusão

Considerando o universo de titulares de dados abrangidos pelo tratamento de dados objeto do Protocolo, bem como a natureza sensível ou especial de algumas das categorias de dados pessoais partilhados entre as entidades públicas, a CNPD sublinha que o presente Protocolo deveria ter sido antecedido da avaliação de impacto sobre a proteção de dados, nos termos previstos na alínea *b)* e porventura na alínea *a)* do n.º 3 do artigo 35.º do RGPD, facto que não se menciona no pedido apresentado, nem se vê refletido no clausulado do Protocolo.

A CNPD recomenda, por isso, que essa avaliação seja ainda concretizada e que o texto do Protocolo seja densificado com a previsão de condições e regras adequadas a tutelar os direitos e interesses em crise.

Em especial, e com os fundamentos acima expostos, a CNPD recomenda:

1. A clarificação, na cláusula 5.ª, n.º 1, alínea a), do Protocolo, dos termos e âmbito do acesso a dados pessoais detidos pela CGA por funcionários do ISS, em respeito pelo princípio da transparência dos tratamentos de dados;
2. A especificação dos critérios subjacentes aos perfis de acesso ao portal da CGA na *Internet*, em termos que permitam verificar o cumprimento dos princípios da integridade e confidencialidade do tratamento, bem como garantir a auditablidade do acesso;
3. A introdução no texto do Protocolo de uma disposição que imponha ou preveja a adoção de medidas de segurança adequadas a garantir a confidencialidade na transmissão dos dados entre os sistemas de informação do ISS e a CGA, em conformidade com os princípios da integridade e confidencialidade;
4. A especificação da forma ou do procedimento que permite identificar os subscritores ou beneficiários de pensões ou prestações da CGA ou os beneficiários do ISS que são elegíveis para a partilha dos respetivos dados entre as entidades em causa, com previsão das medidas adequadas a garantir a auditabilidade e a

mitigação de riscos para os direitos dos titulares, sobretudo, se tal resultar da aplicação sistemática e automatizada de um algoritmo nas bases de dados;

5. A introdução no Protocolo de disposições a prever os prazos máximos de conservação dos dados pessoais, bem como regras sobre a atualização dos dados, em obediência aos princípios da limitação da conservação e da exatidão.

Lisboa, 30 de março de 2020

Filipa Calvão (Presidente, que relatou)