CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2024/8

I. Pedido

1. A Secretaria de Estado da Administração Interna (SGMAI) solicitou à Comissão Nacional de Proteção de Dados (CNPD) a emissão de Parecer sobre a «Proposta de Regulamento de funcionamento da Base de Dados de Violência Doméstica, (BDVMVD)» doravante designada Proposta de Regulamento, que o Governo pretende fazer aprovar por Portaria.

2. O pedido de parecer vem instruído com vários documentos, entre os quais o relatório da avaliação de impacto sobre a proteção de dados (AIPD), pelo Relatório da Comissão Técnica Multidisplinar para a Melhoria da Prevenção e Combate à Violência Doméstica e pela Proposta de protocolo de governação formal entre entidades.

3. 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, alínea b) do n.º 3 do artigo 58.º e 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 da Lei 58/2019, de 8 de agosto, que executa na ordem jurídica interna o RGPD.

II. Contexto

4. A Lei n.º 112/2009, de 16 de setembro, que estabelece o regime jurídico aplicável à prevenção da violência doméstica e à proteção e assistência às suas vítimas, prevê, no artigo 37.º-A, a existência de uma base de dados de violência contra as mulheres e violência doméstica estabelecendo, no número 8 daquele artigo, que determinadas matérias são «objeto de regulamento próprio, submetido a parecer prévio da Comissão Nacional de Proteção de Dados».

5. Através do Parecer/2020/31, de 23 de março de 2020, a CNPD teve oportunidade de se pronunciar, a solicitação do Governo, sobre o anteprojeto da Proposta de Lei de alteração à Lei n.º 112/2009, de 16 de setembro, através do qual se pretendia proceder à alteração da designação da «Base de Dados de violência doméstica» para «Base de Dados de Violência contra as mulheres e Violência Doméstica» (BDVMVD) e proceder à positivação do seu regime jurídico.

6. A CNPD foi igualmente chamada a pronunciar-se, já em sede de processo legislativo parlamentar, sobre a Proposta de Lei n.º 28/XIV/1.ª (GOV), para alteração do regime jurídico da Base de Dados de Violência Doméstica (BDVD), na sequência daquela proposta de lei, tendo na altura emitido o Parecer/2020/65, de 8 de junho de 2020.

7. Com a aprovação daquela alteração, a referida base passou a conter um conjunto mais alargado de dados transmitidos por mais entidades—fonte, bem como uma maior amplitude ao nível das tipologias de dados passíveis de ser objeto de tratamento, passando a designar-se Base de Dados de Violência contra as Mulheres e Violência Doméstica (BDVMVD).

8. A Proposta de Regulamento em análise visa dar cumprimento ao preceituado no número 8 do artigo 37.º-A da Lei n.º 112/2009, de 16 de setembro, que prescreve que são objeto de regulamento próprio, submetido a parecer da Comissão Nacional de Proteção de Dados, as seguintes matérias: «a) O elenco concreto de crimes abrangidos pela BDVMVD; b) O modelo de dados a comunicar segundo a fonte; c) As formas de comunicação dos dados, privilegiando-se, sempre que possível, a implementação de soluções automáticas que visem a interoperabilidade entre sistemas informáticos; d) Os perfis de acesso; e) Os prazos de conservação para os dados; f) As regras e medidas de segurança a implementar, tendo em vista a proteção dos dados pessoais e que se mostrem necessárias em resultado da avaliação de impacto sobre a proteção de dados."»

III. Análise

i. Âmbito e finalidades

9. A Lei n.º 112/2009, de 16 de setembro estabelece, no n.º 1 do artigo 2.º, as finalidades da BDVMVD. Assim, prevê-se que o tratamento dos dados efetuado naquela base de dados se reporta a casos em que foi iniciado o procedimento criminal no âmbito da violência contra as mulheres e ou violência doméstica, tendo como finalidades: «a) Promover um conhecimento aprofundado ao nível da violência contra as mulheres e violência doméstica, contribuindo para o desenvolvimento da política criminal, da política de segurança e das demais políticas públicas especificamente direcionadas para a prevenção e o combate a estas formas de violências; b) Obter uma visão global e integrada em matéria de homicídios e de outras formas de violência contra as mulheres e violência doméstica, através do tratamento e cruzamento de informação proveniente do sistema de justiça penal e que englobe dados com origem noutros setores, e que viabilize a análise da trajetória dos casos». Tal preceito é replicado no n.º 1 do artigo 2.º da Proposta de Regulamento.

10. Para o recorte das finalidades deve, ainda, atender-se ao preceituado no n.º 7 do artigo 37.º-A da referida lei, quando nessa sede se afirma que «o tratamento de dados no âmbito da BDVMVD destina-se a permitir a análise da trajetória de casos através da integração de dados constantes nas diversas fontes, mediante a interconexão entre a BDVMVD e as bases onde se encontrem os dados referidos no n.º 3, por referência ao NUIPC e aos dados estritamente necessários à identificação das vítimas e denunciados, com exclusão de quaisquer outros dados pessoais» (sublinhado nosso).

11. Explicitando a finalidade do «tratamento e análise de trajetórias de casos», afirma-se no número 2 do artigo 2.º da Proposta de Regulamento, que «o tratamento e análise das trajetórias dos casos [...] visam a obtenção de informação estatística sobre a violência contra as mulheres e violência doméstica, contribuindo para o delineamento/aperfeiçoamento de políticas e estratégias para a sua prevenção e combate, e a obtenção de elementos essenciais a uma visão mais completa e integrada de casos concretos, apoiando nesta última vertente a implementação das políticas criminais e de segurança interna.» (sublinhado nosso).

12. Se assim é, e atentas as finalidades expendidas na lei, a pretensão vertida na Proposta de Regulamento, de permitir esse acesso para conhecimento de casos anteriores em que estejam envolvidas as mesmas vítimas ou os mesmos agentes parece relevar mais para efeitos de investigação criminal do que para efeitos da definição de uma política criminal, principalmente se considerarmos a forma como estão atribuídos os perfis de acesso à informação, e o facto de para obter estatísticas não ser necessário aceder aos dados pessoais que resultam da ligação entre casos em que coincidam vítimas e/ou agentes. Tal não encontra uma correspondência total com a lei que legitima os tratamentos na BDVMVD, pelo que se estará, por portaria, a ampliar os termos daquela. Além disso, afigura-se claramente excessiva – e sem respaldo na lei – a referência a políticas de «segurança interna» num contexto de violência doméstica.

13. Faz-se notar que, embora as finalidades indicadas no n.º 1 do artigo 2.º da Proposta de Regulamento repliquem as finalidades explicitadas nas alíneas a) e b) do n.º 2 do artigo 37.º-A da Lei n.º 112/2009, de 16 de setembro, o texto do Regulamento omite parte relevante do preceituado na lei. De facto, na lei se diz, de forma clara, que o tratamento de dados efetuado no âmbito da BDVMVD tem como «finalidades exclusivas» as previstas nas alíneas a) e b) do número 2 do artigo 37.º-A.

14. Tal não é despiciendo porquanto, para que um tratamento de dados pessoais seja lícito é necessário que se verifique, pelo menos, um dos fundamentos de licitude previstos nos artigos 6.º, 9.º ou 10.º do RGPD, consoante o caso.

15. Ora, a determinação do fundamento de licitude no caso concreto deve ter em consideração, nomeadamente, os vários princípios previstos no artigo 5.º do RGPD, desde logo os princípios da responsabilidade, lealdade e da limitação das finalidades.

16. Ou seja, para determinar se um determinado tratamento de dados é lícito, é necessário identificar previamente as finalidades, para poder avaliar se aquele tratamento excede, ou não, o que é necessário para a sua prossecução. No caso concreto da BDVMVD, o fundamento de licitude reside na lei, na qual se inscrevem as finalidades de forma determinada e explícita.

17. Assim, apenas será lícito o tratamento de dados na BDVMVD para os fins inscritos naquela lei, pelo que seria desejável que também do Regulamento constasse a referência a «finalidades exclusivas», assim salvaguardando a taxatividade das finalidades de tratamento de dados que a lei prevê.

18. A este respeito, diz-se na AIPD que «as finalidades resultam do Artigo 37.º-A da Lei n.º 112/2009, de 16 de setembro, na sua redação atual [...] bem como da lei n.º 59/2019, de 8 de agosto» e que «[a] lei n.º 34/2009, de 14 de junho permite o intercâmbio de dados no sistema judicial com outros sistemas, tendo que se entender a remissão que é feita para a Lei de Proteção de Dados (já revogada) como sendo hoje feita para o RGPD, para a Lei Nacional de Execução (Lei n.º 58/2019, de 8 de agosto) e, no caso do tratamento efetuado para efeitos de prevenção, investigação, deteção e repressão de infrações penais (matéria da Diretiva UE 2026/680, de 27 de abril) para a Lei n.º 59/2019, de 8 de agosto».

19. E identifica-se como fundamento de licitude para o tratamento de dados, «o cumprimento de obrigação legal (vide alínea c) do artigo 6.º do RGPD, considerando o cumprimento do artigo 37.º-A da Lei n.º 112/2009, de 16 de setembro, com as alterações introduzidas pela Lei n.º 57/2021, de 16 de agosto, bem como a Lei n.º 58/2019, de 8 de agosto (Lei de Execução do RGPD) e, no caso de tratamento efetuado para efeitos de prevenção, investigação, deteção e repressão de infrações penais (matéria da Diretiva EU 2016/680 de 27 de abril) a Lei n.º 59/2019, de 8 de agosto».

20. Ora, ao tratamento efetuado pela SGMAI, enquanto responsável pelo tratamento, não se aplica a Lei n.º 59/2019, de 8 de agosto, uma vez que esta apenas «respeita ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública», categoria na qual a SGMAI não se enquadra.

21. Também na AIPD é dito que o tratamento se funda em «obrigação jurídica», em «interesses legítimos» e «interesse público ou autoridade pública» (pág. 5).

22. No entanto, tal como previsto na parte final do n.º 1 do artigo 6.º do RGPD, o fundamento de licitude previsto na alínea f) daquele número e artigo (interesses legítimos) não se aplica ao tratamento de dados efetuado por uma autoridade pública na prossecução das suas atribuições, pelo que não poderá este fundamento ser considerado no caso em análise.

23. No caso do tratamento de dados no âmbito da BDVMVD, o fundamento de licitude reside na lei - mais concretamente, na Lei n.º 112/2009, de 16 de setembro - e nos precisos termos em que aquela enquadra o seu regime (artigos 6.º, 9.º e 10.º do RGPD).

CNPD
Comissão Nacional
de Proteção de Dados

ii. Crimes e casos a abranger

24. A Lei n.º 112/2009, de 16 de setembro, determina na alínea a) do n.º 8 do artigo 37.º-A que seja previsto em regulamento o elenco que aquela lei prevê de forma genérica no número 4, ao estabelecer que a «BDVMVD abrange as situações de maus tratos cometidos no contexto de violência doméstica, configurando o crime de violência doméstica previsto no artigo 152.º do Código Penal (CP) ou outro crime cometido contra uma das pessoas previstas no n.º 1 do mesmo artigo e que tenha moldura penal mais grave, incluindo, nomeadamente, homicídio, ofensa à integridade física grave e violação, e ainda outras situações não contidas nas anteriores, mas que se incluam na esfera da violência contra as mulheres, configurando, designadamente, crime de violação, mutilação genital feminina ou perseguição».

25. Constata-se, assim, que na redação atual a lei pretendeu alargar o âmbito dos crimes passíveis de tratamento na base de dados, não os circunscrevendo apenas ao crime de violência doméstica previsto no artigo 152.º do CP, independentemente de a vítima do crime ser homem ou mulher, mas também a crimes passiveis de configurar violência contra a mulher, dir-se-á, pelo facto de ser mulher.

26. Neste contexto, renova-se o entendimento da CNPD, vertido no Parecer/2020/31, de que o elenco de crimes abrangidos pela BDVMVD deveria constar da lei e não de portaria. Trata-se de uma questão substantiva, relativa ao âmbito de aplicação do próprio diploma e com reflexos no tratamento de dados que daí resulta. E, isto, não obstante o esforço de concretização tipológica de crimes que a lei veio a consagrar na sua redação atual e que a CNPD, de resto, reconheceu em anterior parecer, sendo que o catálogo extravasa os quadros da própria lei

27. A Proposta de Regulamento estabelece, no n.º 1 do artigo 3.º, as tipologias de crimes a abranger no tratamento. Trata-se de um catálogo extenso – compreendendo 34 tipos de crime – sendo que os dados a tratar ficarão condicionados aos critérios enunciados no n.º 5 do mesmo artigo: ser relativos a algum daqueles crimes na sua forma tentada ou consumada e, adicionalmente, tratar-se de crimes praticados contra uma das pessoas previstas no n.º 1 do artigo 152.º do CP, ou ser relativo a crime praticado contra vítima do sexo feminismo.

28. No que respeita à tipologia de crimes previstos na Proposta de Regulamento, a CNPD não pode deixar de assinalar que o objeto da Lei n.º 112/2009, de 16 de setembro, se mantém inalterado face à redação originária, não tendo sido modificado pela lei que introduziu alterações ao artigo 37.º-A, devendo ser objeto de uma leitura integrada.

29. Ora, nos termos do artigo 1.º, aquela lei «estabelece o regime jurídico aplicável à prevenção da violência doméstica e à proteção e à assistência das suas vítimas [de violência doméstica]», estando concretizado o

conceito de vítima neste contexto como sendo «a pessoa singular que sofreu um dano emocional ou moral , ou uma perda material, diretamente causada por ação ou omissão, no âmbito do crime de violência doméstica previsto no artigo 152.º do Código Penal, incluindo as crianças ou os jovens até aos 18 anos que sofreram maus tratos relacionados com exposição a contextos de violência doméstica» (alínea a) do artigo 2.º - sublinhado nosso).

30. Ora, as finalidades previstas no n.º 2 do artigo 37.º-A da Lei n.º 112/2009 não podem deixar de se acomodar àquele objeto, nem desconsiderar o conceito de vítima ali consagrado o qual, tal como se encontra gizado na lei, consagra um universo mais restritivo do que se pretende alcançar agora com a Proposta de Regulamento.

31. Assim sendo, não deverá ser suficiente, para integração na base de dados, que um dos crimes seja praticado contra uma mulher, mas que possa ser aferida uma relação com o contexto de violência doméstica, sob pena de violação do princípio da proporcionalidade e minimização do tratamento de dados pessoais, nas vertentes da necessidade e adequação previsto na alínea c) do artigo 5.º do RGPD.

32. Nota-se, neste contexto, uma incongruência legislativa interna que seria oportuno sanar, de forma a garantir o cumprimento dos princípios do RGPD e, nomeadamente, o princípio da licitude do tratamento dos dados neste âmbito.

33. Por seu turno, o tratamento de dados deve respeitar o princípio da adequação. Ora, o facto de se admitir no n.º 4 do artigo 3.º que «nos casos em que as entidades-fonte utilizem notação criminal que inviabilize a desagregação de registos segundo cada um dos crimes previstos no n.º 1, a comunicação dos dados, até que seja implementada solução que permita tal identificação, pode ser realizada com base na notação criminal em uso e mais próxima da realidade que se pretende captar» suscita duas questões: por um lado, parece deixar na discricionariedade da entidade fonte realizar, ou não, a inserção desses dados e, por outro, permite a inserção de dados que podem estar em desconformidade com a tipologia de crimes, alimentando a base com dados pouco corretos o que terá como consequência a não adequação dos mesmos ao tratamento em causa. Tanto mais que não se prevê um mecanismo que permita reclassificar a informação quando a entidade fonte venha a ter uma notação conforme à da tipologia prevista na lei e na Proposta de Regulamento.

iii. Tipologia de dados a abranger

34. A Proposta de Regulamento indica que o tratamento abrange as seguintes tipologias: ocorrências registadas pelos órgãos de polícia criminal, respetivas avaliações de risco, detenções efetuadas e medidas cautelares de polícia adotadas; decisões sobre atribuição de estatuto de vítima; medidas de proteção à vítima adotadas no início do procedimento ou no seu decurso, seja por via dos órgãos de polícia criminal, , do tribunal,

designadamente o acompanhamento da vítima por técnico ou pessoa da sua confiança dos atos processuais, acompanhamento policial para retirada de bens da residência por parte da vítima, recurso a declarações para memória futura e aplicação de teleassistência; recurso a estrutura da Rede Nacional de Apoio às Vítimas de Violência Doméstica (RNAVVD); processos de promoção dos direitos e proteção da criança e do jovem em perigo e existência de procedimentos contemporâneos relacionados com o exercício das responsabilidades parentais; medidas de coação aplicadas; decisões europeias de investigação e decisões europeias de proteção, resultados dos processos ao longo das fases de inquérito, instrução criminal, julgamento e recurso, situações de reclassificação dedo crime inicialmente registado, penas principais e acessórias e medidas de segurança a inimputáveis; decisões condenatórias e elementos sobre a execução das condenações e penas acessórias aplicadas à pessoa agressora e cumprimento do direito da vítima de ser informada sobre a libertação ou evasão da pessoa detida, acusada, pronunciada ou condenada; identificação de processos com análise retrospetiva de homicídio em contexto de violência doméstica e indemnização atribuída às vítimas (cf. n.º 1 do artigo 3.º da proposta, que coincide com a tipologia prevista no número 3 do artigo 37.º-A da Lei n.º 112/2009).

iv. Entidades fonte de informação

35. A Lei n.º 112/2009, de 16 de setembro, elenca, no número 5 do artigo 37.º-A, as entidades fonte dos dados tratados na BDVMVD que são a Guarda Nacional Republicana (GNR); a Polícia de Segurança Pública (PSP); a Polícia Judiciária (PJ); o Sistema Informático de suporte à atividade dos tribunais, gerido pelo Instituto de Gestão Financeira e equipamentos de Justiça, I.P. (IGFEJ), a Procuradoria-Geral da República (PGR); a Comissão para a Cidadania e a Igualdade de Género (CIG) – sendo que neste caso os dados transmitidos a esta entidade serão sempre anonimizados; a Comissão Nacional de Promoção de Direitos e Proteção das Crianças e Jovens (CNPDPCJ); a Direção Geral de Reinserção e Serviços Prisionais (DGRSP); e a Comissão de Proteção de Vítimas de Crimes (CPVC).

36. O artigo 6.º da Proposta de Regulamento transpõe para o seu texto aquela informação, clarificando, no entanto, que o IGFEJ, I.P. intervém na «condição de subcontratante por conta dos responsáveis pelo tratamento, em conformidade com o disposto na Lei n.º 34/2009, de 14 de julho, a qual estabelece o regime jurídico aplicável ao tratamento de dados referentes ao sistema judicial».

37. A este respeito, faz-se notar que no elenco das fontes previstas na Proposta de Regulamento se omitiu a Procuradoria-Geral da República que consta da alínea e) do n.º 5 do artigo 37.º-A da Lei n.º 112/2009, sem que fique percetível a razão de tal eliminação.

v. Responsabilidade pelo tratamento

38. A Proposta de Regulamento indica, no artigo 5.º, que a entidade responsável pelo tratamento dos dados da BDVMVD é a Secretaria-Geral do Ministério da Administração Interna, o que se encontra conforme o preceituado no n.º 1 do artigo 37.º-A da Lei n.º 112/2009, de 16 de setembro.

39. No entanto, no n.º 8 do artigo 3.º, fala-se em «entidades-fonte corresponsáveis pela BDVMVD».

40. Acresce que o pedido vem instruído com vários anexos, entre os quais uma Proposta de «Protocolo de modelo de governação do tratamento de dados pessoais entre entidades fonte da Base de Dados de Violência contra as Mulheres e Violência Doméstica e a Secretaria-Geral do Ministério de Administração Interna», doravante "Protocolo".

41. Embora o texto do Protocolo seja omisso a este respeito, parece pretender-se regular um acordo a celebrar entre as várias entidades-fonte e a SGMAI nos termos do artigo 26.º do RGPD, na premissa de que todos são responsáveis conjuntos. A ideia de corresponsabilidade é reiterada na AIPD (pág. 19), ao afirmar que «se celebrará um acordo de responsabilidade conjunta de tratamento de dados [...] pelas diferentes entidades fontes, que são, nos termos do RGPD, responsáveis conjuntos pelo tratamento».

42. Ainda, consagra-se no Protocolo que se pretende, através da sua celebração, nomeadamente, proceder à definição da «repartição das responsabilidades relativas a tratamentos de dados pessoais realizadas no âmbito do projeto da Base de dados de Violência contra as Mulheres e Violência Doméstica, pelas Partes que subscrevem o acordo» (artigo Primeiro) e, ainda, que as mesmas Partes «determinam em conjunto a licitude para os tratamentos de dados pessoais [...]» (artigo Quarto).

43. O artigo 26.º do RGPD prevê, de facto, que «quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são corresponsáveis» e, ainda, que estes devem determinar entre si as respetivas responsabilidades pelo cumprimento do RGPD (n.º 1 do artigo 26.º). Porém, esta norma não pode ser aplicada ao caso em análise, uma vez que a Lei n.º 112/2009 atribui responsabilidade única à SGMAI, o que esvazia o clausulado do acordo, assente na premissa da responsabilidade conjunta das partes.

44. Não obstante as observações que acima se deixaram expressas, a CNPD não pode deixar de assinalar alguns aspetos do Protocolo que constitui um dos anexos à Proposta de Regulamento.

45. Desde logo, é dito no Artigo Quarto que «as Partes determinam em conjunto a licitude para os tratamentos de dados pessoais de acordo com as possibilidades previstas no artigo 6.º do RGPD e do artigo 9.º, tratando-se de dados de Categorias Especiais».

46. No entanto, a licitude do tratamento não pode ser determinada pelas partes. De facto, ao contrário do que naquela sede se afirma, não se trata de as partes determinarem a licitude de entre as «possibilidades» previstas no artigo 6.º do RGPD e do artigo 9.º porquanto, no caso concreto, o fundamento reside necessariamente em diploma legal, tal como resulta dos termos conjugados dos artigo 6.º, 9.º do RGPD, como se refere no Protocolo e ainda, nos termos do artigo 10.º do RGPD, uma vez que se trata de um tratamento de dados pessoais relacionados com condenações penais e infrações.

47. Suscitam-se igualmente dúvidas quanto ao preceituado no n.º 5 do Artigo Quinto, na parte em que se estabelece que «cada Parte adota as medidas técnicas [e] organizativas adequadas a assegurar o apagamento ou a anonimização de todas as suas cópias dos dados no final do período de conservação determinado», não ficando claro a que cópias se refere a cláusula.

48. Por outro lado, no mesmo Artigo Quinto pretende-se regular por Protocolo as obrigações das Partes quanto ao tratamento de dados pessoais, o qual deve limitar-se ao «necessário para cada finalidade específica, nomeadamente quanto à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, à sua acessibilidade e ao seu prazo de conservação». Ainda, o Artigo Sétimo estabelece o dever de colaboração entre as Partes no que respeita à comunicação dos pedidos de exercício de direitos por parte dos titulares dos dados. Sem embargo de tais obrigações deverem ser reguladas, o instrumento agora em análise não se adequa à realidade que pretende regular, por partir de uma premissa inexistente - a da responsabilidade conjunta das Partes no que tange à BDVMVD - o que preclude a análise da CNPD quanto ao seu clausulado e obrigaria à alteração do seu conteúdo.

vi. Prazo de conservação

49. Os prazos de conservação vêm restabelecidos no artigo 14.º da Proposta de Protocolo, deste modo:

50. No número 1 prevê-se que, sem prejuízo do regime previsto no número 2, os dados constantes da BDVMVD são conservados pelo período máximo de 10 anos a partir da data do arquivamento do processo-crime ou do trânsito em julgado da decisão judicial, desde que neste período não existam novas denúncias envolvendo os mesmos intervenientes (vítimas/suspeitos) ou o incumprimento de pena ou medida judicial.

51. Esta solução suscita algumas observações: por um lado, não determina, em caso de haver novas denúncias ou de o arguido se furtar ao cumprimento da pena, qual o prazo de conservação dos dados relativamente àquele processo. Nomeadamente, se o prazo se repristina, recomeçando a sua contagem por mais 10 anos em virtude dos novos factos e de cada vez que houvesse um facto novo.

52. Tal solução permitiria, na prática, o estabelecimento de prazos mais longos dos que alguns dos prazos de conservação legalmente previstos para os sistemas de informação das polícias - que recolheram os dados e não poderão mantê-los para além desse prazo determinado- e, até, do prazo permitido para manutenção daqueles dados no registo criminal, o que perverteria, por completo, a razão de ser do estabelecimento de prazos de conservação máximos naquele registo.

53. Assim, verifica-se, por um lado, que os prazos inscritos nesta norma poderão ser excessivos e, por outro, a necessidade de compatibilizar com os prazos estabelecidos para as outras bases de dados e as finalidades para as quais tais prazos foram estabelecidos.

54. No número 2 daquele preceito prevê-se que os dados relativos a pessoas suspeitas ou arguidas (neste caso, por interpretação conjugada com o n.º 1, apenas as arguidas que não se encontrem já a cumprir pena) são conservados pelo prazo máximo correspondente ao prazo de prescrição do respetivo procedimento criminal, nos mesmos termos do artigo 118.º do Código Penal.

55. Nada é dito, no entanto, quanto ao prazo de conservação dos dados das vítimas neste caso.

56. Em ambas as situações, fará sentido diferenciar os prazos de conservação dos dados relativos aos infratores e às vítimas. Quanto a estas, seria de ponderar uma solução em que os dados pudessem ser mantidos em registo informático durante algum tempo com a finalidade de reposição de registo indevidamente cancelado ou retirado, por questões de segurança, mas apenas acessível nestas circunstâncias, à semelhança do que ocorre na lei de identificação criminal.

57. É dito no número 3 que, findos aqueles prazos, os dados pessoais serão submetidos a um processo de anonimização que impeça a identificação de casos ou pessoas concretas. No entanto, não são concretizados os detalhes técnicos deste processo. Pela descrição da atribuição de perfis, é possível perceber que o nível de acesso mais alto será atribuído a quem vai gerir a ferramenta de limpeza de registos após o término do prazo de retenção e processo de anonimização, mas é dito que não terão acesso à informação não anonimizada nem à possibilidade de consulta de processos.

vii. Protocolos de transmissão de dados

58. A Proposta de Regulamento explicita, no artigo 7.º, o Modelo de transferência de dados segundo a entidade-fonte de informação, matéria mais particularmente descrita nos protocolos a celebrar entre entidades, que constituem anexos à Proposta. A tipologia de dados mostra-se adequada às finalidades prosseguidas.

59. Na lista de entidades-fonte consta a SGMAI/EARHVD, com a indicação de que os dados a transmitir pela SGMAI à Equipa de Análise Retrospetiva de Homicídios em Violência Doméstica (EARHVD) são a «identificação

de processos com análise retrospetiva de homicídio em contexto de violência doméstica». Tal afirmação vem secundada por uma nota de rodapé (1) da qual consta que se entende ser desnecessária a celebração de um protocolo de comunicação de dados a celebrar entre a SGMAI e a EARHVD para efeitos da BDVMVD, uma vez que nos relatórios publicados por aquela Equipa consta a identificação do NUIPC e cada caso revisto, pelo que essa informação é pública. No entanto, verifica-se que a EARHVD não divulga o NUIPC dos casos por si tratados, o que se aplaude porquanto o NUIPC é um dado que, embora não identifique de imediato uma pessoa, permite a sua identificação sendo, por isso, nos termos da alínea 1) do artigo 4.º do RGPD um dado pessoal cuja proteção fica ao abrigo da legislação de proteção de dados, devendo ser objeto da mesma proteção que os demais.

IV. Medidas técnicas e de segurança

60. Analisada a Proposta de Regulamento e documentação anexa, verifica-se que está assegurado um conjunto de medidas de segurança adequadas ao funcionamento da BDVMVD, havendo, no entanto, alguns aspetos a carecer de revisão.

61. Procede-se à separação de repositórios de informação para fins estatísticos e operacionais, permitindo eliminar dados pessoais do repositório estatístico. Tal segregação é realizada com recurso a instâncias diferentes no moto de base de dados, e é uma separação lógica.

62. É referido que a informação que é vertida para o repositório estatístico não permite a identificação. No entanto, não é dito como é realizado o processo, nem são apresentados exemplos que permitam chegar a uma conclusão quanto ao processo. É declarada a intenção de que os dados que serão guardados para efeitos estatísticos sejam de facto anonimizados sem nenhum dado pessoal que possa identificar cidadão, mas também a este nível a informação é muito insuficiente para que a CNPD possa emitir pronúncia quanto à sua adequação.

63. Ainda, é dito que se procede à atribuição de perfis de acesso com base no nível necessário de acesso à plataforma de acordo com a função e nível de acesso à informação.

64. Os quatro níveis de acesso vêm descritos no artigo 11.º da Proposta de Regulamento e a págs. 19 e 20 da AIPD, do seguinte modo:

a) Perfil 1- é atribuído a utilizadores credenciados para o efeito, da GNR, da PSP, da PJ, do Ministério Público e da SGMAI, com capacidade de extração de dados (anonimizados) para efeitos de tratamento e análise estatística e monitorização dos registos comunicados à BDVMVD.

b) Perfil 2 - atribuído a utilizadores, credenciados para o efeito, da GNR, da PSP, da PJ e do Ministério Público (…)

c) Perfil 3- atribuído aos aprovisionadores da GNR, da PSP, da PJ e do Ministério Público que gerem a atribuição do acesso aos respetivos utilizadores da BDVMVD (…)

d) Perfil 4 - atribuído a utilizadores da SGMAI que efetuam a administração geral da BDVMVD. A sua intervenção será essencialmente na vertente informática (*ex. manutenção e backup*) e na gestão de acessos de utilizadores da SGMAI e dos utilizadores com perfil previsto na alínea anterior.

65. Está descrito que os utilizadores do perfil 1 acedem apenas a dados anonimizados, o mesmo não acontecendo com os utilizadores do perfil 2.

66. Quanto a estes, é percetível a preocupação com a minimização do acesso a informação sensível retornada nas pesquisas, obrigando que o acesso a mais detalhes a ser efetuado numa nova pesquisa.

67. É ainda dito na alínea b) do número 1 do artigo 11.º da Proposta de Regulamento, bem como na AIPD (pág. 19), que o perfil 2 é «atribuído a utilizadores, credenciados para o efeito, da GNR, da PSP, da PJ e do Ministério Público, que [...], para além de possuírem as permissões previstas no perfil 1, podem efetuar consultas, mediante a inserção do NUIPC, podendo aceder a informação mínima relativa a ocorrências anteriores ou outro tipo de registos contidos na BDVMVD envolvendo algum dos intervenientes da nova ocorrência, de modo a possibilitar a necessária articulação entre entidades tendo em vista um apuramento completo de informação sobre o caso, fator essencial para a sua gestão.".

68. Encontra-se ainda estabelecido nos termos conjugados daquela alínea e do número 2 do mesmo artigo, que o NUIPC constitui-se como o anotador chave que permite a consulta e acesso aos dados pessoais e que, sem prejuízo das situações em que a competência de investigação de uma determinada ocorrência for atribuída a entidade diferente da inicialmente notadora, casos em que os dados deixam de estar acessíveis à entidade inicialmente notadora, passando a estar acessíveis apenas à entidade para a qual a competência foi transferida - os utilizadores dos OPC apenas possuem permissões para efetuar extração de dados e consultas relativas ao NUIPC referentes à sua entidade notadora. É ainda dito que estes utilizadores recebem alertas quando existam ocorrências que envolvam algum dos intervenientes, seja a vítima ou o suspeito (crê-se que igualmente quando seja arguido) numa ocorrência registada pela entidade anotadora, sendo indicada como finalidade destes alertas apoiar o levantamento de todas as ocorrências anteriores envolvendo tais intervenientes, e apoiar a recolha de informação para a gestão dos casos.

69. Isto quer dizer que para níveis de acesso mais baixo, o primeiro resultado apenas retorna uma lista de processos, sendo necessário para aceder a um determinado processo, repetir a pesquisa por esse identificador para aceder aos elementos que nele constam.

70. Face ao que é dito, o que está a realizar-se não será exatamente a «análise de trajetória de casos», como disposto nas finalidades previstas na Lei n.º 112/2009, de 16 de setembro, mas a análise de trajetória de pessoas em relação à sua intervenção noutros casos. Não se discute a necessidade de tais instrumentos para efeitos de análise estatística, nem a conveniência sentida pela investigação criminal em ter numa base de dados toda esta informação disponível, mas relembra-se que o critério, em sede de proteção de dados não pode ser o da conveniência. Assim, deve reponderar-se a necessidade da manutenção desta base de dados a par de outras de que constem os mesmos dados, devendo o Regulamento estar adequado à lei que visa regulamentar, pelo que seria desejável uma alteração legislativa que pudesse acomodar o regime que se pretende agora estabelecer através da Portaria.

71. Verifica-se que o acesso à plataforma é efetuado com recurso a múltiplos fatores de autenticação, de acordo com o previsto no n.º 3 do artigo 15.º da Proposta de Regulamento. Porém, não é detalhado o modo de implementação do segundo fator/múltipla autenticação no caso dos utilizadores do MAI.

72. No que respeita a alguns utilizadores externos ao Ministério da Administração Interna (MAI), será necessário recorrerem ao mecanismo Autenticação.Gov, que consiste na utilização do Cartão do Cidadão ou Chave Móvel Digital para efetuarem o acesso à plataforma.

73. Por outro lado, quanto à possibilidade de utilização de mecanismos de autenticação individuais Cartão de Cidadão (CC) e Chave Móvel Digital (CMD) como instrumento para desempenhar os deveres profissionais a CNPD reitera as reservas expendidas no Parecer/2023/91.

74. De facto, a utilização daqueles meios por parte de 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 RGPD.

75. Porém, verifica-se que não existe qualquer norma legal que imponha, ou possibilite que se exija a utilização do CC ou da CMD como instrumento de trabalho. Do mesmo modo, não é possível enquadrar este tratamento de dados pessoais destes utilizadores na necessidade de cumprimento de uma obrigação jurídica, nem no interesse legítimo do responsável pelo tratamento – neste caso a SGMAI – (cf. alíneas c) e f) do artigo 6.º do RGPD e parte final do n.º 1 do artigo 6.º do RGPD).

76. Tão pouco pode ser convocado, no caso, o consentimento como fundamento de licitude deste tratamento. De facto, 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,

[1] Disponível em www.cnpd.pt.

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 constitui uma «manifestação de vontade livre, específica, informada e inequívoca, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento».

77. Ora, a situação de dependência em que se encontram os trabalhadores não permitem, à partida, a formação livre dessa vontade. Se assim é, tem de ficar demonstrada a existência de condições de liberdade para a manifestação dessa vontade. Desde logo, pela existência de alternativa.

78. A 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, deve poder garantir-se ao utilizador um meio alternativo que permita a autenticação sem recorrer aos dados constantes do seu documento pessoal de identificação.

79. Uma vez que a formação livre da vontade depende da existência de alternativa daqueles meios, porque qualquer deles supõe a utilização livre e voluntária, o tratamento de dados pessoais que resulte da utilização do CC ou da CMD para estes fins não será lícita.

80. Por essa razão deverá garantir-se que, à semelhança do que ocorre com a certificação dos trabalhadores da SGMAI envolvidos na BDVMVD, mecanismos alternativos para a autenticação dos profissionais, sem que daí decorra qualquer ónus ou encargo para o trabalhador.

81. Além de que, o recurso ao mecanismo Autenticação.Gov, que consiste na utilização do Cartão do Cidadão ou Chave Móvel Digital para permitir o acesso à plataforma, coloca o acesso de alguns utilizadores na dependência de um serviço externo à gestão e controlo da SGMAI.

82. As comunicações entre os sistemas de cada entidade e o SGMAI utilizam mecanismos de encriptação e segurança dedicados e é dito que na comunicação entre a aplicação e o servidor aplicacional é utilizado HTTPS/TLS1.2 (mínimo)", que demonstra grau de segurança adequado.

83. Ainda no que respeita à comunicação de dados entre os sistemas de informação de cada entidade e a BDVMVD, refere-se que esta é efetuada com recurso a uma *RestAPI*. Tais APIs REST permitem implementar sistemas de autenticação e autorização mais robustos, com uso de tokens de acesso. Embora não são especificados os detalhes técnicos da sua implementação, a adoção da tecnologia de comunicação entre os diversos sistemas afigura-se adequada para estes cenários.

84. Prevê-se que os dados pessoais sejam são encriptados na Base de Dados com encriptação simétrica e que «será utilizado um aplicativo que permitirá a encriptação de dados através da encriptação simétrica e permanente dos campos de dados por forma a assegurar a proteção dos dados de identificação das vítimas" (n.º 9 do artigo 15.º). Tal traduz-se não numa anonimização mas numa pseudonimização, garantindo que os técnicos que poderão necessitar de acesso aos dados para efeitos de manutenção não tenham acesso visível do seu conteúdo, e minimizando o risco em caso de comprometimento do acesso à base de dados. No entanto, desconhecendo a CNPD o protocolo de encriptação, não poderá pronunciar-se sobre a adequação do mesmo àquela função.

85. Existem mecanismo de auditoria de acessos (n.º 5 do artigo 15.º), estando estabelecido que a BDVMVD conterá um módulo de Auditoria que irá rastrear todas as operações realizadas por qualquer utilizador que aceda ao sistema, independentemente do seu perfil de acesso e, desde o momento em que efetua a autenticação no sistema até ao momento que sai do mesmo. Este rastreamento irá incidir permitirá aferir que operação foi realizada, quando foi realizada e por quem foi realizada. De forma a permitir a monitorização eficaz, os perfis a atribuir devem corresponder a utilizadores nominais, devendo a SGMAI deve manter uma lista atualizada dos utilizadores que em cada momento estejam autorizados a proceder ao tratamento de dados em qualquer das suas operações (alínea 2 do artigo 4.º do RGPD).

86. A existência de mecanismos que permitam uma auditoria aos acessos efetuados que acedam a dados pessoais, permite detetar possíveis falhas do sistema ou comportamentos de acesso abusivo a dados pessoais que, não se tratando de uma medida de prevenção, permite, no entanto, detetar falhas para que possam ser corrigidas mais rapidamente.

87. Existem outros aspetos que deverão ser tidos em consideração.

88. Assim, no número 2 do artigo 8º é definido um método alternativo temporário até à implementação do mecanismo automatizado por parte da CPVC à BDVMVD. Este método consiste no envio de um documento não editável assinado digitalmente, cuidado que garante a integridade da informação. No entanto, não se encontra definido qual o método utilizado para a transferência do referido ficheiro. Assim, deverá ser acautelado que o envio deste ficheiro cumpre analogamente os critérios definidos para a transmissão de informação do método principal, mais concretamente:

a) Não ser enviado em comunicações não encriptadas;
b) Não ficar armazenada cópia no mecanismo de envio após o envio ser concluído;
c) Ser eliminado após a sua integração com sucesso na BDVMVD;

d) Se enviado por mecanismo de comunicação não dedicado para o efeito, que não disponha de mecanismo nativo de proteção da informação transmitida, cifrar a informação no documento.

89. Assim, recomenda-se que sejam revistos e densificados na Portaria estes aspetos, em obediência ao preceituado no artigo 5.º do RGPD, nomeadamente quanto ao respeito pelo princípio da confidencialidade e da integridade dos dados

V. Conclusão

Em consequência do atrás expendido e com os fundamentos expostos, a CNPD recomenda, entre outras medidas:

a) Rever os fundamentos de ilicitude considerados na Proposta de Regulamento;

b) Reponderar os critérios de inserção de dados pessoais, por referência ao elenco de crimes, adequando-os aos critérios previstos na Lei;

c) Revisão do texto do Protocolo no que respeita à consideração das entidades fonte como corresponsáveis da BDVMVD;

d) Sejam reponderados os prazos de conservação dos dados na BDVMVD antes da anonimização, bem como as condições de salvaguarda em que os dados são conservados;

e) Sejam disponibilizados aos trabalhadores meios alternativos à autenticação através de Cartão de Cidadão e Chave Móvel Digital;

f) Sejam robustecidas as características do sistema, tendo em consideração o acima indicado;

g) No que respeita ao artigo 9.º, sugere-se que em vez de «dados pessoais», se inscreva «categorias de dados pessoais» por ser este o conteúdo normativo ali previsto.

Aprovado na reunião de 21 de março de 2024

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**
Data: 2024.03.21 20:28:45+00'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

CARTÃO DE CIDADÃO