

PARECER/2026/4

I. Pedido

1. O Gabinete do Secretário de Estado Adjunto e da Justiça solicitou em 03 de dezembro de 2025 à Comissão Nacional de Proteção de Dados (CNPd) a emissão de parecer sobre o Projeto de Portaria que regula as comunicações eletrónicas entre a GNR e PSP com os tribunais e o Ministério Público (doravante Projeto de Portaria).
2. O pedido de parecer não veio instruído com qualquer estudo de impacto sobre a proteção de dados pessoais.
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 pelo n.º 4 do artigo 36.º, assim como pela alínea c) do n.º 1 do artigo 57.º e a alínea b) do n.º 3 do artigo 58.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 LERGD).

II. Análise

i) O quadro político-constitucional

4. A Constituição da República portuguesa (CRP) no seu registo normativo sobre os direitos, liberdades e garantias estabelece os direitos fundamentais à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1), bem como à autonomia informativa e à proteção dos dados pessoais (artigo 35.º, n.º 1 e 2).
5. Trata-se de matéria da competência legislativa exclusiva da Assembleia da República, salvo autorização concedida pela mesma ao Governo, e daí designar-se como reserva relativa de competência legislativa (artigo 165.º, n.º 1, alínea b) CRP).
6. Por sua vez, a CRP ao consagrar no artigo 112.º o quadro supralegal dos atos normativos, estabelece no n.º 1 que “São atos legislativos as leis, os decretos-leis e os decretos legislativos regionais”, acrescentando no n.º 6 que “Os regulamentos do Governo revestem a forma de decreto regulamentar quando tal seja determinado pela lei que regulamentam, bem como no caso de regulamentos independentes” e o n.º 7 que “Os regulamentos devem indicar expressamente as leis que visam regulamentar ou que definem a competência subjetiva e objetiva para a sua emissão”.
7. Mais adiante no artigo 199.º da CRP, mediante a epígrafe “Competência legislativa”, estatui no seu proémio e na alínea c) que “Compete ao Governo, no exercício de funções administrativas: [f]azer os regulamentos necessários à boa execução das leis”.

8. O Código de Procedimento Administrativo (Decreto-Lei n.º 4/2015, de 7 de janeiro – CPA) ao consagrar o conceito de regulamento administrativo no artigo 135.º, considera como tal “as normas jurídicas gerais e abstratas que, no exercício de poderes jurídicos, visem produzir efeitos externos”, acrescentando o artigo 136.º, n.º 1 que “A emissão de regulamentos depende sempre de lei habilitante”.

9. Deste modo, a portaria enquanto regulamento corresponde a um ato normativo ou ordenador emitido pelo Governo, através de um ou mais ministros, com o objetivo de disciplinar pormenorizadamente ou definir os procedimentos técnicos dos designados atos normativos ou legislativos, não podendo contrariar ou exceder a lei habilitante.

10. O presente Projeto de Portaria enumera as seguintes normas e leis habilitantes: “n.º 3 do artigo 2.º da Lei de Organização da Investigação Criminal, aprovada pela Lei n.º 49/2008, de 27 de agosto, nos n.º 3 do artigo 243.º, alínea c) do n.º 1 e alínea c) do n.º 3 do artigo 111.º do Código de Processo Penal, aprovado pelo Decreto-Lei n.º 78/87, de 17 de fevereiro, e no n.º 5 do artigo 132.º do Código de Processo Civil, aprovado pela Lei n.º 41/2013, de 26 de junho e na alínea a) do n.º 1 do artigo 37.º da Lei n.º 34/2009, de 14 de julho, manda o Governo, ..., o seguinte:”.

11. Para melhor compreendermos o sentido da habilitação legal deste Projeto de Portaria, passaremos a transcrever as normas em causa.

12. A Lei de Organização da Investigação Criminal refere no artigo 2.º, n.º 3 que “Os órgãos de polícia criminal, logo que tomem conhecimento de qualquer crime, comunicam o facto ao Ministério Público no mais curto prazo, que não pode exceder 10 dias, sem prejuízo de, no âmbito do despacho de natureza genérica previsto no n.º 4 do artigo 270.º do Código de Processo Penal, deverem iniciar de imediato a investigação e, em todos os casos, praticar os actos cautelares necessários e urgentes para assegurar os meios de prova” – neste segmento normativo não vem mencionado ou precisado qualquer dado pessoal identificativo.

13. O Código Processo Penal menciona no seu artigo 111.º, n.º 1 que “A comunicação dos actos processuais destina-se a transmitir: c) O conteúdo de acto realizado ou de despacho proferido no processo”, enquanto o n.º 3 estipula que “A comunicação entre serviços de justiça e entre as autoridades judiciais e os órgãos de polícia criminal efectua-se mediante: c) Ofício, aviso, carta, telegrama, telex, telecópia, comunicação telefónica, correio electrónico ou qualquer outro meio de telecomunicações: quando estiver em causa um pedido de notificação ou qualquer outro tipo de transmissão de mensagens”.

14. Mais adiante o invocado artigo 243.º, n.º 1, alínea c), consigna que “Sempre que uma autoridade judicial, um órgão de polícia criminal ou outra entidade policial presenciarem qualquer crime de denúncia obrigatória, levantam ou mandam levantar auto de notícia, onde se mencionem: Tudo o que puderem averiguar acerca da

identificação dos agentes e dos ofendidos, ..." – este segmento normativo optou por uma identificação genérica, sem precisar os dados pessoais a referenciar.

15. Mas também adita no n.º 3, que "O auto de notícia é obrigatoriamente remetido ao Ministério Público no mais curto de prazo, que não pode exceder 10 dias e vale como denúncia".

16. O Código Processo Civil (CPC) estipula no artigo 132.º, n.º 5 que "A forma de realização das comunicações eletrónicas entre tribunais, Ministério Público, oficiais de justiça, agentes de execução, administradores judiciais ou outros auxiliares da justiça é definida por portaria do membro do Governo responsável pela área da justiça, e as comunicações entre estes e pessoas singulares e coletivas privadas e públicas que auxiliem os tribunais no âmbito dos processos judiciais são efetuadas de acordo com o artigo 249.º, com as necessárias adaptações" – neste segmento normativo não se faz alusão a qualquer dado pessoal identificativo.

17. Porém, muito embora não venha referenciado como norma habilitante, o CPC através do artigo 498.º, n.º 1, menciona que "As testemunhas são designadas no rol pelos seus nomes, profissões e moradas e por outras circunstâncias necessárias para as identificar", enquanto no artigo 552.º, n.º 1, alínea a) alude à a identificação das partes, consignando o seu cumprimento "indicando os seus nomes, domicílios ou sedes e, sempre que possível, números de identificação civil e de identificação fiscal, profissões e locais de trabalho".

18. A Lei n.º 34/2009, de 14 de julho, que veio estabelecer o regime jurídico aplicável ao tratamento de dados referente ao sistema judicial, estipula no artigo 37.º, n.º 1, que "Para os efeitos previstos na lei, pode haver comunicação de dados, por meios electrónicos, com os seguintes sistemas: a) Dos órgãos de polícia criminal;". Mais uma vez, nada se indica quanto aos dados pessoais que são comunicados.

19. No entanto, mas sem se fazer referência como norma habilitante, a mesma Lei n.º 34/2009 faz uma menção às categorias de dados que podem ser recolhidos nos processos dos tribunais judiciais.

20. Assim, no seu artigo 6.º faz referência aos dados de identificação e contacto das partes principais e acessórias em processo civil e de trabalho [alínea c)], aos dados de identificação e contacto dos assistentes, lesados, ofendidos, partes civis, queixosos e vítimas, em processo penal [alínea d)], aos dados de identificação e contacto dos arguidos e autoridades recorridas, em processo contraordenacional [alínea e)], assim como aos dados de identificação e contacto das testemunhas [alínea f)]. Trata-se de uma identificação genérica das pessoas em causa, sem se precisar quais os respetivos dados pessoais.

21. O mesmo sucede quanto à categoria dos dados pessoais tratados nos inquéritos em processo penal [artigo 8.º, alíneas c) e d)], nos demais processos, procedimentos e expedientes da competência do Ministério Público [artigo 9.º, alíneas c) e d)] e na conexão processual no processo penal [artigo 10.º, alíneas a), b)].

22. Mas já ocorre uma precisão e ampliação desses dados pessoais quando esteja em causa a suspensão provisória do processo penal e no arquivamento em caso de dispensa de pena [artigo 11.º, alíneas a), b) e c)],

sendo ainda mais extenso no que concerne aos dados pessoais a integrar as ordens de detenção [artigo 13.º, alíneas a) a m)].

23. Como se pode constatar, as normas legais habilitantes invocadas fazem essencialmente referência ao *modo de comunicação* a realizar entre as autoridades policiais, os tribunais e o Ministério Público, mas já não quanto ao conteúdo a inserir dos respetivos dados pessoais, sendo que apenas o disposto no artigo 243.º, n.º 1, alínea c) do CPP, possibilita uma identificação genérica dos agentes e dos ofendidos.

24. Porém, noutras disposições legais que não são invocadas como normas habilitantes dos mencionados diplomas, que designaremos como *normas colaterais*, é que vêm referenciadas as distintas categorias dos dados pessoais identificadores, mas sempre com amplitudes distintas.

25. Por sua vez, o Projeto de Portaria ao referenciar o artigo 2.º, através da epígrafe “Comunicações eletrónicas”, consagra no n.º 6 que “Os dados pessoais constantes nas comunicações eletrónicas referidas nos números anteriores, para a identificação do interveniente, são, sempre que exista registo, o nome, género, data de nascimento, nacionalidade e naturalidade, filiação, estado civil, domicílio, contacto de email e/ou telemóvel, documento de identificação civil, militar, passaporte, título de residência, ou outro documento de identificação equivalente, número de identificação fiscal, número de segurança social, profissão, habilitações literárias e alcunha”.

26. Deste modo, o Projeto de Portaria optou por uma uniformidade dos elementos de identificação individual a partir de uma categoria ampla de dados pessoais identificadores a comunicar, com base essencialmente na mencionada Lei n.º 34/2009, mas nesta tal sucede quando apenas está em causa os dados pessoais constantes das ordens de detenção.

27. Em suma, as *normas habilitantes*, sob o ponto de vista da proteção dos dados pessoais, não identificam nenhum elemento individualizador das categorias dos dados pessoais a comunicar e apenas nos segmentos *normativos colaterais* àquelas disposições legais consagra uma categoria de dados mais ampla, mas, em regra, sem que tenha a extensão identificadora tal como consta no n.º 6 do artigo 2.º do Projeto de Portaria, deixando bastante frágil as exigências formais e substantivas da respetiva habilitação legal.

28. Assim, este desfasamento entre *normas habilitantes* e *normas colaterais* deveria conduzir à reformulação da categoria das primeiras, passando a integrar as segundas, caso seja esse o propósito regulamentador deste Projeto de Portaria.

ii) A tutela jurídica dos dados pessoais

29. O quadro jurídico para a proteção dos dados pessoais encontra-se essencialmente centrado na Constituição da República Portuguesa, através do seu artigo 35.º, na Carta dos Direitos Fundamentais da União Europeia (doravante CDFUE) e no Regulamento Geral sobre a Proteção de Dados (RGPD).

30. A noção legal de dados pessoais está estabelecida no artigo 4.º, 1) do RGPD considerando que os mesmos correspondem à "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;".

31. Por sua vez, de acordo com o artigo 8.º CDFUE o tratamento dos dados de carácter pessoal deve processar-se no estrito respeito pelos direitos, liberdades e garantias das pessoas singulares, em especial pelo direito à proteção dos dados pessoais (*princípio da legalidade*).

32. No que concerne ao RGPD, este veio consignar no artigo 5.º, n.º 1 que os dados pessoais são: i) Objeto de um tratamento lícito, leal e transparente (*licitude, lealdade e transparência*); ii) Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados de forma incompatível com essas finalidades (*limitação das finalidades*); iii) Adequados, pertinentes e limitados ao mínimo necessário à prossecução das finalidades para as quais são tratados (*minimização dos dados*); iv) Exatos e atualizados sempre que necessário, devendo ser tomadas todas as medidas razoáveis para que os dados inexatos sejam apagados ou retificados sem demora (*exatidão dos dados*); v) Conservados de forma a permitir a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados (*limitação da conservação*); vi) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidentais, recorrendo a medidas técnicas ou organizativas adequadas (*integridade e confidencialidade*).

33. Por último o artigo 5.º, n.º 2 do RGPD veio estabelecer o comando de que o responsável pelo tratamento deve adotar as medidas que lhe permitam comprovar que o tratamento de dados pessoais é realizado em conformidade com os princípios enunciados (*responsabilidade*).

iii) As posições anteriores da CNPD sobre semelhantes Projeto de Portaria

34. No Parecer 2019/57, de 17 de setembro de 2019, sobre o projeto de Portaria que visa proceder à regulamentação das comunicações eletrónicas realizadas pelos tribunais judiciais e dirigidas ao Banco de Portugal, apresentaram-se as seguintes recomendações: a) A densificação do artigo 2.º do projeto de Portaria, especificando as categorias de dados pessoais envolvidas nas transmissões de informação entre os tribunais judiciais e o Banco de Portugal, bem como os tipos de documentos transmitidos eletronicamente; b) A consagração expressa da obrigatoriedade de o protocolo referido no mesmo artigo ser sujeito à apreciação prévia da CNPD; c) a reformulação do artigo 3.º do projeto de Portaria, por forma a conter as medidas de segurança envolvidas neste tratamento de dados pessoais; d) A clarificação do n.º 2 do artigo 3.º no sentido de incluir o dever do registo (log) de atividade.

35. Este posicionamento seguiu as recomendações já manifestadas nos Pareceres 2019/54 e 2019/56, ambos de 17 de setembro de 2019.

36. No Parecer 2024/10 de 22 de março de 2024, sobre o Projeto de Portaria que procede à regulamentação das comunicações eletrónicas realizadas entre tribunais judiciais, os tribunais administrativos e fiscais, o Ministério Público e os serviços de registo comercial e predial foi recomendado: “a realização do estudo de impacto sobre a proteção de dados pessoais e a submissão à apreciação da CNPD do protocolo a celebrar entre o Instituto de Gestão Financeira e Equipamentos de Justiça, I.P. e o Instituto de Registo e Notariado, I. P.”

37. No Parecer 2024/31, de 28 de agosto de 2024, sobre o Projeto de Portaria que regulamenta as comunicações eletrónicas realizadas entre tribunais judiciais, os tribunais administrativos e fiscais, o Ministério Público e o Instituto de Medicina Legal e Ciências Forenses (IMLCF), apresentaram-se as seguintes conclusões: “a) A especificação da lei habilitante de acordo com o artigo 1.º do Projeto de Portaria; b) A fixação de modo explícito dos intervenientes nas comunicações eletrónicas (funcionário de justiça ou técnico), designadamente através da sua identificação; c) O estabelecimento das especificações técnicas ou funcionais sobre a referida interoperabilidade dos sistemas; d) A necessidade de estabelecer mecanismos de segurança relativamente ao tratamento de dados e interoperabilidade ...; e) A realização do respetivo estudo de impacto sobre a proteção de dados pessoais”.

iv) O objeto e âmbito do Projeto de Portaria

38. O respetivo preâmbulo enuncia que se “privilegia[ndo] a via eletrónica nas comunicações entre a Guarda Nacional Republicana ou a Polícia de Segurança Pública, com os tribunais e o Ministério Público, no envio de participações ou autos de notícia, bem como na consulta do estado e destino dos processos” (2.º §).

39. Acrescentando que “[p]romove-se, deste modo, a celeridade e eficiência da fase de inquérito, enquanto se agiliza e simplifica a atuação dos órgãos de polícia criminal e se fomenta uma utilização mais sustentável de recursos através da redução do consumo de papel, com a consequente desmaterialização da tramitação processual” (3.º §).

40. Daí que o seu artigo 1.º, mediante a epígrafe “Objeto e âmbito”, mencione que “A presente portaria regulamenta as comunicações, por via eletrónica, entre a Guarda Nacional Republicana (GNR) e a Polícia de Segurança Pública (PSP) com os tribunais judiciais ou o Ministério Público (MP), no âmbito do envio de participações e autos de notícia, bem como da consulta do estado e destino dos processos”.

41. A CNPD constata perante a mencionada exposição de motivos e o referenciado no artigo 1.º que o enfoque desta Portaria é essencialmente dirigido ao inquérito, enquanto fase do processo penal, e com predomínio do Código de Processo Penal.

42. Muito embora se trate de matéria essencialmente de política legiferante, estas finalidades, têm nítido impacto na tutela dos dados pessoais, porquanto poder-se-á questionar quais as repercussões deste Projeto de Portaria no processo civil – mas já não no processo de trabalho –, porquanto continua a ter como referência o núcleo processual tramitado nos tribunais judiciais.

43. Deste modo, seria conveniente que tanto o respetivo Preâmbulo, como o normativo que estabelece o seu objeto e âmbito, sejam precisos relativamente às finalidades regulamentadoras deste Projeto de Portaria, obstando a desnecessários conflitos interpretativos sobre quais os processos em que estão em causa a comunicação eletrónica agora reguladas e através das categorias identificadoras envolvendo os respetivos dados pessoais.

44. Mais será de referir, que o Projeto de Portaria muito embora possa estabelecer de modo inovador o desenho e os parâmetros do modo de comunicação, desde que respeite as finalidades legislativas, já relativamente às categorias de dados a informar encontra-se balizado pelas respetivas leis habilitantes, porquanto aquele diploma regulamentar não tem, só por si, qualquer génese legislativa.

v) O desenho regulamentador e a sua sustentabilidade

45. O Projeto de Portaria é composto por cinco normativos, a saber: objeto e âmbito (artigo 1.º); comunicações eletrónicas (artigo 2.º); segurança (artigo 3.º), produção de efeitos (artigo 4.º), entrada em vigor (artigo 5.º).

46. A identificação do utilizador do sistema de comunicação, designadamente mediante o respetivo registo, através do seu histórico ou relatório de operações (log), consta no subsequente artigo 3.º, mais precisamente no seu n.º 2.

47. No entanto, não se explicita se estamos perante a identificação individual do utilizador, mediante um código de acesso pessoal e intransmissível, o que deveria se exigir, ou então se esse acesso é efetuado mediante código partilhado, o que deveria ser afastado.

48. Mas não é realizada qualquer outra menção aos mecanismos de segurança que devem ser assegurados no mencionado sistema de informação.

49. Nesta conformidade, impõe-se a densificação dos mecanismos de segurança que venham a ser implementados no âmbito deste Projeto de Portaria.

vi) O possível impacto na proteção dos dados pessoais

50. A CNPD chama também a atenção para a observância do disposto no n.º 4 do artigo 18.º da Lei n.º 43/2004, de 18 de agosto (Lei de Organização e Funcionamento da Comissão Nacional de Proteção de Dados), segundo o qual “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 pessoais”.

51. Deste modo, tal omissão compromete a realização de um parecer sustentado e sustentável quanto à validade e fiabilidade relativamente aos prováveis riscos decorrentes dos tratamentos de dados pessoais constantes neste “Projeto DL”.

III. CONCLUSÕES

52. Nos termos e com os fundamentos acima expostos, a CNPD emite o presente parecer, formulando as seguintes recomendações ao presente Projeto de Portaria:

- a) A especificação das normas habilitantes constantes no Projeto de Portaria, de modo a precisar o objeto, âmbito e o propósito regulamentador;
- b) A concretização normativa das finalidades regulamentadoras;
- c) A criação e implementação do modo de identificação individual do utilizador, mediante um código de acesso pessoal e intransmissível;
- d) A densificação e explicitação dos mecanismos de segurança a executar;
- e) A realização do respetivo estudo de impacto sobre a proteção de dados pessoais.

Aprovado na reunião de 13 de janeiro de 2026

Paula Meira Lourenço (Presidente)

DECLARAÇÃO DE VOTO

O Projeto de Portaria vem regular as comunicações eletrónicas entre a Guarda Nacional Republicana e a Polícia de Segurança Pública com os tribunais ou o Ministério Público.

Anuncia-se no Projeto a promoção da celeridade e eficiência da fase de inquérito, enquanto se agiliza e simplifica a atuação dos órgãos de polícia criminal e se fomenta uma utilização mais sustentável de recursos através da redução do consumo de papel, com a consequente desmaterialização da tramitação processual.

No art.º 2.º, n.º 8 estatui-se que *«As especificações técnicas e funcionais da interoperabilidade entre os sistemas de informação referidos no n.º 1, assim como a auditabilidade do seu funcionamento, são definidas em protocolo a celebrar entre o Instituto de Gestão Financeira e Equipamentos da Justiça, I. P., a Guarda Nacional Republicana e a Polícia de Segurança Pública, sujeito a parecer prévio da Comissão Nacional de Proteção de Dados.»*

O art.º 3.º, n.º 1 do Projeto estatui que *«Os sistemas de informação referidos no artigo anterior garantem o respeito pelas normas de segurança e de acesso à informação e de disponibilidade técnica legalmente estabelecidas, por forma a assegurar a confidencialidade e a integridade dos dados.»*

Nos termos do art.º 40.º, n.º 4 da Lei n.º 34/2009, de 14 de julho, na redação da Lei n.º 390/2017, de 30.05, *«A eliminação dos dados arquivados eletronicamente processa-se de acordo com o disposto nos diplomas que regulam o arquivamento, os prazos de conservação administrativa e a destruição dos processos e documentos judiciais, com as necessárias adaptações.»* (sublinhado nosso)

O art.º 41.º desta Lei n.º 34/2009, de 14 de julho, na redação da Lei n.º 390/2017, estatui o seguinte:

Artigo 41.º

Arquivo eletrónico

1 - O arquivamento eletrónico dos dados referido no n.º 3 do artigo anterior implica a vedação do acesso aos mesmos, com exceção do disposto nos números seguintes.

2 - Apenas podem aceder aos dados arquivados eletronicamente:

a) Os magistrados e funcionários de justiça que os coadjuvam, na medida do estritamente necessário para o exercício das suas competências legalmente previstas e com apresentação das razões que fundamentam a consulta;

b) As pessoas às quais a lei confira um direito de consulta de auto ou de obtenção de cópia, extrato ou certidão de auto ou parte dele, na medida do estritamente necessário para realização do fim que fundamenta a consulta e sem prejuízo dos regimes do segredo de justiça e do segredo de Estado.

3 - O acesso referido na alínea b) do número anterior é requerido à autoridade judiciária que tenha proferido a decisão que pôs termo ao processo, com apresentação das razões que fundamentam o pedido.

4 - É aplicável ao processo eletrónico o disposto no artigo 28.º

Esta Lei estatui que *«É subsidiariamente aplicável, às matérias relativas à proteção de dados pessoais previstas na presente lei, o disposto na Lei da Proteção de Dados Pessoais, aprovada pela Lei n.º 67/98, de 26 de outubro.»* (leia-se, Lei n.º 58/2019, de 08.08).

O tratamento de dados deve processar-se no estrito respeito pelos direitos, liberdades e garantias das pessoas, em especial o direito à proteção dos dados pessoais, não se podendo esquecer o princípio da minimização dos dados pessoais. No fundo é o que se anuncia ao longo do Projeto.

Segundo o princípio da minimização dos dados (art.º 4º, n.º 2, al.ª c), e 3 da Lei n.º 59/2019, de 08.08) os dados recolhidos devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados, devendo o responsável pelo tratamento adotar as medidas que lhe permitam comprovar que o tratamento de dados pessoais é realizado em conformidade com os princípios enunciados no número anterior. Este princípio aparece assim associado ao princípio da limitação (cf. limitados ao que é necessário).

O prazo de conservação dos dados deve ser limitado ao mínimo: os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser realizada de forma razoável por outros meios, pelo que o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica, de modo que os dados sejam conservados apenas durante o prazo estritamente necessário. Daí a norma do art.º 40.º, n.º 4 da Lei n.º 34/2009, de 14 de julho, na redação da Lei n.º 390/2017, de 30.05.

O Projeto revela que a matéria da conservação da informação é uma matéria sensível (cf. normas atrás citadas).

Podemos identificar três pilares:

- . adequação: impõe a circunscrição dos tratamentos aos dados pessoais que se enquadram nas finalidades prosseguidas. Os dados não relacionados ou inapropriados encontram-se, *ab initio*, excluídos;
- . pertinência: circunscreve as atividades dos responsáveis a tratamentos que possam contribuir para a prossecução dessas finalidades;
- . limitação: o tratamento apenas será juridicamente aceitável se não existir um método alternativo menos invasivo, por exemplo, a anonimização, ou pseudonimização. Da leitura da alínea c) do n.º 2 do art.º 4.º da Lei n.º 59/2019, de 08.08, resulta que os dados devem ser adequados, pertinentes não excessivos em relação às finalidades para que são recolhidos e posteriormente tratados. Nesta exigência de recolha não excessiva podemos identificar um princípio de proporcionalidade.

E a Lei n.º 59/2019, de 08.08, aprovou as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Ora, nesta senda, o art.º 12.º da Lei n.º 59/2019, de 08.08, estatui o seguinte:

Artigo 12.º

Prazos para conservação e avaliação

1 - Os dados pessoais só podem ser tratados durante o período necessário para a prossecução das finalidades da recolha, ou do tratamento posterior autorizado nos termos do artigo 7.º, findo o qual devem ser apagados, sem prejuízo da sua pseudonimização logo que as finalidades do tratamento o permitam.

2 - O responsável pelo tratamento avalia periodicamente a necessidade de conservar os dados pessoais tratados, de acordo com procedimentos internos adotados para esse efeito, nos quais se deve fixar, nomeadamente, a periodicidade da avaliação.

3 - A periodicidade de avaliação da necessidade de conservar os dados pessoais deve ser determinada em função das diferentes categorias de titulares de dados previstos no artigo 9.º, bem como da necessidade de conservação dos dados em causa para as finalidades do tratamento.

4 - A decisão de conservar os dados pessoais por períodos adicionais ao prazo de conservação original deve ser documentada, justificada e notificada aos titulares dos dados, sem prejuízo do disposto no artigo 16.º

5 - As autoridades competentes devem utilizar sistemas informáticos que facilitem a avaliação periódica da necessidade de conservar os dados e o seu apagamento ou pseudonimização, nomeadamente através de alertas e de medidas de proteção automáticas, tais como a limitação de acesso ou a ocultação dos dados.

Ora, acontece que este artigo 12.º não se mostra implementado na prática, quer nos órgãos de polícia criminal, quer nos Tribunais.

Na verdade, o **Regulamento de Conservação Arquivística dos Tribunais Judiciais e dos Tribunais Administrativos e Fiscais** estabelecido pela Portaria n.º 368/2013, de 24 de dezembro (cf. Declaração de Retificação n.º 7/2014 - 1.ª Série), não foi desenhado para o processo eletrónico, o qual só em datas mais recentes se tornou obrigatório no processo penal, num processo legislativo que culminou com a recente Portaria n.º 350-A/2025, de 09.10, que revogou a Portaria n.º 280/2013, de 26.08, objeto de sete alterações legislativas e de revogação, como referido, **sendo estas portarias omissas quanto a prazos de conservação de processos**, até pela necessidade de um Regulamento.

Repita-se: nos termos do art.º 40.º, n.º 4 da Lei n.º 34/2009, de 14 de julho, na redação da Lei n.º 390/2017, de 30.05, «A eliminação dos dados arquivados eletronicamente processa-se de acordo com o disposto nos diplomas que regulam o arquivamento, os prazos de conservação administrativa e a destruição dos processos e documentos judiciais, com as necessárias adaptações.» (sublinhado nosso)

Assim, o contexto atual é de violação manifesta do princípio de minimização de dados.

A vertente de limitação e proporcionalidade na conservação dos dados tem estado ausente, e com este Projeto assume-se como simples remissão para algo que não funciona, por inadequado.

Sem um Regulamento específico para a tramitação digital não se vislumbra que exista instrumento jurídico ou prática suficiente para dar resposta a um princípio nuclear em matéria de proteção do bem jurídico em causa.

Por outro lado, importa recordar que, mesma na área da investigação criminal, em que o Ministério Público é a autoridade judiciária que detém a direção funcional das investigações, o certo é que os órgãos de polícia criminal trabalham em plataformas informáticas próprias, com regras próprias, num esquema de interoperabilidade, parecendo-nos até que essa interoperabilidade colide com a norma constitucional que consagra a qualidade do Ministério Público como magistratura detentora da direção funcional da investigação, o que nos parece impor, até por comando constitucional, uma plataforma única nesta sede da investigação de inquéritos-crime que reflita essa realidade, princípio este cuja violação se perpetua com este Projeto (!), o que é revelador da falta de visão do legislador na matéria e de investimento nos tribunais, em especial na plataforma informática do Ministério Público.

Não existindo uma plataforma única, no esquema atual, a informação recolhida nas investigações, existente e conservada nas plataformas informáticas dos órgãos de Polícia Criminal, deveria de estar indexada ao resultado final (cf. arquivamento ou acusação e, neste caso, não pronúncia/pro-núncia, condenação/absolvição), pois é ele que define o ponto de partida da contagem dos prazos de preservação digital. Isso não acontece e não vai acontecer com as plataformas existentes, pelo menos tão cedo, a não ser por cuidados acrescidos dos OPC por insuficiência de interconexão.

Ou seja, não só é necessário garantir o estrito cumprimento do **art.º 12.º da Lei n.º 59/2019, de 08.08**, nos tribunais, como também se impõe o seu cumprimento nas plataformas dos OPC.

Sem um Regulamento de Preservação Digital abrangente, a modalidade de conservação da informação assenta hoje numa conservação global da informação nas plataformas eletrónicas, com mera anotação de processo destruído no processo eletrónico, quando a destruição se refira a processo físico, numa lógica paradoxal que viola o art.º 12.º da Lei n.º 59/2019, de 08.08. E a vedação de acessos, opção escolhida para contornar o problema, não é suficiente, pois não deixa de existir tratamento de dados pessoais de forma injustificada, como melhor se verá da jurisprudência a seguir indicada.

Esta Portaria “*coloca a carruagem à frente dos bois*”, usando uma terminologia mais popular, não se vislumbrando um instrumento jurídico vinculativo habilitado a suprir tais problemas de falta de implementação de uma verdadeira proteção de dados pessoais.

Convém citar jurisprudência do Tribunal Europeu dos Direitos Humanos, uma vez que existem direitos fundamentais e necessidade de os mesmos serem respeitados (implementados).

No Acórdão do Tribunal Europeu dos Direitos Humanos de 04/12/2008 (Queixas n.ºs 30562/04 et 30566/04; Marper), o Tribunal Europeu dos Direitos Humanos considerou que a retenção indefinida das impressões digitais, amostras de células e perfis de ADN era desproporcionada e desnecessária numa sociedade democrática, considerando que o processo penal tinha terminado com uma absolvição:

«125. O Tribunal considera que a natureza geral e indiferenciada do poder de retenção de impressões digitais, amostras biológicas e perfis de DNA de pessoas suspeitas de terem cometido crimes, mas não condenadas, conforme aplicado aos requerentes no presente caso, não reflete um equilíbrio justo entre os interesses públicos e privados concorrentes em jogo, e que o Estado demandado excedeu qualquer margem de apreciação permitida nesta área. Portanto, a retenção impugnada constitui uma interferência desproporcional no direito dos requerentes ao respeito pela sua vida privada e não pode ser considerada necessária numa sociedade democrática...[...].

126. Consequentemente, houve uma violação do artigo 8.º da Convenção no presente caso.»

No Acórdão do Tribunal Europeu dos Direitos Humanos de 06/06/2006 SEGERSTEDT-WIBERG ET AUTRES c. SUÈDE; (Queixa n.º 62332/00), o TEDH constatou uma violação do art.º 8.º da CEDH uma vez que o armazenamento contínuo de dados não era pertinente, devido ao longo período decorrido (cf. ingerência desproporcionada no exercício do direito ao respeito pela vida privada).

Em suma, este Projeto é o perpetuar de uma falta de visão no que respeita a um sistema informático que cumpra as exigências constitucionais decorrentes do Estatuto do Ministério Público, um anúncio de falta de investimento na justiça por recurso a segundas opções, a dita interoperabilidade, e aparece antes da regulação em matéria de dados pessoais, não se curando sequer de elaborar previamente ao Projeto um Regulamento de preservação digital, tudo se resumindo a uma remissão para um regulamento já inadequado e ultrapassado, com lacunas de regulamentação, e não desenhado para o mundo digital, e para um futuro protocolo, não tendo havido sequer o cuidado de

preparar uma avaliação de risco imposta por lei, como muito bem referido no Parecer que se acompanha.

Assinado por: **JOSÉ MÁRIO NOGUEIRA DA COSTA**
Num. de Identificação: [REDACTED]
Data: 2026.01.13 15:35:59+00'00'

