

PARECER/2024/24

I. Pedido

1. Sua Excelência o Secretário de Estado Adjunto e da Defesa Nacional solicitou à Comissão Nacional de Proteção de Dados (CNPD) que emitisse Parecer sobre a observância das regras relativas à segurança do tratamento de dados no pedido de autorização para a utilização de câmaras portáteis de uso individual pela Polícia Marítima.

2. 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, a 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, todos da Lei n.º 58/2019, de 8 de agosto, que executa na ordem jurídica interna o RGPD.

II. ENQUADRAMENTO JURÍDICO

3. O presente parecer tem como objeto específico a utilização de câmaras portáteis de uso individual (vulgo *bodycams*), pela Polícia Marítima¹, após aquisição de 112 “Kits Coercivos”, dos quais fazem parte câmaras portáteis de uso individual, decorrendo, conjugadamente, do previsto nos artigos 10.º da Lei n.º 95/2021, de 29 de dezembro e artigo 3.º do Decreto-Lei n.º 2/2023, de 2 de janeiro.

4. A utilização de câmaras portáteis de uso individual pelas forças policiais encontra, presentemente, estribo específico no ordenamento jurídico português, nomeadamente na Lei n.º 95/2021 e Decreto-Lei n.º 2/2023, sendo aplicável, igualmente, o elenco definitório constante no artigo 3.º da Lei n.º 59/2019, de 8 de agosto

5. Na verdade, ainda que o uso deste tipo de sistemas de videovigilância seja suscetível de convocar dimensões problemáticas várias nem sempre de fácil resposta, no que toca à proteção de dados pessoais, o regime fundamentador de licitude da sua utilização e, por conseguinte, das operações de tratamento de dados a que se lhes refere, viria a ser desenhado, no essencial, por aqueles diplomas, tendo, de resto, esta Comissão, em

¹ Doravante, PM.

pareceres emitidos² aquando dos respetivos projetos legislativos, realizado um conjunto de observações espelhantes dessas dimensões, mesmo jusfundamentais - e na apreciação contextual e material dos conteúdos e intenções legislativas sobre esta matéria particular- , para as quais ora se remete, que constituirão subsídios hermenêuticos valiosos em vista à interpretação desses diplomas sob a ótica da proteção de dados pessoais.

6. Primariamente, esta Comissão não poderá deixar de sublinhar que a matéria de dados pessoais partilha a dimensão jurídica de direitos fundamentais, assumindo-se, portanto, como parte desse património comum nuclear de direitos e liberdades na qual assenta a vivência de uma sociedade democrática, com as consequências que tal dignidade reclama.

7. Destarte, a proteção de dados pessoais encontra-se diretamente prevista na Carta dos Direitos Fundamentais da União Europeia³, e os seus tratamentos deverão obedecer aos princípios e ideias-matriz amplamente reconhecidos na legislação europeia e nacional que se difunde dessa identidade, e que procuram confirmar e promover a ideia de direitos humanos que lhe está na origem, enquanto uma das suas manifestações.

8. Enquanto matéria jusfundamental, a proteção de dados pessoais goza, também, da consagração de um conjunto de princípios próprios, que emergem na dependência axiológica daquele núcleo essencial, no sentido de lhes confirmar eficiência.

9. É assim que, nesse sentido, resultam como princípios conformadores desta matéria⁴, para além dos da licitude⁵, lealdade e transparência, e os da exatidão, integridade e confidencialidade⁶, os da necessidade, pertinência e adequação às finalidades específicas que justificam o tratamento⁷ e, conjugadamente, a minimização dos dados a tratar, em pelo menos duas vertentes: a quantidade e tipo de dados tratados, e a extensão dos tratamentos a realizar, com incidência na limitação da sua conservação.

10. É, pois, a esta luz maior que todos os tratamentos de dados devem ser considerados, e, bem assim, serem avaliados, pelo que também servirão as observações que se lavrarão de seguida.

11. *Brevitatis causa*, desde logo, qualquer tratamento de dados pessoais, dada a natureza retratada, só poderá ocorrer quando exista fundamento de licitude que os autorize.

² Cfr. os Pareceres 143/2021 e 101/2022.

³ Veja-se o seu artigo 8.º.

⁴ Veja-se, em geral, o artigo 5.º do RGPD.

⁵ Cfr. o elenco taxativo constante no artigo 6.º do RGPD.

⁶ Os dados devem ser tratados de uma forma que garanta a sua segurança, incluindo contra o seu tratamento não autorizado ou ilícito, e contra a sua perda, destruição ou danificação accidental.

⁷ Trata-se, deste modo, de um juízo de proporcionalidade.

12. No artigo 8.º da Carta dos Direitos Fundamentais refere-se que os dados pessoais “devem ser objeto de um tratamento leal, para fins específicos”⁸, não podendo esses dados serem tratados posteriormente de uma forma incompatível com essas finalidades⁹. Dito doutro modo, o responsável pelo tratamento só poderá recolher dados para finalidades determinadas, explícitas e legítimas e, uma vez recolhidos, não os poderá utilizar para outras finalidades que não sejam compagináveis com aquelas.

13. Os fins do tratamento assumem-se, pois, como pedra-de-toque para o tratamento de dados pessoais – a determinação de finalidade constitui um passo primário de um tratamento de dados pessoais, já que, ao mesmo tempo que é suscetível de o justificar e autorizar, co-determina o preenchimento de outros princípios e aspetos a executar no tratamento, tão amplos quanto as categorias de dados a considerar, até à sua conservação ou medidas técnicas e de segurança a garantir.

14. De resto, as finalidades assumem um papel preponderante no juízo de proporcionalidade em que cada um destes juízos jusfundamentais deve assentar, num julgamento amplo de licitude, a aferir em concreto.

15. É por essa razão que o Legislador, através da Lei n.º95/2021, veio regular a utilização e o acesso a sistemas de videovigilância pelas força e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil, especificando, no seu artigo 3.º, que tais sistemas apenas podem ser usados para fins de: a) *Proteção de edifícios e infraestruturas públicas e respetivos acessos;* b) *Proteção de infraestruturas críticas, pontos sensíveis ou instalações com interesse para a defesa e a segurança e respetivos acessos;* c) *Apoio à atividade operacional das forças e serviços de segurança em operações policiais complexas, nomeadamente em eventos de grande dimensão ou de outras operações de elevado risco ou ameaça;* d) *Proteção da segurança das pessoas, animais e bens, em locais públicos ou de acesso público, e a prevenção da prática de factos qualificados pela Lei n.º como crimes, em locais em que exista razoável risco da sua ocorrência;* e) *Prevenção de atos terroristas;* f) *Resposta operacional a incidentes de segurança em curso;* g) *Controlo de tráfego e segurança de pessoas, animais e bens na circulação rodoviária;* h) *Prevenção e repressão de infrações estradais;* i) *Controlo de circulação de pessoas nas fronteiras externas;* j) *Proteção florestal e deteção de incêndios rurais;* k) *Apoio em operações externas de busca e salvamento e, ainda, em instalações policiais de atendimento ao público.*

16. Também nessa Lei n.º (artigo 10.º) se deixou previsto o regime essencial sobre o uso deste tipo de câmaras, remetendo-se, porém, para aquele Decreto-Lei a matéria respeitante “*As características e normas de colocação, ativação, sinalização e utilização das câmaras [...], e a forma de transmissão, armazenamento e acesso aos dados recolhidos.*”

⁸ Sublinhado nosso.

⁹ Cfr. artigo 5.º, n.º 1, alínea b) do RGPD.

17. O referido Decreto-Lei n.º, com o n.º 2/2023, vem assim definir “[...] as normas de colocação, ativação, sinalização e utilização das câmaras portáteis de uso individual [...]”, “[...] assim como a forma de transmissão, armazenamento e acesso aos dados recolhidos e as características e requisitos técnicos mínimos das CPUI. ”

18. Este diploma, inserido na pressuposta esfera material de regulação da Lei n.º a que se fez menção, deve ser considerado conjuntamente com aquela, daqui decorrendo que a utilização das câmaras portáteis de uso individual pelos agentes policiais só poderá acontecer quando se verificarem os fins previstos naquele artigo 3.º da Lei n.º 95/2021, que, enquanto condição necessária e autorizante para o tratamento de dados em causa, devem previamente aí encontrar subsunção, o que não vem indicado no pedido de parecer, nem nos documentos que o instruem.

19. Na verdade, sendo o diploma aplicável a todas as forças policiais, alguns dos fins aí constantes não são, sequer, suscetíveis de articulação com as competências legais atribuídas à PM¹⁰.

20. Ainda que no anexo B dos seus documentos instrutores sob o título “Normas tendentes a assegurar o correto uso dos dados registados” se enuncie que “Apenas é permitido o recurso às bodycams para gravação de intervenções policiais, quando ocorra: a. A prática de ilícito criminal; b. Agressão atual e ilícita dirigida contra o próprio agente policial ou contra terceiros; c. Desobediência e resistência a ordens legais e legítimas de agente policial, no exercício de funções policiais; d. Situação de perigo ou emergência ou em operação que envolva risco para o agente policial ou para terceiros; e. Ação para efetuar a captura ou impedir a fuga de pessoa suspeita da prática de crime punível com pena de prisão; f. Operação que vise efetuar a prisão de pessoa evadida ou objeto de mandado de detenção ou para impedir a fuga de pessoa regularmente presa ou detida; g. Situação de alteração da ordem pública.

21. E, ainda, que “É obrigatório o recurso às bodycams para gravação das intervenções policiais, quando ocorra: a. Uso da força pública sobre qualquer cidadão, nomeadamente quando for aplicado o procedimento de restrição física ou algemagem; b. O recurso ou uso de quaisquer meios coercivos ou armas policiais, especialmente arma de fogo; c. A emissão de ordens a suspeitos relativas à cessação de comportamentos ilegais ou agressivos e à adoção de posições de segurança.”,

22. os trechos que se acabam de deixar citados resultam de transcrição dos números 4 e 5 do artigo 7º do Decreto-Lei n.º n.º 2/2023, sob epígrafe “gravação”, onde se circunstancia a permissibilidade e a obrigatoriedade da gravação das intervenções policiais (e o seu *modus*) que, previamente, como se disse, haverá sempre de pressupor a inclusão genética nos fins previstos no artigo 3.º da Lei n.º 95/2021, situando-se, assim, em planos diferentes.

¹⁰ Ainda que, refira-se, atenta a natureza de OPC da PM, outros seguramente serão.

23. Os critérios respeitantes às gravações não correspondem aos *fins* que fundamentam e justificam autorizadamente a utilização destes sistemas, servindo, em abstrato, para subsunção a qualquer uma daquelas alíneas do n.º 1 do referido artigo 3.º, ou a todas, seja a PM ou outros Órgãos de Polícia Criminal.

24. Em conclusão, o que deve ser entendido como fins ou finalidades, para estes efeitos, haverá de reputar a ou as concretas utilizações que pretendem ser dadas pela PM no recurso a estes sistemas, no exercício e âmbito das suas competências, atribuições e tarefas de OPC, a realizar em juízo concreto, e que encontre acolhimento nos fins que permitem a utilização destes sistemas, e que permitam a sua invocação. Apesar de se afigurar como uma representação ampla, o conteúdo dos fins previstos no referido artigo 3.º não é irrestrito.

25. Em reforço, logo no artigo subsequente da Lei n.º (4.º), sublinhando-se a mesma importância, declara o Legislador que *1 - A utilização de câmaras de vídeo rege-se pelo princípio da proporcionalidade. 2 - É autorizada a utilização de câmaras de vídeo quando tal meio se mostre adequado para os fins previstos no artigo anterior, tendo em conta as circunstâncias concretas do local a proteger. 3 - Na ponderação, caso a caso, da finalidade concreta a que o sistema de videovigilância se destina, deve ser considerada a possibilidade e o grau de afetação de direitos pessoais, decorrentes da utilização de câmaras de vídeo. 4 - São proibidas a instalação e a utilização de câmaras fixas ou portáteis em áreas que, apesar de situadas em locais públicos, sejam, pela sua natureza, destinadas a ser utilizadas em resguardo. 5 - É vedada a utilização de câmaras de vídeo quando a captação de imagens e de sons abranja o interior de casa ou edifício habitado ou sua dependência, ou de estabelecimentos hoteleiros e similares, salvo consentimento dos proprietários e de quem o habite legitimamente, ou autorização judicial. 6 - É igualmente vedada a captação de imagens e sons quando essa captação afete, de forma direta e imediata, a esfera da reserva da vida íntima e privada. 7 - As imagens e os sons acidentalmente obtidos, em violação do disposto nos n.os 5 e 6, devem ser destruídos de imediato pelo responsável pelo sistema. " [sublinhado nosso].*

26. E, ainda que o artigo 10.º da mesma Lei n.º seja aquele que se refere especificamente à utilização de câmaras portáteis de uso individual, não se afastará do regime geral em que vem incluído, já que, para além de remeter para o Decreto-Lei n.º 2/2023, apenas refere que "[...] 3 - As câmaras portáteis de uso individual devem ser colocadas de forma visível no uniforme ou equipamento, sendo dotadas de sinalética que indique o seu fim. 4 - A captação e gravação de imagens e sons apenas pode ocorrer em caso de intervenção de elemento das forças de segurança, nomeadamente quando esteja em causa a ocorrência de ilícito criminal, situação de perigo, emergência ou alteração da ordem pública, devendo o início da gravação ser precedido de aviso claramente perceptível, sempre que a natureza do serviço e as circunstâncias o permitam. 5 - A captação e gravação de imagens é obrigatória quando ocorra o uso da força pública sobre qualquer cidadão ou o recurso a quaisquer meios coercivos, especialmente arma de fogo. 6 - É proibida a gravação permanente ou indiscriminada de factos que não tenham relevância probatória, devendo, em todas as circunstâncias, ser respeitada a dignidade dos cidadãos e preservados os direitos pessoais, designadamente o direito à imagem e à palavra. 7 - Os dados

gravados são armazenados no sistema, em ficheiro encriptado que assegure a sua inviolabilidade, não podendo ser eliminados ou alterados pelo agente que procedeu à gravação. 8 - As características e normas de colocação, ativação, sinalização e utilização das câmaras referidas no n.º 1, e a forma de transmissão, armazenamento e acesso aos dados recolhidos, são objeto de Decreto-Lei..”

27. É também significativa, crê-se, a expressão legislativa constante no artigo 16º da Lei n.º, sob epígrafe “Recolha e tratamento de dados”, quando se dispõe que “1-Para os fins previstos no artigo 3.º, o tratamento de dados pode ter subjacente um sistema de gestão analítica dos dados captados, por aplicação de critérios técnicos, de acordo com os fins a que os sistemas se destinam.”

28. Em conclusão, deverá a utilização do uso de *bodycams* pela PM ser em concreto definida, nomeadamente atendendo aos fins previstos no artigo 3.º da Lei n.º 95/2021.

29. Isto posto, como se deixou provocado no início deste parecer, é também importante para avaliação da licitude ampla de um tratamento de dados o *modus* como esta é executada e operacionalizada, não se tratando de matéria subsidiária ou secundária dos respetivos tratamentos, na medida em que são tais aspetos que, na execução de tratamento, constituem a irradiação ôntica dos juízos e direitos em ação, levando-os à prática.

30. Acresce que nem no pedido, nem nos anexos, está expressa se existirá gestão analítica de dados e, a existir, se esta é efetuada por alarmística baseada em algoritmos pré-definidos ou baseada em inteligência artificial (IA) generativa. Sem estes elementos a CNPD não pode aferir o potencial discriminatório deste tratamento de dados pessoais.

31. Não será de mais lembrar que o novo Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, (doravante Regulamento) que cria regras harmonizadas em matéria de inteligência artificial, e que se encontra em vigor desde o dia 1 de agosto de 2024, impõe que para que o conjunto de normas vinculativas aplicáveis aos sistemas de IA seja proporcionado e eficaz, deverá seguir-se uma abordagem baseada no risco claramente definida.

32. Aliás, a utilização da IA neste âmbito, atento o papel das autoridades policiais e a consciência que as suas ações são caracterizadas por um grau substancial de desequilíbrio de poder e podem conduzir à vigilância, detenção ou privação da liberdade de uma pessoa singular, bem como ter outras repercussões negativas nos direitos fundamentais, em especial se não forem cumprido os requisitos adequados em termos de desempenho, de exatidão ou solidez, ou não tiver sido devidamente concebido e testado antes de ser colocado no mercado ou em serviço, o sistema de IA pode ser altamente discriminatório.

33. Além disso, o exercício de importantes direitos fundamentais processuais, como o direito à ação e a um tribunal imparcial, o direito à defesa e a presunção de inocência, pode ser prejudicado, em particular, se esses

sistemas de IA não forem fiáveis, transparentes e documentados. Por essa razão o Regulamento classifica como sendo de risco elevado a utilização de IA pelas forças de segurança (cf. n.º 6 do Anexo III do Regulamento).

III. DA CONCRETA UTILIZAÇÃO DO SISTEMA DE CÂMARAS PORTÁTEIS DE USO INDIVIDUAL PELA POLÍCIA MARÍTIMA.

34. Pretende a PM a implementação de um sistema de videovigilância através da utilização de câmaras portáteis de uso individual, mais concretamente, com os equipamentos constantes no anexo A e com a regras operacionais plasmadas no Anexo B juntos ao pedido de parecer.

35. Dos documentos constantes do pedido, resulta que as regras de utilização operacional das *bodycams* (Anexo B) correspondem, na generalidade, aos ditames específicos do legislador para a sua correta utilização, previstas no Decreto-Lei n.º 2/2023, mormente no que toca ao modo de porte, à permissão e/ou obrigatoriedade e proibição de gravação, necessidade de anúncio verbal de utilização e dever de relato e comunicação.

36. Já quanto às câmaras adquiridas e que se pretendem implementar para este uso, deverá reputar-se que estas deverão ser pré-configuradas antes da sua colocação em utilização pelos operadores, sem possibilidade de estes poderem alterar essas configurações nos aparelhos, de forma a adequá-las, a todo tempo, ao regime jurídico que conforma este seu uso, como de seguida melhor se procurará explicar.

37. Quer o artigo 10.º n.º 7 da Lei n.º 95/2021, quer o artigo 12.º do Decreto-Lei n.º 2/2023 sublinham que o agente policial que executou a gravação não poderá apagá-la ou alterá-la, devendo ser respeitada em permanência a integridade dos dados tratados, e os dados recolhidos só podem ser ocorrer no cumprimento escrupuloso das regras fixadas que as autorizam.

38. Importa ainda referir que a existência de registos de auditoria é, no caso em análise, imprescindível, e que, para que não seja possível questionar a sua integridade, devem estar digitalmente assinados

39. Da informação feita chegar conclui-se que as câmaras são do modelo Axon Body 3, do fabricante Axon Enterprise, Inc., uma empresa norte americana baseada no estado do Arizona.

40. Compulsadas as características técnicas destes aparelhos, repara-se que estas são capazes da gravação simultânea de imagem e som, sem a necessidade de manuseio por parte operador, e possuem as seguintes

características¹¹: gravação de imagem em Full HD¹²; bateria que suporta 14 horas de operação; 64GB de armazenamento; encriptação AES-XTS 128-bit; *buffer* pré-evento¹³ configurável até 120 segundos.

41. Estas câmaras são, também, capazes de interagir com outros dispositivos do mesmo fabricante, nomeadamente os *Taser*, podendo a gravação ser acionada mediante o acionar daqueles dispositivos.

42. A revisão das especificações técnicas da câmara no *site* do fabricante¹⁴ levam também a concluir que a encriptação nas câmaras está ativa para o conteúdo do disco onde as imagens e som são gravados, requisito que, sublinhe-se, deve ser cumprido em qualquer circunstância, não só na utilização de recolha de imagens e som, mas também no processo de transferência dos dados captados e guardados, como dispõe os artigos 11.º, n.º 5, e 16.º n.º 2, alínea k) do Decreto-Lei n.º /2023 e o artigo 10.º n.º 7 da Lei n.º 95/2021.

43. Antes de poderem ser usadas pelos operadores as câmaras terão de ser registadas.

44. O registo poderá, de acordo com as características dos aparelhos, ser feito de dois modos: através de uma *app* Axon Device Manager (ADM), instalada em *smartphone*, ou através da aplicação View XL Standalone, instalada em computador Windows.

45. No caso de o registo ser feito através da ADM, a câmara terá de estar acoplada a uma *docking station*¹⁵ (Axon Dock). Estas estações estão ligadas à rede e devem ter acesso ao servidor Axon Evidence (descrito infra). Quando acopladas a estas *docking stations* as câmaras carregam a bateria, recebem *updates* do sistema, sincronizam o relógio interno, e descarregam os filmes que têm gravados no disco interno para o servidor Axon Evidence, apagando-os de seguida com a confirmação de que a transmissão foi bem-sucedida.

46. Para registar a câmara usando a ADM, o operador da aplicação deve ter as necessárias permissões configuradas no servidor Axon Evidence.

¹¹ https://www.axon.com/products/enterprise-commercial_axon-body-3

¹² Full High Definition refere uma resolução de vídeo de 1920x1080, ou seja, imagens com 1920 pontos (pixel) horizontais por 1080 verticais.

¹³ As câmaras estão continuamente a recolher imagem e som. Quando o operador pressiona o botão para iniciar a gravação, as câmaras gravarão as imagens que antes tinham captado, se a captura foi feita dentro do intervalo de tempo definido. As câmaras Axon Body 3 permitem um *buffer* máximo de 120 segundos o que significa que, se esse período não for alterado na configuração, quando o operador pressionar o botão para iniciar a gravação a câmara grava as imagens que captou nos últimos 120 segundos antes dessa ativação. O som do período pré evento só é gravado se a câmara for configurada para esse efeito.

¹⁴ https://www.axon.com/products/enterprise-commercial_axon-body-3

¹⁵ Estação de acoplamento é um dispositivo eletrónico onde a câmara Axon Body 3 é acoplada de modo a que os filmes aí gravados sejam descarregados, a que a câmara receba *updates* de sistema, a que sincronize o relógio interno e carregue a bateria.

47. O registo realizado através da aplicação View XL Standalone instalada em computador Windows é feito mediante a conexão da câmara ao computador via cabo USB, estando a aplicação igualmente em contacto com o servidor Axon Evidence através da rede.

48. Após o registo, as câmaras deverão ser atribuídas a um utilizador, mediante configuração no servidor Axon Evidence. Esta atribuição consiste apenas na associação do registo da câmara ao utilizador (através de nome ou ID do agente policial, por exemplo) de modo a que todos os filmes (vídeo e áudio) gravados identifiquem o agente a quem a câmara estava atribuída no momento da captura do vídeo e áudio. As câmaras podem mudar de operador bastando para tal a execução do *reassign* no servidor Axon Evidence, devendo cuidar-se de criar procedimentos quanto a esta matéria que permitam registar, em ambiente seguro, qualquer alteração realizada, e que permita a rastreabilidade subjetiva e objetiva de qualquer operação no tocante à utilização das câmaras.

49. De resto, também se especifica claramente no artigo 11.º do Decreto-Lei que *"8 - Deve ser assegurada a criação de diferentes perfis de acesso que assegure que cada elemento policial tem os acessos estritamente necessários para o desempenho das respetivas funções, e que "9 - Os perfis a criar devem ser diferenciados de acordo com as funções desempenhadas, prevendo para cada um destes o respetivo âmbito e extensão, diferenciando permissões de visualização, tratamento, extração e conservação."*

50. Também no tocante ao acesso às gravações, apenas é permitido aos agentes policiais devidamente credenciados para o efeito, através do sistema, em estação de trabalho fixa colocada em instalação policial, e, em auxílio do que se disse, *"4 - Todas as operações de acesso às gravações são registadas no sistema, com indicação da data e hora, justificação e identificação do responsável pela intervenção."* Nesse sentido, deverá entender-se por "acesso" qualquer intervenção realizada no sistema que tenha por objeto, direta ou indiretamente, as referidas gravações, bem como se devem fixar com clareza as atribuições de perfis de manipulação do sistema que permitam exercitar um mecanismo de *checks and balances*, não devendo ser permitida a sobreposição concentrada de possibilidades de operação/acesso/configuração/alteração/eliminação.

51. Todavia, pela consulta do manual não se consegue concluir se uma câmara ainda não atribuída fica inabilitada de gravar. Poderá entender-se que a câmara pode operar no modo gravação sem ter sido previamente atribuída a um agente, situação que deverá ser obviada, por evidente colisão com os princípios a que ora se alude.

52. A ativação/inativação das várias definições dos aparelhos é feita no servidor Axon Evidence e transmitida à câmara no momento em que a mesma está acoplada a uma *docking station*. As configurações podem também

ser enviadas para as câmaras caso estas tenham conectividade Wi-Fi ou LTE¹⁶, o que não resulta evidente da informação instrutória. Como se disse, as câmaras, uma vez configuradas de acordo com as restrições legislativas para o seu uso não devem permitir configurações distintas daquelas, devendo ser criados mecanismos técnicos e de segurança que impeçam esses riscos, tanto mais se puderem ser realizadas à distância e a qualquer momento e, eventualmente, sem registos que permitam esse controlo, bem como riscos de intrusão.

53. De entre as definições que podem ser ativas/inativas destacam-se algumas que têm especial relevância tendo em conta a utilização permitida das câmaras portáteis de uso individual no contexto da intervenção das forças de segurança.

54. Sem configuração adicional, as câmaras não gravam o som do período pré-evento, ou seja, dos 30 segundos definidos legislativamente imediatamente anteriores ao momento de ativação da gravação. Como se disse supra, o *buffer* de gravação do modelo do aparelho em causa pode ser de até 120 segundos, devendo ser configuradas as câmaras de modo a que este se restrinja aos 30 segundos previstos no número 2 do artigo 7.º do Decreto-Lei n.º 2/2023.

55. As câmaras têm, também, a capacidade de funcionar em *stealth mode*¹⁷, onde todos os indicadores luminosos, sonoros e de vibração são desligados. No manual de utilizador da câmara Axon Body 3 não é possível determinar se o modo *stealth* pode estar ativo durante o período em que a câmara está em gravação. Na consulta do manual de modelos mais antigos a descrição do modo *stealth* dá a entender que o mesmo pode estar ativo quando a câmara está a gravar¹⁸.

56. Em qualquer caso, não poderá deixar de se notar que a intenção legislativa não prevê ou autorizará uma utilização deste tipo, desde logo por aplicação do princípio de proporcionalidade que a rege, a verter no equilíbrio jusfundamental entre os direitos dos titulares dos dados e o interesse público que subjaz aos fins que autorizam este tratamento.

57. Na verdade, logo na exposição de motivos do Decreto-Lei n.º pode ler-se que “[...] a utilização das câmaras portáteis de uso individual deve ser objeto de um enquadramento exaustivo que delimite as situações em que o elemento policial pode fazer uso deste equipamento, com respeito pelos direitos, liberdades e garantias individuais, preservando a dignidade pessoal daqueles cujas imagens venham a ser recolhidas. Para o efeito, revela-se

¹⁶ Wi-Fi designa uma família de protocolos de rede sem fios usados para a ligação de um dispositivo a uma rede local; LTE (Long Term Evolution) é um standard de redes de comunicação móvel.

¹⁷ Modo furtivo; neste modo os indicadores das câmaras estão desligados (https://my.axon.com/s/article/Configure-your-camera-AB3?language=en_US#stealth).

¹⁸ https://my.axon.com/s/article/Axon-Body---Enabling-stealth-mode?language=en_US

essencial que a ativação das câmaras portáteis de uso individual seja claramente perceptível pelos distintos intervenientes, razão pela qual se impõe, nos termos do n.º 4 do artigo 10.º da Lei n.º 95/2021, de 29 de dezembro, que os elementos das forças de segurança devam proceder ao aviso claro e perceptível do início da gravação. Através do presente Decreto-Lei n.º é elencada a forma como as câmaras portáteis devem ser fixadas para garantir a sua visibilidade por terceiros, bem como a obrigatoriedade de advertência ou aviso que deve preceder o início da gravação.”

58. Em regra, pois, deve sempre procurar garantir-se que as pessoas gravadas sejam informadas de que a gravação está a ocorrer, o que não deve ser confundido com o seu consentimento, que é o que vem afastado no número 8 do artigo 7.º do Decreto-Lei n.º.

59. Ademais, o Legislador exige, via da regra, o anúncio verbal e claramente perceptível de se estar a proceder à gravação de imagens e som, pelo que, *a fortiori*, também as câmaras deverão possuir indicação permanente que assinala os momentos em que se encontram a gravar, por forma a sinalizar a operação, já não só instantaneamente, mas também durante todo o momento em que decorrer a gravação, e nos diferentes espaços e intervenientes com os quais se possa cruzar, atento o carácter dinâmico de uma gravação vídeo e áudio.

60. A isto acresce que, nos requisitos mínimos de que os aparelhos devem cumprir, constam expressamente as características de “c) Assinalar o início e o fim da gravação por sinal sonoro;” e “d) Ativar sinal luminoso quando o modo de gravação se encontre ativo;”. – cfr. Artigo 16.º n.º 2, alíneas c) e d) do Decreto-Lei n.º 2/2023.

61. Tudo a concluir, desta maneira, que também o modo “furtivo” deve ser desativado definitivamente em todas as câmaras antes da sua utilização.

62. As câmaras permitirão, também, a visualização dos filmes gravados através do uso da *app* Axon View instalada em dispositivo *smartphone* emparelhado¹⁹ com a câmara. Através do uso da *app* o operador pode também incluir metadados²⁰ (ID do caso, título e categoria) nos filmes gravados, incluindo também a localização georreferenciada do *smartphone*.

63. As câmaras podem incluir, na gravação vídeo, informação referente à localização do aparelho, mediante a recolha de dados do sensor GNSS/GPS.

64. A necessidade de geolocalização não vem referida como requisito técnico mínimo das câmaras, prescrevendo-se apenas no artigo 11.º n.º 6, alínea f) do Decreto-Lei n.º 2/2023 que o sistema deverá permitir

¹⁹ O emparelhamento entre dois dispositivos refere o processo de estabelecimento de um canal de comunicação entre dois equipamentos de modo a poderem trocar informações.

²⁰ https://my.axon.com/s/global-search/can%20a%20camera%20axon%20body%203%20recording%20under%20stealth%20mode?language=en_US

que as gravações armazenadas incluam o número único e inalterável correspondente e a data hora e local da gravação, devendo também poder permitir-se a pesquisa no sistema através desse campo, o que, em tese, permitirá a inserção desta informação de forma manual.

65. As questões relacionadas com a geolocalização podem assumir avaliações complexas. No caso vertente, por exemplo, uma coisa seria se esta funcionalidade apenas se encontrasse ativa no momento da justificada gravação, outra seria se se encontrasse ativa mesmo quando a câmara se encontre em repouso, acabando por, na prática, constituir um aparelho GPS que acompanha todo o percurso do agente policial enquanto estiver de turno, dando azo eventual, por hipótese, a um possível controlo dos seus movimentos enquanto se encontrar fardado ou equipado, situação que exigirá um juízo bem diferente, pelo menos nestes termos²¹.

66. Na verdade, no anexo D junto ao pedido de parecer, refere-se que *“Quando o modo de gravação é ativado, o vídeo e o áudio são gravados assim como as coordenadas do GPS, data, hora e ID do utilizador. Este processo continuará durante toda a gravação até que o evento seja considerado como terminado e acionado o modo de pronto (buffer) no equipamento.”*

67. Destas declarações parece resultar que os dados de geolocalização apenas são registados no momento em que é espoletada a gravação. Esta Comissão, porém, sobre este ponto, não dispõe de informação suficiente que lhe permita realizar um juízo sustentado sobre este relevante aspeto, ainda que, sempre se diga, deverão ser implementadas medidas técnicas e de segurança que não permitam, então, um qualquer uso diferente desses dados que não aqueles que se enunciaram.

68. De resto, louva-se que também se tenha feito constar que relativamente à recolha de imagens de terceiros que não estejam diretamente relacionados com o evento de intervenção policial, o sistema permitirá a colocação de “máscaras” capazes de ocultar da gravação elementos não essenciais à obtenção de prova em vista a uma eventual partilha autorizada legalmente, nomeadamente com autoridade judiciária, mantendo-se o original inalterado no sistema.

69. As câmaras permitem entrar no modo “mute”, modo esse em que a câmara não guarda o registo áudio quando está no modo gravação. Esta função também deve, por definição, ser desligada, já que utilização destes sistemas pressupõe a gravação de imagem e som.

70. Relativamente à utilização de dispositivos *smartphone* emparelhados, estes devem, também, não ser permitidos, e desativada a função previamente, na medida em que se poderão permitir o acesso aos vídeos e

²¹ A convocar uma ponderação distinta e de distintos direitos, fora do escopo desta análise.

áudios gravados e a outras funcionalidades facultadas pela *app*, que não são conformes, desde logo, à matéria prescrita nos artigos 11.º, 12.º e 13.º do Decreto-Lei n.º 2/2023.

71. Apesar de longa, crê-se importante, neste ponto, deixar-se a citação dos referidos artigos, não compagináveis com acessos remotos, em direto ou não, que permitam obviar às seguintes prescrições imperativas:

Artigo 11.º

Sistema de gestão e armazenamento dos dados captados

- 1 - Os dados captados pelas CPUI são geridos, catalogados e armazenados por um sistema digital de gestão e armazenamento, adiante designado por sistema.
- 2 - Os componentes do processamento, armazenamento e de manutenção do sistema são mantidos em local reservado, de acesso restrito, dotado de mecanismo de controlo e registo de acessos.
- 3 - Sem prejuízo de outras medidas de segurança, o sistema valida a comunicação com as CPUI por via do identificador único e inalterável atribuído pelo fabricante, transferindo apenas as gravações das CPUI que forem previamente autorizadas pelo comandante máximo da força, devendo estar munido de funcionalidade que exija a associação da identificação do elemento policial aos dados transferidos.
- 4 - O acesso e a transferência dos dados captados pelas CPUI são realizados exclusivamente através do sistema, nos termos do presente artigo.
- 5 - No processo de transferência dos dados captados pelas CPUI, o sistema deve garantir a sua encriptação imediata, por via do algoritmo de cifra seguro, e ainda a sua segurança, integridade e inviolabilidade, assegurando que o método de verificação da integridade esteja disponível, a título gratuito, em qualquer fase da cadeia de custódia de prova.
- 6 - No armazenamento dos dados gravados, o sistema deve obedecer aos seguintes requisitos técnicos mínimos:
 - a) Não permitir que as gravações sejam eliminadas por utilizador que não se encontre devidamente credenciado;
 - b) Eliminar as imagens gravadas nas CPUI logo que proceda à sua transferência para o sistema de armazenamento;
 - c) Garantir o armazenamento dos dados gravados, pela totalidade das câmaras associadas, por um período mínimo de 30 dias;
 - d) Decorridos 30 dias após a respetiva gravação proceder à sua destruição, exceto nas situações previstas no n.º 2 do artigo 13.º;
 - e) Ao esgotar a capacidade de armazenamento, não deve permitir a substituição dos dados já gravados;
 - f) Permitir que as gravações armazenadas incluam o número identificador único e inalterável correspondente e a data, hora e local da gravação.
- 7 - No acesso, visualização e extração dos dados gravados, o sistema deverá obedecer aos seguintes requisitos técnicos:
 - a) Permitir a definição de perfis de utilizador e respetivas permissões de acesso, designadamente de visualização, extração e de auditoria dos dados, bem como o registo de todas as alterações;
 - b) Registar todas as operações exercidas sobre os dados gravados, nomeadamente a sua visualização e extração, bem como as alterações às configurações do sistema;
 - c) Permitir a visualização por meio incorporado;
 - d) Permitir a pesquisa de gravações armazenadas por número único identificador de processo-crime (NUIPC) ou número de processo policial, data, hora e local da gravação e unidade policial ou número de identificação policial.
- 8 - Deve ser assegurada a criação de diferentes perfis de acesso que assegure que cada elemento policial tem os acessos estritamente necessários para o desempenho das respetivas funções.
- 9 - Os perfis a criar devem ser diferenciados de acordo com as funções desempenhadas, prevendo para cada um destes o respetivo âmbito e extensão, diferenciando permissões de visualização, tratamento, extração e conservação.

Artigo 12.º

Segurança e armazenamento das gravações

- 1 - As gravações são armazenadas no sistema digital de gestão e armazenamento, em ficheiro encriptado que assegure a sua inviolabilidade.
- 2 - Ao agente policial que executou a gravação não é permitido apagá-la ou alterá-la.
- 3 - A transmissão das gravações para o sistema é obrigatoriamente efetuada no final do serviço, através da colocação da CPUI em estação adequada para esse fim, sob a supervisão de superior hierárquico ou elemento policial responsável nomeado para o efeito.
- 4 - O agente policial responsável pela gravação procede, o mais rapidamente possível, à identificação do ficheiro de dados, acrescentando o NUIPC associado, quando aplicável, ou número de registo interno.
- 5 - As gravações são conservadas no sistema, em servidor exclusivo para o efeito, durante um período de 30 dias
- 6 - Excetuam-se do disposto no número anterior as gravações apresentadas como prova em processos judiciais ou procedimentos disciplinares, as quais devem ser eliminadas logo que comunicado pela autoridade judiciária ou entidade

decisora do procedimento que cessou a necessidade da sua conservação.

Artigo 13.º

Acesso a gravações

1 - Exceto nas situações previstas no presente artigo, é proibido o acesso, cópia ou transmissão de imagens ou som recolhidos.

2 - As gravações de imagens e som recolhidos só podem ser acedidas nas seguintes situações:

- a) No âmbito de processo de natureza criminal;
- b) No âmbito de processo de natureza disciplinar contra agente das forças de segurança;
- c) Para apurar a eventual existência de infração disciplinar, quando for o caso, ou criminal por ou contra o agente policial;
- d) Para inspecionar as circunstâncias da intervenção policial, sempre que tal seja fundamentadamente determinado pelo dirigente máximo da força de segurança.

3 - O acesso às gravações apenas é permitido aos agentes policiais devidamente credenciados para o efeito, através do sistema, em estação de trabalho fixa colocada em instalação policial.

4 - Todas as operações de acesso às gravações são registadas no sistema, com indicação da data e hora, justificação e identificação do responsável pela intervenção.

72. Em reforço, afirma-se nos requisitos a cumprir pelos aparelhos (artigo 16.º do Decreto-Lei n.º), que as câmaras não podem permitir a eliminação ou alteração das imagens gravadas (f) e que não podem permitir a extração de imagens gravadas, exceto através de estação específica, destinada a esse fim (g). [sublinhado nosso].

73. Deverá, também, ser configurada uma “marca de água” com a informação prevista no artigo 11.º, nº 6, alínea f).

74. O correto uso das câmaras prevê que o agente insira a câmara que tem atribuída na estação Axon Dock no final do serviço. Esta estação carregará a bateria da câmara e enviará os filmes capturados para o servidor, eliminando-os imediatamente após confirmação do sucesso do envio.

75. O sistema centra a recolha das gravações no servidor Axon Evidence. O fabricante oferece duas modalidades para a configuração desta solução: utilização de um servidor remoto, em solução de nuvem (Axon Evidence.com²²); utilização de um servidor local (Axon Evidence Local), mantido nas instalações da entidade responsável.

76. No manual da câmara Axon Body 3, que acompanha o ofício, é mencionada a aplicação Axon Commander, como sistema de recolha centralizado das gravações. Essa aplicação deverá ser instalada numa máquina local na infraestrutura do responsável.

22 Com acesso através da internet usando o URL https://nome_organizacao.evidence.com (https://my.axon.com/s/article/Accessing-your-agency?language=en_US); trata-se de uma solução na nuvem Azure, detida pela Microsoft ([https://partner.microsoft.com/en-us/case-studies/axonevidence#:~:text=Built%20on%20Microsoft%20Azure%2C%20Axon,%2C%20efficient%2C%20and%20trustworthy%20way.\);](https://partner.microsoft.com/en-us/case-studies/axonevidence#:~:text=Built%20on%20Microsoft%20Azure%2C%20Axon,%2C%20efficient%2C%20and%20trustworthy%20way.);) <https://www.axon.com/news/secure-dems-storage>

77. Sucede que, analisando a versão *online* do manual da câmara Axon Body 3, atualizada a maio de 2024²³, a aplicação Axon Commander deixou de ser mencionada, tendo sido substituída pela Axon Evidence, que pode ter duas configurações distintas, como referido no ponto anterior.

78. Além disso, na parte C. do nº1 do Anexo D junto aos autos, afirma-se que “[...] [O] armazenamento e [...] preservação da informação (vídeo e áudio) está de acordo com o preconizado pelo Gabinete Nacional de Segurança (GNS) para estes casos. Toda a informação será recolhida e armazenada de forma digital pelo período legalmente estabelecido, findo o qual serão eliminados os elementos recolhidos. Durante este período, a informação é armazenada no servidor Microsoft Azure, dentro da União Europeia, numa cloud protegida por protocolos de segurança [...] e existindo um controlo efetivo dos elementos que possuem acesso aos dados.”.

79. Compulsados os documentos enviados, neles se refere, amiúde, que os dados de vídeo e áudio gravados nas câmaras são transferidos para o “[...] servidor/software Evidence ou Commander”.

80. Como mencionado atrás, a versão mais atual do manual da câmara Axon Body 3 não refere a aplicação Axon Commander, tendo-a substituído pela Axon Evidence, que pode ser implementada em duas soluções: em nuvem (Axon Evidence.com) ou instalada localmente (Axon Evidence.com), não se conseguindo alcançar qual das duas soluções foi a adotada.

81. Tudo parece indicar, porém, que a solução escolhida para o armazenamento das imagens no servidor Axon Evidence foi a solução em nuvem (Axon Evidence.com), em detrimento da versão Axon Evidence Local (ou eventualmente a Axon Commander), que permitiria ter as mesmas funcionalidades em máquinas administradas pela entidade.

82. A plataforma de nuvem onde a plataforma Axon Evidence.com está alojada é a Azure²⁴, gerida pela empresa Microsoft Corporation, com sede nos Estados Unidos da América, i.e., país terceiro em relação à União.

83. Sobre este sensível ponto, não poderá deixar de referir-se que, em 16 de Junho de 2018, o EDPS (European Data Protection Supervisor) publicou as “*Guidelines On The Use of Cloud Computing services by the European Institutions and Bodies*”, onde se deixaram um conjunto de alertas e recomendações acerca da utilização dos serviços “cloud” e dos seus riscos para a proteção de dados que, apesar de dirigidos a instituições, órgãos e agências europeias serão também para aqui transponíveis, pela natureza dos dados e qualidade subjetiva dos

23 Na secção “User guides” em https://my.axon.com/s/axon-body-3?language=en_US

24 <https://www.axon.com/news/secure-dems-storage>; https://partner.microsoft.com/en-us/case-studies/axonevidence#:~:text=Built%20on%20Microsoft%20Azure%2C%20Axon,%2C%20efficient%2C%20and%20trustworthy%20way;https://azuremarketplace.microsoft.com/en-US/marketplace/apps/axon.axon_evidence?tab=overview

responsáveis pelo tratamento no caso presente, que deverá tomá-las em consideração na avaliação do uso destes serviços.

84. Mais, não pode também deixar de se referir que o EDPS, após uma investigação sobre a utilização do *Microsoft 365* pelas instituições europeias, emitiu, a 8 de março de 2024, uma ordem de limitação de utilização deste software, exatamente por ter recolhido provas que o sistema em causa não é seguro²⁵.

85. Ainda que se afirme a existência de controlo efetivo dos dados e que se deixe *en passant* que os servidores estão situados na União Europeia e, portanto, sujeita a informação às regras vinculativas europeias, não poderá deixar-se de considerar que, tratando-se de dados relacionados com matéria de eventual prevenção, deteção, investigação ou repressão de infrações penais, ou de segurança nacional, nomeadamente de uso probatório, sob responsabilidade de OPC português, deverá ponderar-se a utilização de servidores locais ou nacionais, conquanto, naturalmente, se cumpram todas as medidas técnicas e de segurança em vista à integridade, exatidão e confidencialidade dos dados armazenados e tratados, atendendo às características e sensibilidade dos tratamentos que se pretendem realizar²⁶.

86. De facto, daquele documento poderá resultar como interpretação, *passim*, que poderão conceber-se circunstâncias em que o país terceiro, por razão legislativa pública própria, supervenientes, emergentes, controláveis ou não, possa introduzir regras que autorizem o acesso à informação. Desejavelmente, a informação, tanto mais sensível e de interesse nacional que ela seja, deve estar do domínio total do seu responsável²⁷.

87. A circunstância de, em 10 de julho de 2023, a Comissão Europeia, nos termos dos artigos 44.º e 45.º do RGPD, ter adotado uma decisão de adequação em relação à transferência internacional de dados entre a União Europeia e os Estados Unidos da América²⁸, que inclui a empresa Microsoft, não afasta as razões que se acabam de invocar nos termos que aqui se expuseram, uma vez que o risco de possibilidade de transferências deste tipo de dados deve, simplesmente, procurar eliminar-se.

²⁵ Disponível em https://www.edps.europa.eu/system/files/2024-03/24-03-08-edps-investigation-ec-microsoft365_en.pdf

²⁶ Veja-se, a este propósito, a Directriz 1/2023, da autoria desta Comissão.

²⁷ Na página 39 dessas “Guidelines” pode ler-se: “Therefore, in the light of the above, the EDPS recommends that -as a rule- the processing of personal data entrusted by EU institutions to CSPs (including for back up, business continuity purposes and transit, as well as locations from where remote operations are performed), and any sub-processing, takes place within the EU”

²⁸ Disponível em https://commission.europa.eu/document/download/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en?filename=Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf

88. E, o Legislador, no artigo 12.º n.º 5 do Decreto-Lei n.º 2/2023 dita que: “5 - As gravações são conservadas no sistema, em servidor exclusivo para o efeito, durante um período de 30 dias” [sublinhado nosso], o que parece ir ao encontro do que se acaba de recomendar.

89. Finalmente, nos documentos juntos afirma-se, também, a eliminação dos vídeos armazenados no sistema Axon Evidence que não foram selecionados para prova e que já ultrapassaram o prazo de 30 dias. Nada se diz, porém, sobre o modo como essa eliminação é efetuada, em concreto, se resulta de um processo automático ou manual.

90. Como também se retira do trecho citado, deve ser seguido escrupulosamente o prazo de conservação a que a Lei n.º alude, criando-se mecanismos procedimentais que garantam esse mesmo cumprimento.

IV. Conclusão

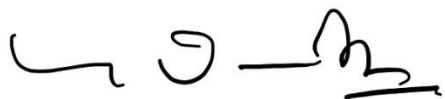
53. Nos termos e com os fundamentos expostos a CNPD recomenda:

- a) Determinar-se a utilização das câmaras portáteis de uso individual em razão dos fins previstos no artigo 3.º da Lei n.º 95/2021, enquanto condição concreta, necessária e autorizante para o tratamento de dados em causa, conforme melhor exposto no ponto I. deste parecer;
- b) Garantir-se que as câmaras sejam pré-configuradas antes da sua colocação em utilização pelos operadores, cumprindo as regras previstas no Decreto-Lei n.º 2/2023, sem possibilidade de poderem ser alteradas essas configurações nos aparelhos ou pelos operadores;
- c) Garantir-se que a encriptação nas câmaras está ativa para o conteúdo do disco onde as imagens e som são gravados, não só na utilização de recolha de imagens e som, mas também no processo de transferência dos dados captados e guardados;
- d) Garantir-se a rastreabilidade subjetiva e objetiva de qualquer operação no tocante à utilização das câmaras, bem como em relação a qualquer acesso aos dados, entendendo-se por “acesso” qualquer intervenção realizada no sistema que tenha por objeto, direta ou indiretamente, as referidas gravações, bem como dever fixarem-se com clareza as atribuições de perfis de manipulação do sistema que permitam exercitar um mecanismo de *checks and balances*, não permitindo a sobreposição

concentrada de possibilidades de operação/acesso/configuração/alteração/eliminação nos mesmos utilizadores.

- e) Garantir-se que as câmaras não podem operar no modo gravação sem terem sido previamente atribuídas a um agente/operador.
- f) Garantir-se a impossibilidade de utilização, controlo ou alteração de definições através de aplicação para *smartphone*, ou através de tecnologia Wi-Fi ou LTE;
- g) Garantir-se que o *buffer* de gravação do aparelho se restringe aos 30 segundos previstos no número 2 do artigo 7.º do Decreto-Lei n.º 2/2023.
- h) Garantir-se a não utilização do modo furtivo, ou *stealth*, pelas razões melhor explicadas em 50 e seguintes deste parecer;
- i) Garantir-se a implementação de medidas técnicas e de segurança que não permitam a utilização de informação ou uso de geolocalização quando não se esteja a proceder a gravação;
- j) Definirem-se as câmaras para não ser possível a utilização da função “mute”;
- k) Configurarem-se os aparelhos para registarem “marca de água” com a informação prevista no artigo 11.º, nº 6, alínea f);
- l) Tratando-se de dados relacionados com matéria de eventual prevenção, deteção, investigação ou repressão de infrações penais, ou de segurança nacional, nomeadamente de uso probatório, sob responsabilidade de OPC português, deverá ponderar-se a utilização de servidores locais ou nacionais, em qualquer caso, sob domínio do responsável pelo tratamento, e especialmente criados para esse fim;
- m) Garantir-se o cumprimento do prazo de conservação de 30 dias que a legislação determina, criando-se mecanismos procedimentais, eventualmente automatizados, que garantam essa mesma sujeição.

Lisboa, 6 de agosto de 2024



Luis Barroso (Vogal em substituição da Presidente)