

## DELIBERAÇÃO/2020/292

### I. Introdução

1. O VITÓRIA SPORT CLUBE - FUTEBOL SAD (NIPC 510646638) e o VITÓRIA SPORT CLUBE (NIPC 501144013), ambos com sede na Praça 26 de Maio, 4810-914 Guimarães, grupo empresarial (VSC) submeteu a consulta prévia da Comissão Nacional de Proteção de Dados (CNPd) uma avaliação de impacto sobre a proteção de dados em relação à utilização de tecnologias de reconhecimento facial associadas a um circuito fechado de videovigilância instalado no Estádio D. Afonso Henriques com a exclusiva finalidade de identificar e impedir a entrada de indivíduos sobre os quais recaia uma proibição judicial ou administrativa de ingresso no recinto desportivo.
2. O sistema destina-se, segundo os requerentes, a funcionar *exclusivamente em espetáculos desportivos de natureza profissional ou não profissional considerados de risco elevado, de âmbito nacional ou internacional*, seguindo a qualificação prevista no artigo 12.º da Lei n.º 39/2009, de 30 de Julho, segurança e combate ao racismo, à xenofobia e à intolerância nos espetáculos desportivos, sucessivamente alterada, em último pela Lei n.º 113/2019, de 11 de setembro (doravante Lei n.º 39/2009).
3. Apesar da finalidade declarada e citada no ponto 1, é também descrita a utilização da tecnologia *Unusual Motion Detection*, com a qual, de acordo com o declarado pelos requerentes, *não [se] pretende fazer a análise de dados pessoais ou traçar perfis, mas, tão-só alertar a segurança do recinto para movimentos considerados anormais, de acordo com quatro vetores: velocidade, presença, ausência e localização*.
4. A CNPD nota que, salvo quanto a casos específicos<sup>1</sup>, não lhe compete aprovar tratamentos, mas tão-só, à luz do disposto nas disposições combinadas dos n.ºs 1 e 2 do artigo 36.º e alínea I) do n.º 1 do artigo 57.º do Regulamento (UE) 2016/679 – Regulamento Geral sobre a Proteção de Dados (RGPD), dar orientações sobre as operações de tratamento, podendo, ainda exercer todos os poderes previstos no artigo 58.º desse regulamento.

---

<sup>1</sup> Sendo eles os previstos no n.º 5 do artigo 36.º do RGPD.

5. A avaliação de impacto sobre a proteção de dados (AIPD), prevista no artigo 35.º do RGPD, demonstra-se omissa quanto a vários aspetos críticos do sistema.
6. É certo e reconhecido pelo requerente a inexistência de um enquadramento legal que claramente autorize a utilização destes sistemas para a(s) finalidade(s) declarada(s).

## II. Descrição do sistema reconhecimento facial

7. De acordo com o descrito pelo requerente, o sistema será composto por:

- *Duas câmaras H5A Camera Line da Avigilon, dotadas de CNN, ou seja, tecnologia de análise inteligente de vídeo (Inteligência artificial), sendo uma de 6 megapíxeis e outra de 4 megapíxeis, tendo, cada uma, pelo menos, 10 regras definidas;*
- *middleware analytics appliance para aplicação da analítica sobre as 9 câmaras móveis IP modelo SD49225T e a câmara fixa do atual sistema de videovigilância;*
- *servidor de gravação e gestão de vídeo onde serão conservadas as imagens, não tendo este servidor qualquer ligação à rede e sendo acessível remotamente pela Avigilon apenas mediante solicitação e autorização do VSC, em caso de necessidade de assistência técnica;*
- *comutador para alimentação das câmaras PoE ou PoE+, conforme padrão IEEE 802.3af ou IEEE 802.3at, de camada de enlace (Layer 2);*

8. Neste ponto da descrição técnica do sistema, estranham-se algumas asserções dos requerentes quanto a capacidades contraditórias ou, pelo menos, de dúvida viabilidade. Como exemplo disso mesmo, refira-se a garantia de que o servidor não possui qualquer ligação à rede, para, logo de seguida, se afirmar a possibilidade de ser acessível remotamente.

9. Voltando ao declarado pelo requerente, *O software inclui um pacote de licença de reconhecimento facial; Uma licença de software base; Um pacote de serviços de analíticas (de análise de violações das regras criadas após período de estudo e aprendizagem da "normalidade"), sendo estas, as seguintes:*

- i. *Objectos na área – O evento é disparado quando o tipo de objecto seleccionado se move para a região de interesse;*

- ii. *Objectos de permanência prolongada – O evento é disparado quando o tipo de objecto seleccionado permanece dentro da região de interesse por um período prolongado;*
- iii. *Objectos cruzando o feixe – O evento é disparado quando um número especificado de objectos atravessa o feixe direccionado, que foi configurado no campo de visão da câmara. O feixe pode ser unidireccional ou bidireccional;*
- iv. *Objectos aparecem ou entram na área – O evento é disparado por todos os objectos que entram na região de interesse. Esse evento pode ser usado para contar objectos;*
- v. *Objectos não estão presentes na área – O evento é disparado quando não há objectos presentes na região de interesse;*
- vi. *Objectos entram na área – O evento é disparado quando um número especificado de objetos entra na região de interesse;*
- vii. *Objectos deixam a área – O evento é disparado quando o número especificado de objetos sai da região de interesse;*
- viii. *Objectos parados na área – O evento é disparado quando um objecto, que é detectado numa região de interesse, para de se mover, por um limite de tempo especificado;*
- ix. *Direcção violada – O evento é disparado quando um objecto se movimenta numa direcção de movimento proibida;*
- x. *Detecção de violação – O evento é disparado quando a cena muda inesperadamente.*

Esta descrição do software aparenta respeitar apenas ao sistema *Unusual Motion Detection*.

O requerente declara que *esta tecnologia, em síntese, é capaz de captar, processar e analisar metadados de identificação de imagem e biometria, através de um software que permite a qualificação do objecto captado, de acordo com a sua aparência, permitindo, em abstracto, efectuar procura avançada por aparências físicas de pessoas.*

Declara, ainda, que *As imagens apenas poderão ser visualizadas em computador instalado na sala de videovigilância, mediante introdução de password de pessoa autorizada a visualizar as imagens.*

### III. Dados pessoais tratados

10. Para que a finalidade principal (a sinalização dos titulares de dados sujeitos a decisão de interdição e cumprimento dessa decisão) do tratamento seja atingida, é utilizado um conjunto de dados que resulta da combinação da informação previamente transmitida

aos promotores do espetáculo desportivo (como o requerente) com as imagens captadas pelo sistema de videovigilância previsto no n.º 1 do artigo 18.º o qual, para além do recinto desportivo, abarca o respetivo anel ou perímetro de segurança.

11. Os titulares dos dados que compõem o universo de pessoas a quem se aplica proibição judicial ou administrativa de ingresso no recinto desportivo não podem desconhecer a obrigação legal de remeter tais dados pessoais aos promotores dos espetáculos desportivos<sup>2</sup>, a qual impende sobre quem deve determinar essa proibição.
12. Neste sentido, a decisão sobre a proibição é disponibilizada aos promotores dos espetáculos desportivos, nos termos do n.º 1 do artigo 38.º (também *ex vi* n.º 2 do artigo 42.º).
13. Na Lei n.º 39/2009 não vêm previstas as categorias de dados pessoais que devem ser transmitidas aos promotores, embora se admita que o conceito de “decisões” abarque, pelo menos, o nome, um elemento de identificação (Cartão do Cidadão ou outro documento equivalente) e o conteúdo da decisão.
14. Não é claro como é obtida a fotografia da pessoa sujeita à proibição judicial ou administrativa de ingresso no recinto desportivo, já que tal não é descrito pelo requerente, mas antecipa-se que essa informação seja também disponibilizada pela entidade que decretou a proibição.
15. O sistema de videovigilância referido no ponto 10 recolhe, como é evidente, imagens de todos aqueles que entram ou apenas circulam no respetivo anel ou perímetro de segurança.
16. É declarado pelo requerente o tratamento dos dados *nome, número de identificação civil, imagens* do público em geral, fotografias dos indivíduos sujeitos a decisão de interdição e respetivas sentenças ou decisões que as aplicam.
17. No campo dos dados biométricos e quanto ao público em geral, descreve-se a recolha de “*metadados biométricos*”, indicando-se a existência de *reconhecimento facial captado em dia de evento desportivo - análise das características biométricas*

---

<sup>2</sup> Como vêm descritos na alínea k) do artigo 3.º da Lei n.º 39/2009.

L

*i. Detecção da face; ii. Criação de template numérico baseado nas características da face captada.*

18. Quanto aos titulares dos dados sujeitos a medida de interdição, declara-se serem recolhidos “*metadados biométricos*” (*template numérico*) *obtidos a partir das fotografias* em posse do requerente.

19. Finalmente, os prazos de conservação especificados são os seguintes:

- a. O nome e o número de identificação civil serão mantidos enquanto durar a medida de restrição;
- b. As imagens captadas pelo sistema de videovigilância respeitarão o prazo de 60 dias previsto no artigo 18.º da Lei n.º 39/2009;
- c. Dados biométricos:
  - i. “metadados” relativos ao público em geral - *Tempo necessário à execução do estudo (Comparação deste template com os conservados em base de dados). Eliminação automática em caso de não coincidência / durante a execução do estudo;*
  - ii. “metadados” relativos aos interditos - *enquanto durar a ordem de restrição, sendo comparados, sistematicamente, com os metadados biométricos captados em dia de evento desportivo.*

20. Sobre as fotografias nada se diz quanto ao prazo de conservação.

#### IV. Fluxos internos de dados

21. Das informações prestadas no documento, conclui-se haver os seguintes fluxos internos de tratamento de dados:

- Reconhecimento facial
  - a. O sistema de videovigilância capta e grava as imagens;



- b. aproximadamente 5 segundos depois, o software de reconhecimento facial capta os dados biométricos das imagens gravadas, analisa a aparência dos objetos captados, pré-qualifica os objetos em categorias (pessoas, carros, garrafas, etc), quando identifica a categoria pessoa tenta focar a cara e criar o *template* numérico baseado nas características físicas (posição relativa dos seus componentes, tamanho e características distintivas); o *template* numérico é comparado com os *templates* constantes da base de dados;
  - c. se houver coincidência, é lançado um alarme e é solicitada a intervenção de autoridade competente para confirmação da fidedignidade do alarme, como forma de evitar falsos-positivos;
  - d. a autoridade acede ao sistema, que lhe permitirá, então, reconstituir o percurso do indivíduo em causa, captado em câmara, e descobrir a sua localização nos 5 segundos anteriores ao momento atual;
- *Unusual motion detection*
    - a. após uma primeira fase de estudo e aprendizagem do que é considerado como "normalidade" quanto aos acontecimentos dentro de um estádio de futebol, o software será capaz de detetar movimentos de massas "não padrão", mediante a alteração dos parâmetros normalmente medidos para a ausência, presença, velocidade e localização de objetos ou multidões em locais específicos do estádio.
    - b. aproximadamente 5 segundos depois de o sistema de videovigilância gravar as imagens, o sistema realiza a análise para detetar movimentos de massas "não padrão", mediante a alteração dos parâmetros normalmente medidos para a ausência, presença, velocidade e localização de objetos ou multidões em locais específicos do estádio.

## V. Entidades Envolvidas

22. Para além do VSC, existem 3 entidades subcontratantes que prestam serviços relacionados com o CCTV e a tecnologia à qual se recorrerá para o tratamento em apreço, cada um com *uma função específica, com um propósito perfeitamente delimitado* e com as quais o VSC realizou um DPA – Data Processing Agreement, o que configurará um contrato na aceção do artigo 28.º do RGPD.

23. É afirmado que as Forças e Serviços de Segurança (FSS) *terão acesso aos resultados da aplicação desta tecnologia, ou seja, terão acesso às identificações de indivíduos que permaneçam indevidamente no estádio e sua localização.*

24. Propõe-se, ainda, *que sejam os elementos das FSS a assumir a responsabilidade de determinar a validade do reconhecimento, eliminando os falsos positivos, atuando, assim, como terceiros, com finalidades próprias.* Mas tal dependerá *de avaliação própria por parte das FSS, enquanto responsável pelo tratamento.* Para além da fragilização do processo de verificação da identidade das pessoas sujeitas a medida de interdição, não se percebe quais as finalidades próprias em causa. Também a atribuição às FSS da qualidade de responsável pelo tratamento, no presente contexto, afigura-se como problemática, já que apenas lhes competiria, caso aceitassem a proposta do VSC, validar resultados positivos devolvidos pelo sistema e atuar seguidamente na esfera das suas competências.

25. No que respeita às “regras aplicáveis ao tratamento” está previsto:

- A obrigação de os subcontratantes oferecerem garantias de segurança no mínimo iguais às do VSC;
- A responsabilização da empresa e pessoal dos técnicos dos subcontratantes no caso de não ser respeitado o sigilo, os dados serem copiados para dispositivos não aprovados, serem enviados por email não encriptado ou serem utilizados para finalidades diferentes das previstas na avaliação de impacto;
- O VSC só acederá aos dados *quando a isso for legalmente obrigado ou quando estiver a prosseguir ou defender interesses ou direitos legalmente protegidos, no âmbito de processo crime;*
- O acesso à sala de videovigilância por um alargado grupo de pessoas e entidades:
  - Do VSC: o responsável pelo departamento de IT, o responsável pelo departamento de gestão de infraestruturas e equipamentos desportivos (ou em quem este delegue competência por escrito), o diretor de segurança e o diretor de campo;



- O subcontratante que presta serviços relacionados com a manutenção do sistema de videovigilância e dados por ele armazenados;
- O subcontratante que presta serviços de segurança privada, nos quais se incluem a gestão e a monitorização de videovigilância no papel de assistente do recinto desportivo nos termos do artigo 3.º da Lei n.º 113/2019;
- As FSS e as autoridades administrativas ou judiciais;
- A empresa de manutenção do sistema de deteção de incêndios por intermédio do responsável pelo departamento de gestão de infraestruturas e equipamentos desportivos (ou em quem este delegue competência por escrito);
- O EPD, sempre que o solicite ao responsável pelo departamento de IT ou ao responsável pelo departamento de gestão de infraestruturas e equipamentos desportivos;
- O único ponto onde as imagens de videovigilância podem ser visualizadas é um computador instalado na sala de videovigilância, mediante introdução de *password*, não sendo explicitamente indicado se há utilizadores nominais para quem realize o acesso.

## VI. Medidas implementadas

26. O requerente indicou que implementará as seguintes medidas de segurança

- Cifragem – é referido que o sistema permite a encriptação a 256 bits na captura do vídeo, transporte e na apresentação ao utilizador – não se percebe de que forma se pode utilizar cifragem na apresentação de imagens ao utilizador;
- Controlo de acesso físico / organização
  - o acesso à sala de CCTV é controlado e feito por cartões com tecnologia RFID atribuídos ao grande número de entidades já enumeradas em “regras aplicáveis ao tratamento”. O VSC informa ainda que é guardado registo apenas referente aos últimos 50 acessos, propondo uma melhoria ao sistema que permita conservar o registo de todos os acessos à sala por um período mínimo de 60 dias e a assinatura de termo de responsabilidade que explicitamente estabeleça que o cartão é pessoal e intransmissível – Apesar de a medida de



alargar o prazo de conservação dos registos de acesso ser positiva, bem como a explicitação da não partilha do cartão, não se pode considerar o acesso previsto seguro, dado estar baseado apenas num fator, o cartão, que pode ser objeto, mesmo sem ónus por parte do seu detentor, por exemplo, de perda ou furto. É necessário, portanto, serem previstos fatores adicionais que apenas sejam do conhecimento do detentor, como por exemplo password;

- neste ponto, é referido um sistema de gestão interno nunca antes referido no documento, nem contextualizado. Merecendo concordância a previsão de segmentar acessos de acordo com funções específicas, independentemente do sistema em causa, não é possível fazer qualquer avaliação adicional de um sistema desconhecido;
- Política – acordo de confidencialidade, regras procedimentais e de segurança;
- Logs – o VSC afirma que *serão definidos perfis de utilizadores conforme o tipo de operador e as funções/informações a que pode aceder*, não indicando quantos e quais os tipos de funções, e consequentemente de perfis, que estão previstos. Também não se encontra especificada a informação que será guardada nem o prazo de conservação dos logs;
- Acesso lógico<sup>3</sup>
  - Será realizado registo em papel dos acessos às imagens gravadas e à base de dados biométricos com a data, hora, autoria, fundamentação e, sempre que possível, parecer do EPD sobre a necessidade do acesso. Caso não seja possível obter o parecer previamente, o EPD terá conhecimento *à posteriori*;
  - O VSC declara que *“não deverão ser introduzidos nesta sala quaisquer smart devices, (smartphone, tablet, etc.) câmara de vídeo ou câmara fotográfica”* – sugere-se uma alteração da formulação para tornar a intenção uma proibição;
  - *“O acesso e download de imagens, bem como a atualização e acesso à base de dados biométricos apenas será possível pela introdução conjunta das passwords do responsável pelo departamento de IT e do responsável pelo departamento de gestão de infraestruturas e equipamentos desportivos.”* – não fica claro se esta introdução conjunta de passwords é complementar à

---

<sup>3</sup> O requerente identifica ou agrupa erradamente estas como medidas referentes aos acessos físicos.

autenticação por parte de quem efetivamente realizará o acesso, sendo essencial que assim seja para permitir o correto registo eletrónico do acesso.

## VII. Quanto aos riscos considerados e sua avaliação

27. O requerente considerou três riscos potenciais: Acesso ilegítimo aos dados, Modificação indesejada dos dados e Desaparecimento de dados – identificando, para cada um deles, os impactos para os titulares dos dados, as ameaças que a eles podem conduzir, as fontes do risco, as medidas estabelecidas que podem contribuir para mitigar o risco, e classificando-os quanto à probabilidade e à gravidade. Resume tal classificação na imagem seguinte:

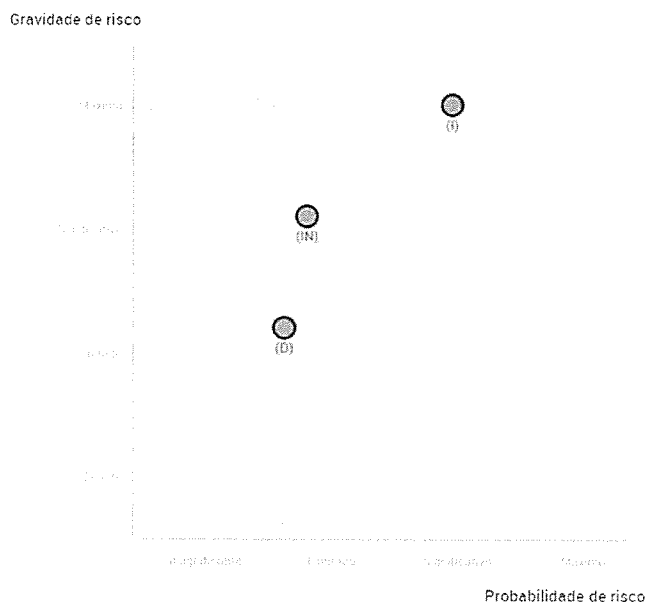


Figura 1 – Classificação, quanto à gravidade e à probabilidade, dos 3 riscos identificados - Acesso ilegítimo aos dados (I), Modificação indesejada dos dados (IN) e Desaparecimento de dados (D)

28. De acordo com a classificação padronizada (risco insignificante, limitado, significativo e máximo), foi atribuído um nível máximo da gravidade e significativo da probabilidade ao potencial acesso ilegítimo aos dados, enquanto o risco de modificação indesejada dos dados apresentou um nível significativo de gravidade e limitado de probabilidade. Finalmente, o risco de desaparecimento dos dados mereceu um nível limitado nessas duas categorias.



### VIII. Apreciação

29. Os tratamentos de dados pessoais visados pelo requerente representam um aprofundamento muito considerável das capacidades do sistema de videovigilância atualmente instalado.

30. Ainda que a consulta prévia não se destine a autorizar os tratamentos levados a cabo pelos responsáveis pelo tratamento, a CNPD entende que a pronúncia que lhe compete não se pode remeter apenas aos aspetos valorados como de elevado risco por aqueles.

31. Ainda assim, comecemos por sinalizar quais os aspetos que, na ótica do requerente, configuram um risco elevado nos tratamentos sujeitos a avaliação:

- a. Quanto aos princípios fundamentais de proteção de dados, foi considerado existir um elevado risco quanto à salvaguarda do princípio da minimização de dados. Não é feita qualquer explicação sobre esse resultado, mas depreende-se que a conclusão decorre do facto de todos os titulares dos dados presentes no recinto e no perímetro de segurança do mesmo poderem ser visados pelo tratamento, ainda que nenhuma decisão de interdição tenha sido tomada contra eles. Aliás, toda a argumentação expendida pelo requerente parece indicar não existir outra solução que garanta a finalidade visada com idêntica eficácia, dando-se conta da dificuldade da identificação individual à entrada dos recintos desportivos e das soluções pouco equilibradas ou exequíveis da lei, quanto à obrigatoriedade, por parte dos interditos, de apresentação na esquadra em horas coincidentes com as dos espetáculos desportivos;
- b. Na avaliação dos riscos e especificamente quanto à potencial ocorrência de um “acesso ilegítimo [a]os dados” (cfr. pág. 37 e ss.), atribui-se um nível máximo à “gravidade do risco, especialmente de acordo com impactos potenciais e controlos planeados”, sendo a probabilidade do mesmo ocorrer “significativa” e resultando a avaliação global num “Risco alto”. Está aqui em causa a intromissão no local onde são visionadas e conservadas as imagens, o que poderá advir de uma intervenção humana “negligente ou dolosa”, podendo dela decorrer a “intromissão na vida privada de um titular não visado pela tecnologia”. Reconhece-se que qualquer sistema com as características do sujeito a avaliação de impacto pode causar uma intromissão na vida privada de qualquer dos titulares dos dados por ele captados, mas tal pode e deve ser



mitigado através de medidas técnicas e organizativas adequadas. Neste aspeto, a CNPD reconhece o acerto da intenção de alargar o prazo de conservação dos registos de acesso, bem como a explicitação da não partilha do cartão do pessoal devidamente autorizado. No entanto, estando o controlo de acessos limitado a um fator, no caso, o cartão atribuído a quem deva aceder e/ou frequentar os locais referidos, essas medidas revelam-se insuficientes, dado apenas estar em causa um único fator - o cartão - que pode ser extraviado ou perdido. É necessário, portanto, serem previstos fatores adicionais como por exemplo password;

- c. Quanto à modificação indesejada dos dados, cuja avaliação de risco permitiu sinalizar a hipótese de identificações erradas de titulares dos dados e invasão da sua privacidade, por força dos resultados “falsos-positivos” que o sistema possa devolver, importa registar duas notas. A primeira quanto à classificação destes riscos. Podendo existir uma potencial ameaça à integridade dos dados através da sua modificação intencional ou negligente, a matéria dos falsos positivos ultrapassa largamente esse domínio, ligando-se entre outros aspetos, à própria robustez e fiabilidade da tecnologia utilizada.

Depois, a existência destes resultados errados ou anómalos não pode deixar de ser considerada como de elevado risco quando diga respeito a uma situação como a que aqui se coloca. Sendo provável ou, pelo menos, possível que sejam erradamente identificadas pessoas como estando interditas de aceder a recintos desportivos, tal é duplamente penalizador. Por um lado, esse falso-positivo pode redundar no impedimento à entrada num dado espaço por quem tem toda a legitimidade para o frequentar. Depois, ainda que a atuação das autoridades ou dos seguranças do recinto seja discreta, ela dificilmente evitará a publicitação dessa condição, o que afeta a reputação do titular dos dados, produzindo um efeito estigmatizante intolerável. Acresce que é o próprio responsável pelo tratamento que não garante que haja uma verificação dos resultados obtidos pela análise biométrica, já que as autoridades policiais têm inteira liberdade para aceitar ou declinar o papel fiscalizador que o responsável pelo tratamento lhes pretende atribuir.



- d. Há, no entanto, um aspeto mais crítico relacionado com o aspeto já sublinhado da fiabilidade do sistema que a CNPD não pode avaliar. É que o responsável pelo tratamento em nenhum momento demonstra ter avaliado a probabilidade desses falsos-positivos, um dos elementos fundamentais na avaliação da adequação do meio à finalidade<sup>4</sup>. Como pode admitir-se a utilização deste sistema de confirmação de identidade sem que se conheça em detalhe o seu grau de fiabilidade, sobretudo quando em causa estão categorias de dados “relacionad[a]s com condenações penais e infrações” (cfr. artigo 10.º do RGPD)? E este é um aspeto a que voltaremos.

32. A CNPD nota que a avaliação de impacto excluiu qualquer consideração sobre a utilização da tecnologia *Unusual Motion Detection*. Tal ligar-se-á à errónea interpretação que o responsável pelo tratamento terá feito do que constitui ou não um dado pessoal. Ao afirmar que *Esta tecnologia não pretende fazer a análise de dados pessoais ou traçar perfis, mas, tão-só alertar a segurança do recinto para movimentos considerados anormais*, confunde-se a intenção com a finalidade.

33. Note-se que é o próprio responsável pelo tratamento que admite que esta tecnologia permitirá efetuar procura avançada por aparências físicas de pessoas, sendo mesmo descrito como *o ponto de partida para identificar, através da videovigilância, espectadores que cometam algum crime ou contraordenação*<sup>5</sup> de forma automatizada.

34. Com efeito, não é apenas dado pessoal aquele que diretamente permite a identificação de uma pessoa, mas é-o também toda a informação que contribua para essa identificação, atento o conceito abrangente do n.º 1 do artigo 4.º do RGPD e conhecida que é a posição do Tribunal de Justiça da União Europeia sobre esta matéria (em especial o Acórdão de 19 de outubro, C-582/14, pontos 41-45, ECLI:EU:C\_2016:779).

35. Deste modo, no momento presente, não parecem estar reunidas as condições para a operacionalização desta tecnologia por falta deste requisito formal, sem prejuízo de sobre ele se

<sup>4</sup> Sobre a utilização desta tecnologia, o Comité Europeu para a Proteção de Dados produziu algumas notas úteis no ponto 5 das orientações sobre o tratamento de dados pessoais através de sistemas de videovigilância, disponíveis em [https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video\\_en](https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en).

<sup>5</sup> Cfr. pág. 9 da AIPD.

dever questionar a adequação e legalidade no contexto atualmente existente, algo que aparece igualmente omissa ou deficitariamente tratado na avaliação de impacto.

36. Voltando ao sistema de reconhecimento facial, e tal como já se referiu no ponto 31 c., a utilização de sistemas de reconhecimento facial coloca desafios particularmente exigentes que não podem ser descartados sem que se proceda a uma cuidadosa avaliação.

37. E isto é tanto mais importante quanto mais sensíveis forem os tratamentos, colocando-se o devido enfoque nas consequências que deles podem advir para os titulares dos dados.

38. Ao assentar toda a sua ação de identificação dos interditos num sistema cujo grau de fiabilidade parece ser desconhecido<sup>6</sup>, de resto, sem garantias de que exista uma confirmação humana dos resultados gerados automaticamente, corre-se o risco de não só incorrer na existência de múltiplos e injustificados resultados negativos, como também incorrer na violação do n.º 1 do artigo 22.º do RGPD.

39. Sem prejuízo desses desafios legais, sobra ainda a questão do respeito pleno pelo artigo 10.º do RGPD que apenas admite *O tratamento de dados pessoais relacionados com condenações penais e infrações ou com medidas de segurança conexas com base no artigo 6.º, n.º 1, (...) sob o controlo de uma autoridade pública ou se o tratamento for autorizado por disposições do direito da União ou de um Estado-Membro que prevejam garantias adequadas para os direitos e liberdades dos titulares dos dados. Os registos completos das condenações penais só são conservados sob o controlo das autoridades públicas.*

40. E se é verdade que a lei expressamente determina a remessa da informação sobre as pessoas sujeitas a medida de interdição, ela não estabelece as “garantias adequadas para os direitos e liberdades dos titulares dos dados” no que concerne à utilização de sistemas como o que aqui está em causa.

41. Reconhecendo-se a dificuldade de garantir a interdição decretada, sobretudo num contexto em que se estabelecem penalidades para os responsáveis pelo tratamento quando tal não suceda<sup>7</sup>, parece que deverá caber ao legislador estabelecer as condições em que estes

---

<sup>6</sup> Sendo cada vez mais públicas e notórias as deficiências e incapacidades desta tecnologia, como atestam recentes notícias: <https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html>; <https://www.tsf.pt/mundo/sorria-esta-a-ser-identificado-bruxelas-debate-reconhecimento-facial-na-ue-11837808.html> ; <https://www.bbc.com/news/technology-52978191>;

<sup>7</sup> Cfr. n.º 1 do artigo 42.º da Lei n.º 39/2009.

tratamentos poderão ser auxiliados por sistemas e tecnologias deste tipo, nomeadamente prevendo a intervenção das autoridades policiais na validação dos resultados devolvidos pelo sistema e a duração pela qual a recolha de imagens deve perdurar.

42. Quanto ao papel das Forças de Segurança no quadro dos tratamentos de dados pessoais 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, este vem regulado na Lei n.º 59/2019, de 8 de agosto, a qual transpõe a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. E aí se estatui expressamente que a licitude dos tratamentos levados a cabo neste contexto depende de previsão legal *e apenas na medida em que for necessário para o exercício de uma atribuição da autoridade competente* (cfr. n.º 1 do artigo 5.º). Como se determina, no n.º 2 do artigo 5.º, que *A lei [que vier a regular esses tratamentos] indica, pelo menos, os objetivos do tratamento, os dados pessoais a tratar e as finalidades do tratamento*.

43. No artigo 11.º da lei referida, acentua-se a imprescindibilidade da intervenção do legislador sempre que estejam em causa decisões individuais automatizadas, como aqui sucede.

44. Acresce que a utilização de categorias especiais de dados (como os dados biométricos) não podem sustentar tais decisões, atento o disposto no n.º 2 do citado artigo 11.º, o que supõe a invariável intervenção humana na verificação e validação dos resultados por parte das autoridades competentes (cfr. alínea i) do n.º 1 do artigo 3.º da Lei n.º 59/2019).

45. Outro aspeto que revela a insuficiência da AIPD submetida é a inexistência da especificação da informação que será guardada e do prazo de conservação dos *logs* do sistema, aspeto crítico na avaliação da proporcionalidade e adequação do tratamento, mas também do princípio da minimização.

46. Admite-se finalmente que o meio possa até ser adequado à finalidade, mas sem que haja uma intermediação concretizadora dos elementos essenciais do tratamento por parte do legislador, não se antevê como possa legitimar-se o seu uso em face das várias questões e interrogações sublinhadas.

## IX. Quanto ao parecer do EPD

47. A Encarregada de Proteção de Dados considera o tratamento justificado, admitindo que o mesmo constitui uma obrigação legal, que decorre da avaliação realizada, que as medidas de segurança e corretivas previstas são adequadas à proteção dos dados pessoais e que não se vislumbram medidas exequíveis e menos gravosas para os titulares que possam atingir as mesmas finalidades. Não obstante teme “*ainda assim, a proporcionalidade deste tratamento, dada a abrangência dos titulares afetados e a ausência de legislação específica na área, jurisprudência ou doutrina*”, pelo que sugeriu a consulta prévia da CNPD.

48. Atenta a posição assumida pela CNPD no ponto VIII, não se subscreve esta interpretação, segundo a qual o tratamento de dados por reconhecimento facial se enquadra numa obrigação legal, ainda que se reconheça ser uma obrigação legal do VSC garantir que as pessoas sujeitas a medida de interdição não acedam ao recinto desportivo.

49. Acompanhamos, ainda assim, a preocupação expressa quanto à proporcionalidade do meio e à ausência de regulação específica para este tratamento.

## X. Questões a esclarecer:

50. Independentemente da justeza ou licitude da utilização do sistema de reconhecimento facial para lograr a finalidade visada - impedir qualquer pessoa sujeita a medida de interdição de acesso a recintos desportivos de a eles aceder – existem vários pontos carentes de concretização:

- qual a fonte das fotografias a partir das quais serão extraídos os templates biométricos que constarão na base de dados biométricos e quais as características do sistema que fará tal extração?
- de que forma é realizada a reconstituição da localização nos 5 segundos anteriores ao momento atual sem que tal capacidade por parte do sistema implique o rastreamento de todas as pessoas presentes no recinto desportivo a todo o tempo?
- em que circunstâncias a componente de inteligência artificial das duas câmaras que a possuem irá ser utilizada?



- qual a interação com o atual sistema de videovigilância, que, apesar de referido, não se encontra incluído no documento?
- de que forma se realizará um acesso remoto a um servidor sem qualquer ligação à rede e, no caso de efetivamente se realizar, quais as medidas previstas nessa situação (como por exemplo VPN)?
- porque considera o VSC não ser possível o controlo da identidade de cada espectador aquando da sua entrada no estádio?
- qual a probabilidade de ocorrência de erros, corporizada nas taxas de falsos positivos/negativos do sistema?
- como reage o sistema quando não consegue focar a cara de um titular dos dados e, por conseguinte, não consegue extrair o *template* biométrico?
- de que forma o sistema atuará se, por exemplo, o número de correspondências for superior a 1 no intervalo de tempo necessário à validação humana?
- de que forma está prevista a utilização de cifragem na apresentação de imagens ao utilizador?
- se relevante para o tratamento em apreço, importa juntar a descrição do sistema de gestão interno, o qual é referido sem qualquer consideração adicional;
- qual a informação que é guardada em *log* e qual o prazo de conservação do mesmo?
- se a introdução conjunta de passwords *do responsável pelo departamento de IT e do responsável pelo departamento de gestão de infraestruturas e equipamentos desportivos* para acesso às imagens e à base de dados biométricos é complementar à autenticação por parte de quem efetivamente realizará o acesso, sendo essencial que assim seja para permitir o correto registo eletrónico do acesso?

## XI. Conclusões

Com base nos fundamentos acima expostos, a CNPD considera que, de momento, e porque estão em causa tratamentos de dados enquadráveis no conceito explanado no artigo 10.º do RGPD, a aplicação da tecnologia de reconhecimento facial aos sistemas de videovigilância instalados nos recintos desportivos, como o estádio D. Afonso Henriques, carece de intermediação prévia por parte do legislador nacional.

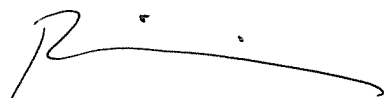
Tal conclusão é reforçada pelo facto de parecer inevitável a intervenção das Forças de Segurança no controlo e validação do funcionamento desta tecnologia, atento o âmbito de

aplicação da lei n.º 59/2019, de 8 de agosto e a expressa previsão que nela se encontra de proibição de decisões individuais automatizadas tomadas com base em dados biométricos (categoria especial de dados). Sem prejuízo da sua potencial utilidade e adequação à finalidade visada, as categorias de dados pessoais envolvidas (dados biométricos e dados sobre condenações penais ou infrações) e as potenciais restrições dos direitos fundamentais dos titulares dos dados, resultantes do uso desta tecnologia, obrigam ao delinear de um plano de implementação universal e que preveja garantias adequadas para os direitos e liberdades dos titulares dos dados. E tal só pode ser uniformemente concretizado através de lei ou decreto-lei autorizado, onde se definam os critérios e exigências mínimos a aplicar em qualquer sistema semelhante.

Ainda que se admitisse a licitude do meio, o que, por ora, não se reconhece, subsistem insuficiências de relevo na AIPD submetida em conjunto com o pedido de consulta prévia, as quais devem ser alvo de ponderação numa futura reapreciação por parte do responsável pelo tratamento.

Quanto à utilização do sistema de *Unusual Motion Detection*, não tendo ele sido devidamente contemplado na AIPD, e em face das suas potencialidades específicas, deverá ser sujeito a uma avaliação semelhante à que aqui foi efetuada para a tecnologia de reconhecimento facial.

Aprovada na reunião de 8 de julho de 2020



Filipa Calvão (Presidente)