r

national mission

DATA PROTECTION

RESOLUTION/2020/292

1. Introduction

1.0 VITÓRIA SPORT CLUBE - FOOTBALL SAD (NIPC 510646638) and VITÓRIA SPORT CLUBE (NIPC 501144013), both headquartered at Praça 26 de Maio, 4810-914 Guimarães, business group (VSC) submitted the prior consultation of the National Commission for the Protection of Data (CNPD) an impact assessment on data protection in relation to the use of facial recognition technologies associated with a closed circuit video surveillance installed at Estádio D. Afonso Henriques with the exclusive purpose of identifying and preventing the entry of individuals over the which there is a judicial or administrative ban on entering the sports venue.

2. The system is intended, according to the applicants, to operate exclusively in professional or non-professional sports events considered to be of high risk, national or international, following the qualification provided for in article 12 of Law No. 39 /2009, of 30 July, security and combat against racism, xenophobia and intolerance in sports, successively amended, lastly by Law No. 113/2019, of 11 September (hereinafter Law No.).

3. Despite the stated purpose mentioned in point 1, the use of Unusuai Motion Detection technology is also described, with which, as stated by the applicants, it is not intended to analyze personal data or draw profiles, but, just alert the security of the enclosure to movements considered abnormal, according to four vectors: speed, presence, absence and location.

4. The CNPD notes that, except in specific cases1, it is not responsible for approving treatments, but only, in light of the provisions of the combined provisions of paragraphs 1 and 2 of article 36. 1 of article 57 of Regulation (EU) 2016/679 - General Regulation on Data Protection (RGPD), provide guidance on processing operations, and may also exercise all the powers provided for in article 58 of that regulation .

These being those provided for in paragraph 5 of article 36 of the GDPR.

5. The data protection impact assessment (AIPD), provided for in Article 35 of the GDPR, is silent on several critical aspects of the system.

6. It is certain and acknowledged by the applicant that there is no legal framework that clearly authorizes the use of these systems for the stated purpose(s).

II. Description of the facial recognition system

7. As described by the applicant, the system will consist of:

• Two Avigilon H5A Camera Line cameras, equipped with CNN, that is, intelligent video analysis technology (Artificial Intelligence), one with 6 megapixels and the other with 4 megapixels, each having at least 10 defined rules,

® ana/ytics appiiance middleware for application of analytics on the 9 mobile IP cameras model SD49225T and the fixed camera of the current video surveillance system;

• video recording and management server where the images will be stored, this server not having any connection to the network and being remotely accessible by A vigiion only upon request and authorization from the I/SC, in case of need for technical assistance,

• switch for powering PoE or PoE+ cameras, according to IEEE 802.3af or IEEE 802.3at, link layer (Layer 2}-.

8. At this point in the technical description of the system, some assertions by the applicants regarding contradictory capabilities or, at least, dubious feasibility, are strange. As an example of this, mention the guarantee that the server does not have any connection to the network, so that, immediately afterwards, the possibility of being remotely accessible is affirmed.

9. Returning to the statement by the applicant, The software includes a facial recognition license package; A base software license; A package of analytics services (analysis of violations of the rules created after a period of study and learning of "normality"), these being the following: i.

i. Objects in Area - The event is fired when the selected object type moves to the region of interest;

ii. Long-stay objects - The event is triggered when the selected object type remains within the region of interest for an extended period of time;

iii. Objects crossing beam - The event is triggered when a specified number of objects cross the targeted beam, which has been set in the camera's field of view. The beam may be unidirectional or bidirectional;

iv. Objects appear or enter the area - The event is triggered by all objects that enter the region of interest. This event can be used to count objects;

v. Objects not present in the area - The event is triggered when there are no objects present in the region of interest;

saw. Objects Enter Area - The event is fired when a specified number of objects enter the region of interest;

vt Objects leave the area - The event is fired when the specified number of

objects leave the region of interest;

viii. Objects stationary in area -O and wind is triggered when an object, which is detected in a region of interest, stops moving, for a specified time limit;

ix. Violated Direction - The event is triggered when an object moves in a prohibited direction of movement;

x. Tamper Detection - The event is triggered when the scene changes unexpectedly.

This software description appears to apply only to the Unusuai Motion Detection system.

The applicant declares that this technology, in short, is capable of capturing, processing and analyzing metadata for image identification and biometrics, through software that allows the qualification of the captured object, according to its appearance, allowing, in abstract , perform advanced search for physical appearances of people.

It also declares that the images may only be viewed on a computer installed in the video surveillance exit, by entering a password of a person authorized to view the images.

III. Personal data processed

10. In order to achieve the main purpose (signaling data subjects subject to interdiction decision and compliance with that decision), a set of data that results from the combination of previously transmitted information is used.

to promoters of the sports show (like the applicant) with the images captured by the video surveillance system provided for in paragraph 1 of article 18, which, in addition to the sports venue, includes the respective ring or security perimeter.

11. The holders of the data that make up the universe of people to whom a judicial or administrative prohibition of entry to the

sports venue applies cannot ignore the legal obligation to send such personal data to the promoters of sports shows2, which depends on who must determine this prohibition.

12. In this sense, the decision on the ban is made available to the promoters of sporting events, under the terms of Article 38(1) (also ex vin. 2 of Article 42).

13. Law no. 39/2009 does not provide for the categories of personal data that must be transmitted to promoters, although it is accepted that the concept of “decisions” encompasses, at least, the name, an identification element (Cartão do Citizen or other equivalent document) and the content of the decision.

14. It is not clear how the photograph of the person subject to the judicial or administrative ban from entering the sports venue is obtained, as this is not described by the applicant, but it is anticipated that this information will also be made available by the entity that decreed the ban.

15. The video surveillance system referred to in point 10 obviously collects images of all those who enter or only circulate in the respective ring or security perimeter.

16. The applicant declares the processing of data: name, civil identification number, images of the general public, photographs of individuals subject to the interdiction decision and the respective sentences or decisions that apply them.

17. In the field of biometric data and with regard to the general public, the collection of "biometric data" is described, indicating the existence of facial recognition captured on the day of a sporting event - analysis of biometric characteristics

2 As described in Article 3(k) of Law No. 39/2009.

/ NATIONAL COMMISSION

' DATA PROTECTION

i.Face detection; ii Creation of numerical temp/ate based on the features of the captured face.

18. As for the data subjects subject to the interdiction measure, it is stated that “biometric metadata” (numeric tem/ate) obtained from the photographs in the applicant's possession are collected.

19. Finally, the specified retention periods are as follows:

The. The name and civil identification number will be kept for the duration of the restriction measure;

B. The images captured by the video surveillance system will respect the period of 60 days provided for in article 18 of Law no.

39/2009;

ç. Biometric data:

i. “metadata” related to the general public - Time required to carry out the study (Comparison of this temp/ate with those kept in the database). Automatic elimination in case of non-coincidence / during the execution of the study,

ii. “metadata” related to the bans - while the restriction order lasts, being systematically compared with the biometric metadata captured on the day of a sporting event.

20. About the photographs nothing is said about the conservation period.

IV. Internal data flows

21. From the information provided in the document, it is concluded that there are the following internal data processing flows:

• Facial recognition

The. The video surveillance system captures and records the images;

B. approximately 5 seconds later, the facial recognition software captures the biometric data of the recorded images, analyzes the appearance of the captured objects, pre-qualifies the objects into categories (people, cars, bottles, etc), when identifying the category person tries to focus on the face and create the numerical template based on the physical characteristics (relative position of its components, size and distinguishing characteristics); the numeric template is compared with the temp/ates contained in the database;

ç. if there is a coincidence, an alarm is raised and the intervention of the competent authority is requested to confirm the reliability of the alarm, as a way of avoiding false positives;

d. the authority accesses the system, which will then allow him to reconstruct the path of the individual in question, captured on camera, and discover his location in the 5 seconds prior to the current moment;

• Unusual motion detection

The. after a first phase of studying and learning what is considered "normality" regarding events inside a football stadium, the software will be able to detect "non-standard" mass movements, by changing the parameters normally measured for the absence , presence, speed and location of objects or crowds at specific locations in the stadium.

B. approximately 5 seconds after the video surveillance system records the images, the system performs the analysis to detect "non-standard" mass movements, by changing the parameters normally measured for the absence, presence, speed and location of objects or crowds in places stadium specific.

V. Entities Involved

22. In addition to the VSC, there are 3 subcontracting entities that provide services related to CCTV and the technology that will be used for the treatment in question, each with a specific function, with a perfectly defined purpose and with which VSC carried out a DPA - Data Processing Agreement, which will constitute a contract within the meaning of article 28 of the RGPD.

23. It is stated that the Security Forces and Services (FSS) will have access to the results of the application of this technology, that is, they will have access to the identifications of individuals who unduly remain in the stadium and their location.

24. It is also proposed that the FSS elements take responsibility for determining the validity of the recognition, eliminating false positives, thus acting as third parties, with their own purposes. But this will depend on the FSS's own assessment, as the person responsible for the treatment. In addition to the weakening of the process of verifying the identity of persons subject to the interdiction measure, it is not clear what the specific purposes in question are. In the present context, attributing to the FSS the quality of controller also appears to be problematic, since it would only be up to them, if they accepted the VSC proposal, to validate positive results returned by the system and then act in the sphere of their competences.

25. With regard to the “rules applicable to treatment” it is foreseen:

o The obligation of subcontractors to offer security guarantees at least equal to those of the VSC;

• The liability of the company and personnel of the subcontractors' technicians in the event that confidentiality is not respected, the data is copied to unapproved devices, is sent by unencrypted email or is used for purposes other than those provided for in the impact assessment;

• VSC will only access the data when it is legally obliged to do so or when it is pursuing or defending legally protected interests or rights, within the scope of criminal proceedings,

• Access to the video surveillance room by a large group of people and entities:

o From the VSC: the person responsible for the IT department, the person responsible for the infrastructure and sports

equipment management department (or to whom he delegates competence in writing), the safety director and the field director;

o The subcontractor that provides services related to the maintenance of the video surveillance system and data stored by it; o The subcontractor that provides private security services, which include the management and monitoring of video surveillance in the role of assistant to the sports venue, pursuant to article 3 of Law No. 113/2019; o FSS and administrative or judicial authorities;

o The fire detection system maintenance company through the person responsible for the infrastructure and sports equipment management department (or to whom he delegates competence in writing);

o The EPD, whenever requested by the person responsible for the IT department or the person responsible for the infrastructure and sports equipment management department;

« The only point where the video surveillance images can be viewed is a computer installed in the video surveillance room, by entering a password.\ It is not explicitly indicated whether there are nominal users for whom the access is made.

SAW. Measures implemented

26. The applicant has indicated that it will implement the following security measures

• Encryption - it is mentioned that the system allows 256-bit encryption in video capture, transport and presentation to the user - it is not clear how encryption can be used in the presentation of images to the user;

• Physical access control / organization

o access to the CCTV room is controlled and made using RFID technology cards assigned to the large number of entities already listed in “rules applicable to treatment”. The VSC also informs that a record is kept only referring to the last 50 accesses, proposing an improvement to the system that allows keeping the record of all accesses to the room for a minimum period of 60 days and the signature of a disclaimer that explicitly establishes that the card is personal and non-transferable - Although the measure of

extending the period of storage of access records is positive, as well as the clarification of the non-sharing of the card, the foreseen access cannot be considered safe, since it is based on only one factor, the card, which can be object, even without charge by part of its holder, for example, from loss or theft. It is therefore necessary to provide for additional factors that are only known to the holder, such as password; o at this point, an internal management system is never mentioned before in the document, nor in context. Deserving agreement the provision of segmenting accesses according to specific functions, regardless of the system in question, it is not possible to make any additional assessment of an unknown system;

• Policy - confidentiality agreement, procedural and security rules;

• Logs - VSC states that user profiles will be defined according to the type of operator and the functions/information they can access; not indicating how many and what types of functions, and consequently of profiles, are foreseen. Neither the information that will be stored nor the period of conservation of the logs is specified;

• Logical access3

o A paper record of accesses to recorded images and to the biometric database will be carried out with the date, time, authorship, reasoning and, whenever possible, the EPD's opinion on the need for access. If it is not possible to obtain the opinion in advance, the EPD will know later.] o The VSC declares that “no smart devices (smartphone, tabiet, etc.) video camera or photographic camera should be introduced into this skirt.' -suggests- whether a wording change to make the intent a ban; o “Accessing and downloading images, as well as updating and accessing the biometric database will only be possible through the joint introduction of the passwords of the person responsible for the IT department and the person responsible for the management department of infrastructure and sports equipment." - not applicable clear whether this joint introduction of passwords is complementary to the

J The applicant misidentifies or groups these as measures relating to physical access.

authentication by the person who will actually carry out the access, which is essential to allow the correct electronic registration of the access.

VII. Regarding the risks considered and their assessment

27. The applicant considered three potential risks: Illegitimate access to data, Unwanted modification of data and

Disappearance of data - identifying, for each of them, the impacts for data subjects, the threats that could lead to them, the sources of risk , the established measures that can contribute to mitigating the risk, and classifying them in terms of probability and severity. Summarizes such classification in the following image:

risk severity

O

risk probability

Figure 1 - Classification, in terms of severity and probability, of the 3 identified risks - Illegitimate access to data (I), Unwanted modification of data (IN) and Disappearance of data (D)

28. According to the standardized classification (insignificant, limited, significant and maximum risk), a maximum level of severity and significant probability was assigned to the potential illegitimate access to the data, while the risk of unwanted modification of the data presented a significant level of severity and bounded probability. Finally, the risk of data disappearance deserved a limited level in these two categories.

VIII. appreciation

29. The processing of personal data envisaged by the applicant represents a very considerable enhancement of the capabilities of the video surveillance system currently installed.

30. Although the prior consultation is not intended to authorize the treatments carried out by those responsible for the treatment, the CNPD understands that the pronunciation that it is responsible for cannot refer only to the aspects valued as high risk by those responsible for the treatment.

31. Even so, let us begin by pointing out which aspects, from the applicant's point of view, constitute a high risk in the treatments subject to evaluation:

The. As for the fundamental principles of data protection, it was considered that there was a high risk in terms of safeguarding the principle of data minimization. No explanation is given about this result, but it appears that the conclusion stems from the fact that all data subjects present in the premises and within the security perimeter of the same may be targeted by the

processing, even though no interdiction decision has been taken. against them. In fact, all the arguments put forward by the applicant seem to indicate that there is no other solution that guarantees the intended purpose with the same effectiveness, taking into account the difficulty of individual identification at the entrance to the sports venues and the unbalanced or feasible solutions of the law, regarding the mandatory , on the part of those interdicted, to appear at the police station at times coinciding with the sporting events;

B. In the risk assessment, and specifically with regard to the potential occurrence of “illegitimate access [to] the data” (cf. page 37 et seq.), a maximum level is assigned to the “severity of the risk, especially according to potential impacts and planned controls”, with the probability of this occurring being “significant” and resulting in the overall assessment being “High risk”. What is at issue here is the intrusion into the place where the images are viewed and preserved, which could result from a “negligent or willful” human intervention, which may lead to “intrusion into the private life of a holder not targeted by technology”. that any system with the characteristics of the subject to impact assessment can cause an intrusion into the privacy of any of the data subjects captured by it, but this can and should be

mitigated through appropriate technical and organizational measures. In this regard, the CNPD recognizes the correct intention to extend the period of storage of access records, as well as the clarification of not sharing the card of duly authorized personnel. However, as access control is limited to one factor, in this case, the card assigned to those who must access and/or frequent the aforementioned places, these measures prove to be insufficient, as only one factor is at stake - the card - that can be misplaced or lost. It is therefore necessary to provide for additional factors such as password;

As for the unwanted modification of the data, whose risk assessment allowed to signal the hypothesis of wrong identification of data subjects and invasion of their privacy, due to the “false-positive” results that the system can return, it is important to record two notes. The first concerns the classification of these risks. There may be a potential threat to the integrity of the data through its intentional or negligent modification, the matter of false positives goes far beyond this domain, linking, among other aspects, to the very robustness and reliability of the technology used.

Then, the existence of these erroneous or anomalous results cannot fail to be considered as high risk when it concerns a situation such as the one presented here. As it is probable or at least possible that people are wrongly identified as being

prohibited from accessing sports venues, this is doubly penalizing. On the one hand, this false positive can result in the impediment of entry to a given space by those who have all the legitimacy to attend. Then, even if the actions of the authorities or security guards of the premises are discreet, they will hardly avoid publicizing this condition, which affects the reputation of the data subject, producing an intolerable stigmatizing effect. Furthermore, it is the controller himself who does not guarantee that the results obtained by the biometric analysis will be verified, since the police authorities are entirely free to accept or decline the supervisory role that the controller intends to assign them.

d. There is, however, a more critical aspect related to the already underlined aspect of the system's reliability that the CNPD cannot assess. It is that the person responsible for the treatment never demonstrates having evaluated the probability of these false-positives, one of the fundamental elements in the assessment of the adequacy of the medium for the purpose4. How can the use of this identity confirmation system be accepted without knowing in detail its degree of reliability, especially when data categories “related to criminal convictions and infractions” are involved (cfr. article 10 .° of the GDPR)? And this is an aspect to which we will return.

32. The CNPD notes that the impact assessment excluded any consideration of the use of Unusuai Motion Detection technology. This will be linked to the erroneous interpretation that the controller has made of what constitutes or does not constitute personal data. By stating that This technology does not intend to analyze personal data or draw profiles, but only alert the security of the premises to movements considered abnormal, the intention is confused with the purpose.

33. It should be noted that it is the person responsible for the treatment who admits that this technology will make it possible to carry out an advanced search for physical appearances of persons, being even described as the starting point to identify, through video surveillance, spectators who commit a crime or administrative offence5 of automated way.

34. In fact, it is not just personal data that directly allows the identification of a person, but also any information that contributes to that identification, given the comprehensive concept of Article 4(1) of the GDPR. and known is the position of the Court of Justice of the European Union on this matter (in particular the Judgment of 19 October, C-582/14, points 41-45, ECLI:EU:C_2016:779).

35. Thus, at the present time, the conditions for the operationalization of this technology do not seem to be met due to the lack of this formal requirement, without prejudice to the

4 On the use of this technology, the European Data Protection Board produced some useful notes in point 5 of the guidelines on the processing of personal data through video surveillance systems, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en.

5 Cf. page 9 of the IAPD.

must question the adequacy and legality in the currently existing context, something that appears equally omitted or poorly addressed in the impact assessment.

36. Returning to the facial recognition system, and as mentioned in point 31 c., the use of facial recognition systems poses particularly demanding challenges that cannot be ruled out without careful assessment.

37. And this is all the more important the more sensitive the treatments are, with due focus being placed on the consequences that may arise from them for data subjects.

38. By basing all of your action to identify those prohibited on a system whose degree of reliability seems to be unknown6, moreover, without guarantees that there is human confirmation of the results generated automatically, you run the risk of not only incurring the existence of multiple and unjustified negative results, as well as infringing Article 22(1) of the GDPR.

39. Without prejudice to these legal challenges, there is still the issue of full compliance with Article 10 of the GDPR, which only allows the processing of personal data related to criminal convictions and offenses or related security measures based on Article 6 no. .0 1, (...) under the control of a public authority or if the processing is authorized by provisions of Union or Member State law that provide adequate guarantees for the rights and freedoms of data subjects. Complete records of criminal convictions are only kept under the control of public authorities.

40. And while it is true that the law expressly determines the transmission of information on persons subject to the interdiction measure, it does not establish “adequate guarantees for the rights and freedoms of data subjects” with regard to the use of systems such as which is at issue here.

41. Recognizing the difficulty of guaranteeing the interdiction decreed, especially in a context in which penalties are

established for those responsible for the treatment when this does not happen7, it seems that it should be up to the legislator to establish the conditions under which these

6 As the deficiencies and incapacities of this technology are increasingly public and notorious, as recent news: https://vvvvvv.nvtimes.com/2019/l2/l9/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:

7 Cf. no. 1 of article 42 of Law no. 39/2009.

’7~~ r- /

M: mm W

S NATIONAL COMMISSION ON DATA PROTECTION

treatments may be supported by systems and technologies of this type, namely by providing for the intervention of the police authorities in the validation of the results returned by the system and the duration for which the collection of images must last.

42. As for the role of the Security Forces in the context of processing personal data for the purposes of prevention, detection, investigation or prosecution of criminal offenses or the execution of criminal sanctions, including safeguarding and preventing threats to public security, this comes regulated in Law No. 59/2019, of 8 August, which transposed Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016. And it expressly states that the lawfulness of the processing carried out in this context depends on a legal provision and only to the extent necessary for the exercise of an attribution of the competent authority (cf. Article 5(1)). As is determined, in paragraph 2 of article 5, that A iei [who will regulate such treatments] indicates, at least, the purposes of the treatment, the personal data to be processed and the purposes of the treatment.

43. Article 11 of the aforementioned law emphasizes the indispensability of the legislator's intervention whenever automated individual decisions are at stake, as is the case here.

44. Furthermore, the use of special categories of data (such as biometric data) cannot support such decisions, given the provisions of paragraph 2 of the aforementioned article 11, which presupposes the invariable human intervention in the verification and validation of the results by the competent authorities (cf. subparagraph i) of paragraph 1 of article 3 of Law n.° 59/2019).

45. Another aspect that reveals the insufficiency of the AI PD submitted is the lack of specification of the information that will be stored and the period of conservation of the yogsúo system, a critical aspect in the assessment of the proportionality and adequacy of the treatment, but also of the principle of minimization.

46. Finally, it is accepted that the means may even be suitable for the purpose, but without an intermediation that materializes the essential elements of the treatment on the part of the legislator, it is not possible to foresee how its use can be legitimized in the face of the various issues and underlined questions.

THE

IX. Regarding the opinion of the EPD

47. The Data Protection Officer considers the treatment to be justified, admitting that it constitutes a legal obligation, which arises from the assessment carried out, that the security and corrective measures provided for are adequate for the protection of personal data and that no feasible measures are envisaged. and less burdensome for holders who can achieve the same purposes. Nevertheless, he fears “even so, the proportionality of this treatment, given the scope of the affected holders and the absence of specific legislation in the area, jurisprudence or doctrine”, for which he suggested the prior consultation of the CNPD.

48. Bearing in mind the position taken by the CNPD in point VIII, this interpretation, according to which the processing of data by facial recognition is part of a legal obligation, is not subscribed, even though it is recognized that the VSC has a legal obligation to ensure that persons subject to interdiction measure do not access the sports grounds.

49. Even so, we follow the expressed concern about the proportionality of the medium and the absence of specific regulation for this treatment.

X. Questions to clarify:

50. Regardless of the fairness or legality of using the facial recognition system to achieve the intended purpose - to prevent anyone subject to a measure banning access to sports venues from accessing them - there are several points that need to be implemented:

• what is the source of the photographs from which the biometric templates that will be included in the biometric database will

be extracted and what are the characteristics of the system that will perform such extraction?

• How is the location reconstitution carried out in the 5 seconds prior to the current moment without this capacity on the part of the system implying the tracking of all people present in the sports venue at all times?

• under what circumstances will the artificial intelligence component of the two cameras that have it be used?

Process PRE/2020/3 9

and

ê-mWF9^êk

S; mmm

m. mMr M;

..g NATIONAL COMMISSION

DATA PROTECTION

• what is the interaction with the current video surveillance system, which, despite being mentioned, is not included in the document?

o How will remote access to a server be carried out without any connection to the network and, if it is actually carried out, what measures are foreseen in this situation (such as VPN)?

• why does the VSC consider that it is not possible to control the identity of each spectator upon entering the stadium?

® What is the probability of errors occurring, embodied in the system's false positive/negative rates?

• how does the system react when it cannot focus on a data subject's face and therefore cannot extract the biometric time stamp?

® How will the system act if, for example, the number of matches exceeds 1 in the time interval necessary for human validation?

• How is the use of encryption foreseen in the presentation of images to the user?

• if relevant for the treatment in question, it is important to add the description of the internal management system, which is mentioned without any additional consideration;

« What information is stored in the log and what is the retention period?

® if the joint introduction of passwords by the person responsible for the IT department and the person responsible for the

infrastructure and sports equipment management department for accessing images and the biometric database is complementary to authentication by those who will actually carry out the access, being essential that it be so to allow the correct electronic registration of access?

XI. conclusions

Based on the reasons set out above, the CNPD considers that, for the time being, and because the processing of data falling under the concept explained in Article 10 of the GDPR, the application of facial recognition technology to video surveillance systems installed in sports venues , like the D. Afonso Henriques stadium, requires prior intermediation by the national legislator.

This conclusion is reinforced by the fact that the intervention of the Security Forces in the control and validation of the operation of this technology seems inevitable, given the scope of

application of law No. 59/2019, of August 8, and the express provision contained therein of the prohibition of automated individual decisions made on the basis of biometric data (special category of data). intended purpose, the categories of personal data involved (biometric data and data on criminal convictions or offences) and the potential restrictions on the fundamental rights of data subjects, resulting from the use of this technology, require the design of a universal implementation plan that provides for adequate guarantees for the rights and freedoms of data subjects. And this can only be uniformly implemented through an authorized law or decree-law, which defines the criteria and minimum requirements to be applied in any similar system.

Even if the legality of the environment were admitted, which, for the moment, is not recognised, there are still significant insufficiencies in the AI PD submitted together with the request for prior consultation, which should be considered in a future re-examination by the person in charge. by the treatment.

As for the use of the UnusualMotion Detection system, since it has not been duly contemplated in the AI PD, and given its specific potential, it should be subject to an assessment similar to that carried out here for facial recognition technology.

Approved at the meeting of July 8, 2020