CNP©

National Data Protection Commission

OPINION/2021/125

I. Order

1. By order of the Assistant Secretary of State and Internal Administration, an opinion was requested from the National Data Protection Commission (CNPD) on the request for authorization to use a video surveillance system in the Oura and Baixa areas of the city of Albufeira, submitted by the Republican National Guard (GNR).

2. The CNPD considers the request under the terms of paragraph 2 of article 3 of Law no. 1/2005, of 10 January, amended and republished by Law no. 9/2012, of 23 February (hereinafter, Law No. 1/2005), which regulates the use of video cameras by security forces and services in public places of common use, for capturing and recording images and sound and their subsequent processing.

3. The request is accompanied by a document containing the reasons for the request and the technical information of the system, hereinafter referred to as “Rationale”, as well as the impact assessment on data protection (AIPD).

II. appreciation

i. Object of the opinion to be issued under the terms of article 3 of Law No. 1/2005, of 10 January

4. Pursuant to paragraph 2 of article 3 of Law no. 1/2005, the CNPD's opinion is limited to pronouncing on the compliance of the request with the rules regarding the security of the treatment of the collected data, as well as as well as about the special security measures to be implemented, adequate to guarantee entry controls on the premises, data carriers, insertion, use, access, transmission, introduction and transport, as well as verification of compliance with the duty of information and before whom the rights of access and rectification can be exercised.

5. Pursuant to the provisions of the same legal precept and paragraphs 4, 6 and 7 of article 7 of that law, the CNPD's opinion is also subject to respect for the prohibition of installing fixed cameras in areas that, despite being located in public places, are, by their nature, intended to be used in guarding or the use of video cameras when the capture of images and sounds covers the interior of an inhabited house or building or its dependence, or when this capture affects , directly and immediately, the

privacy of people, or results in the recording of conversations of a private nature.

6. The CNPD must also verify that all persons appearing in recordings obtained in accordance with this law are guaranteed the rights of access and elimination, with the exceptions provided for by law.

Av. D. Carlos 1,134.1° T (+351) 213 928 400 geral@cnpd.pt

1200-651 Lisbon F (+351) 213 976 832 www.cnpd.pt

7. Pursuant to paragraph 7 of article 3 of the same law, the CNPD may also formulate recommendations with a view to ensuring the purposes set out in the law, subjecting the issuance of a totally positive opinion to the verification of the completeness of the fulfillment of its recommendations.

ii. The purposes of the treatment resulting from Video Surveillance in public places of use in Oura and downtown Albufeira

8. Notwithstanding, under the terms of the legal powers defined in Law no. 1/2005, it is not up to the CNPD to pronounce on the proportionality of the use of video surveillance systems in public places of common use, this competence already exists when it comes to cameras are installed in areas that are, by their nature, intended to be used for guarding or capturing images or sound that directly and immediately affect people's privacy, or result in the recording of conversations of a private nature (cf. paragraphs 4 and 7 of article 7 of Law no. 1/2005).

9. However, the use of a video surveillance system in the Oura and Baixa areas of the city of Albufeira implies the processing of personal data capable of significantly affecting the private life of people who circulate or are there.

10. In fact, the issue is the installation and use of 64 (sixty-four) fixed cameras in areas where there are buildings intended for housing as well as occupation by tourists and which are known to have great tourist influx, especially during the bathing season. (cf. point 4.b. of the statement of reasons accompanying the request).

11. In this regard, it should be noted that, although the authorization request concerns 64 chambers, in the accompanying grounds, 65 (sixty-five) chambers are described (cf. annex A to the said grounds). As the CNPD is not aware of whether this discrepancy is due to an oversight or if there is a clearinghouse that is not intended to be covered in any authorization to issue, this entity confines itself to pointing out this fact, drawing attention to the circumstance that, in the absence of specification of the camera to be excluded, the lawfulness of the processing of personal data carried out on the basis of the images captured

by any of the cameras is at risk.

12. In addition, most cameras have PTZ features (Pari, Tilt and Zoom), which means the ability to capture images of people and vehicles in all directions and with great acuity. Among those that don't have PTZ, some seem to have at least Pan functionality.

13. The processing of data has, as stated, the purpose of protecting people and goods, public and private, and preventing the practice of facts qualified by law as crimes, in places where

there is a reasonable risk of its occurrence, as well as the purpose of preventing terrorist acts, pursuant to paragraphs c) and e) of paragraph 1 of article 2 of Law n.° 1/2005.

14. To this end, it is stated that the video surveillance system only captures and records images, but, although it is not intended to record sound, the installation and use of the operating mechanism of the system called “voice alert” (cf. point 4.c. of the Justification).

15. And it is further stated that “[e]if necessary, video analytics may be used, however rules integrated directly into the camera are defined (Annex B), in order to make any creation of profiles or discrimination of persons, as provided for in article 6 of Law no. We will turn to this point, but for the assessment of compliance with the conditions and limits imposed in article 7 of Law No. rules in Annex B, but merely functionalities or capabilities of the camera. For this reason, the use of video analytics using Artificial Intelligence technology, of soft recognition, without specifying the terms in which it will take place, allows or promotes the tracking of any citizen without guarantees of non-discrimination and without guarantees of proportionality in the compression of the fundamental right to reserve private life that is recognized by everyone, including in the context of circulation in public space (cf. article 26 of the Constitution of the Portuguese Republic - CRP).

16. Even without considering, for the time being, the application of this technology, the impact on citizens' privacy of the use of this video surveillance system is clearly high, not only taking into account the scope and extension of the areas on which the

cameras that capture and record images (see above point 10), but also because of the apparent potential for capturing sound, which a «voice alert» mechanism initially entails and whose terms and conditions of execution do not appear at any point in the request or the Rationale described - although in point 1.a) of Annex B and the AIPD it is stated, respectively, that "the cameras do not allow any type of sound to be captured" and "the system does not technically allow the capture and recording of sound"

17. In fact, despite the provision for the installation and use of the operating mechanism of the system called «voice alert», nowhere is it explained what this mechanism consists of and, therefore, it remains unclear whether the alert is triggered through the sound capture by the cameras or is operated via a loudspeaker that allows the GNR to issue alerts to anyone in the vicinity of the cameras. Even if what is at stake is the second hypothesis considered here, the system can allow that when the loudspeaker is activated, sound is also captured, in which case it is essential to ensure that the sound capture functionality is deactivated. It should be noted that, as there is no room for capturing and recording sound from the video surveillance cameras, the

requirement for the monitoring workstation to «have an internal speaker that is automatically deactivated when any external audio device is connected to the front line-out sound interface, transferring the sound reproduction to that device», patent in point 3. of Annex B, shows that it is intended to contemplate the listening of audio of some nature.

18. It is insisted that the capture of sound, in the vicinity of housing and hotel or local accommodation buildings, but also in public spaces, has a great impact on privacy, and should not occur unless it is demonstrated that it is essential for the purpose pursued with this data processing and the objective conditions under which it takes place are established.

19. In addition, although measures are foreseen to safeguard the privacy of people inside buildings and private spaces - «placement of masks in the cameras so as not to capture and record images in private places, such as the interior of dwellings or backyards' (cf. point 4.c. of the Grounds) - the fact is that the elements presented do not allow an assessment of compliance with the limits imposed in paragraph 6 of article 7 of Law no. /2005. In fact, in Annex A, the probable angles of view of the cameras are presented, and although the opening paragraph refers to "a configurable system to hide defined areas of the image, making them undisplayable, such as windows or building entrances, as inside. These masks will even be dynamically

adjusted based on the current zoom factor and the operator cannot display the protected contents», in the images that follow, the areas to be filtered or hidden are not marked, nor do they indicate a work to identify the exact cameras that affect these areas.

20. Thus, on the grounds set out above, the CNPD believes that there is not enough information in the request and in the documents presented to allow the CNPD, nor the competent body for authorizing the use of the system, to assess compliance with the limits imposed in paragraph 6 of article 7 of Law no. 1/2005.

21. As for sound recording, if it is confirmed that the cameras have such functionality, the CNPD recommends that, in order to be authorized, it is in the aforementioned authorization framed by precise guidelines, and cannot be dependent on the subjective criteria of the agent who is currently operate the system.

iii. Capability of the video surveillance system for tracking citizens

22. As mentioned above, in point 15, the request states that '[ej if necessary, video analytics may be used, however rules integrated directly into the camera are defined (Annex B), in order to make any creation of profiles or discrimination against persons, as provided for in article 6.0 of Law no.

23. It is clarified that, according to the characteristics of the cameras described in point 1.a) of the aforementioned Annex B, this means the ability of the video surveillance system to identify citizens based on physical characteristics and to track them, including for monitor their behaviors and habits. In fact, despite stating in point 5 of Annex B that "[the] system does not collect metadata for identification, so it does not identify people or vehicles, only appearances", the very purpose of the video surveillance system and the soft recognition technology it cannot be other than the identification of people and the recognition of objects. Eventually, with that statement, it is intended to invoke that facial recognition is not performed, as they reaffirm elsewhere, but this does not mean that the non-identifiable people captured in the images and their automated tracking.

24. However, the use of this technology, especially in an environment of systematic and large-scale control of areas accessible to the public, must be preceded by a careful consideration of its consequences, not only for people's privacy, but also for the

dimensions fundamental rights of freedom, personal identity and non-discrimination. It is therefore essential that the circumstances of its use be predefined - that is, the characterization of situations that may reveal the need for its use in view of the purposes of data processing - so that the proportionality of the restrictions to those fundamental rights can be assessed. , enshrined in articles 13 and 26 of the CRP, under the terms imposed by paragraph 2 of article 266 of the Fundamental Law.

25. And, for that purpose, it would also be essential that the IAPD carried out had specifically focused on this processing of personal data. However, the AIPD only mentions that “the system has the ability to add video analytics to protect people and goods, with defection rules” and it is concluded that “sufficient guarantees are safeguarded” for rights, freedoms and guarantees.

26. Simply, in point 1 .a) of Annex B, in addition to the express reference that the cameras do not allow facial recognition, only the potential or functionalities of the video surveillance cameras that they integrate are listed, at no point defining the criteria and the limits of its use. In fact, from the statement it follows that the system allows selecting and tracking a certain «object», which can be a person or a vehicle, making it explicit that «the event is triggered when the type of object selected moves to the region of interest » «stays within the region of interest for an extended period», «stops moving for a specified time limit», etc. of interest'.

27. In other words, the request and the accompanying reasoning are silent on the situations that justify the use of the image analysis algorithm, as well as on the criteria or factors that

Av. D. Carlos 1,134.1° 1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

<

may underlie the selection of persons or vehicles for tracking. And the definition of the assumptions for their use and of these selection criteria or factors must be made in advance in terms that prevent the risk of discrimination based on certain

characteristics or profiles, in compliance with the conditions and limits set in article 13 of the CRP and in paragraph 1 of article 9 of the GDPR, perhaps requiring that inadmissible factors or analysis criteria be defined ex ante.

28. These assumptions and factors, in the absence of a law listing and densifying them, must be defined in any authorization to be issued, otherwise it will not be possible to understand whether the results presented by the system, and on the basis of which the GNR will take decisions on the targeted citizens are discriminatory and therefore inadmissible under the Constitution.

29. In view of the omission of such elements in the request and in the reasoning, the CNPD recommends that any authorizing decision on the installation and use of this video surveillance system does not cover the use of this video analytics technology, expressly prohibiting the activation of the Artificial Intelligence that allow automated tracking of citizens or vehicles.

iv. subcontracting

30. Regarding the use and maintenance of the video surveillance system, because it is directly related to information security and the system's ability to fulfill the intended purposes, it is important to emphasize that this obligation falls on the data controller, regardless of whether who owns the video cameras and other equipment that make up the system.

31. Establishing Law No. 1/2005, in Article 2(2), that the data controller is the security force with jurisdiction in the catchment area or the requesting security service, any subcontracting in company to ensure the maintenance or replacement of equipment must be formalized, contractually, with the GNR. It is not excluded that the GNR subcontracts the Municipality of Albufeira, which may subcontract companies, under the terms regulated in article 23 of Law No. 59/2019, of 8 August. What cannot be a reversal of roles, leaving the GNR without the domain or control of the processing of personal data that the video surveillance system performs.

32. Since it is true that in point 5. of the Justification, it is stated that the GNR will be the only entity to have control over the chambers, it is therefore important that a contract or agreement be entered into specifically to regulate this subcontracting relationship, binding the Municipality under the terms of that legal rule - which in this case does not seem to occur, since the text of the protocol annexed to the Grounds is insufficient in this perspective.

33. Specifically with regard to subcontracting, it is recalled that under the terms of the same article 23, they depend on the prior authorization of the person in charge.

v. Video surveillance system security

34. There are aspects described in the Justification that give rise to reservations to the CNPD regarding the security of the video surveillance system, first of all with regard to the communications architecture.

35. First, consider the reference, in point 1.a) of Annex B, with regard to the characteristics of video surveillance cameras, that they 'contain an integrated web server for video capture and configuration available in an Internet browser standard, using HTTP with no need for additional software».

36. This functionality presents an access vulnerability in case of network compromise, as there may be capture of access credentials to the cameras, given that the HTTP protocol is not encrypted. The credential for accessing the camera's integrated server is also in question. If the default password that comes from the factory is not changed, the system is compromised from the beginning

37. Therefore, it is recommended that the server integrated in the cameras be reconfigured for HTTPS and that a password management policy be foreseen in the cameras, and a single password should not be used for all equipment.

38. Incidentally, the Justification refers to the encryption of all images, between the camera and the recording server, but, despite referring in point 1.a) of Annex B to HTTPS encryption, in the same point it is stated that the cameras are compatible with other protocols. The CNPD, in addition to stressing that that encryption protocol is only secure if implemented in version TLS1.2 or higher, recommends that all protocols that are not essential for the operation of the video surveillance system should be deactivated.

39. Greater apprehension raises the interconnection of this video surveillance system with the RNSI (National Internal Security Network).

40. In fact, as stated in the Justification, the images will be transmitted to two different locations, for monitoring purposes: the Territorial Detachment of Albufeira and the Situation Room of the Territorial Command of Faro.

41. In addition to not being clear how the two monitoring rooms are articulated (for example, assuming that the system has only one video matrix (video wall), it would be useful to clarify whether the changes in its visualization

Av. D. Carlos 1,134,10 1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

affect the two checkpoints and what articulation is planned between them), there are questions that arise regarding the connection between the communications network of the video surveillance system and the RNSI. Let's see.

42. On the one hand, in point 4.g. of the Rationale states that «[t]he transmission of images to the Situation Room of the Faro Territorial Command will be through the National Internal Security Network (RNSI) with all the security policies in the communications inherent to this network» and that the Entrance to rooms for viewing images is reserved for “military personnel accredited for this purpose, being registered and controlled by entering an entry code and access to the viewing system by assigning RNSI access profiles”. 0 which is confirmed in the AIPD (cf. annex D), where it is mentioned that "access to the visualization system is only possible through the allocation of RNSI access profiles" and that "the transfer of images to the Situation Room of the Command Territorial de Faro is carried out through the RNSI».

43. On the other hand, according to the protocol signed between the GNR and the Municipality of Albufeira, the installation and management of the communications network that will link the video surveillance cameras to the control room and to the recording server will be the responsibility of the Municipality of Albufeira - which can only happen on a subcontracting basis, as noted above, points 30 to 32.

44. These facts indicate that there will be an interconnection between the RNSI and the video surveillance network, the latter, in fact, managed by the Municipality, about which, however, nothing is said in the Justification.

45. However, if the communication network of the Municipality of Albufeira is a private network, as the Municipality's workers have access to the Municipality's network, there is a risk that any of them (provided they are certified in the Municipality's

network) access the cameras of video surveillance, easily acquiring control over them (which allows them, for example, to zoom, remove masks or filters, turn cameras on or off, replace images with others, etc.). But if the Municipality's network is an open public network (simplifying the language, an HTTP Internet network), there is still the risk of anyone accessing the cameras and gaining control over them.

46. Even more serious is that the vulnerabilities of the Municipality's network extend to the RNSI, due to the interconnection between the two networks. In fact, an eventual intrusion or propagation of malicious software in the municipality's network could spread to the RNSI. On the other hand, despite stating that all security policies inherent to the RNSI are safeguarded, they may not apply to a network managed by a third entity, in this case a municipality.

47. The CNPD therefore recommends that the authorization imposes the physical and logical segregation of video surveillance networks from other networks, with the application of the HTTPS protocol. And it draws attention to the fact that, unless it is demonstrated that the network of video surveillance cameras and the recording server are

physically dedicated and segregated from other municipal network assets and that the management of this network by the Municipality is governed by the same security policies inherent to the RNSI, the proposed interconnection scenario is of high risk.

48. Another feature of the video surveillance system that raises the greatest concern is the reference to the management console that allows «remote viewing from any device» - cf. point 5. of Annex B. From a system security perspective, remote access implies a very high risk, and this possibility should therefore be prohibited. It is useless to have a segregated and isolated network if a communication channel on the Internet is occasionally opened, thus exposing the system to the vulnerabilities of an open network. Indeed, it is essential to ensure that access to the video surveillance system is physically located in the control room, and remote access is not admissible as it may compromise security.

49. Now focusing on the physical security of the video surveillance system, it should be noted that it is not clear how the physical installation of the cameras will be carried out, nor where the communication cabinets will be installed.

50. With regard to video surveillance cameras, point 1.a) of Annex B specifies that they have 'anti-vandal features with tamper-resistant screws'. But an "anti-tampering" mechanism is not mentioned in the cabinets, with alerts. It is true that, in the same Annex, point 5., it is stated that «[the] software platform has a "Site health" for the GNR to know at all times the status of all the equipment that is interacting with the platform» It seems that by equipment we mean the cameras and not the communication assets, if a camera is operational but its communication rack is compromised, an alert in the system does not seem to be guaranteed.

51. Thus, the CNPD recommends that the solution to be adopted include intrusion alarms also in the cabinets of communication where the cameras will be connected. Furthermore, taking into account the risk of acts of vandalism or intentional actions to attack the system, such as turning off cameras to prevent filming of acts planned offenses, it is essential that communications cabinets (installed in public space) are not located on the floor or at a height that makes them easily accessible.

52. Considering that, in the same Annex B, it is stated that the cameras, from the point of view of network connectivity, have only «one Gigabit Ethernet port 7 OOOBASE-TX, using a standard RJ-45 socket», it is concluded that , according to the defined architecture, each camera will connect to the communication cabinet by UTP cable. In this assumption, it is essential that this cable is not exposed, ideally being underground.

53. It is also important to consider the conditions relating to data recovery in the event of accidental deletion. Refer to point 2.1. of Annex B that data storage '[has a RAID controller

with 32GB DDR RAM or higher, supporting multiple RAID levels. The RAID controller configurations are replicated on the hard disks thus allowing greater fault tolerance». Therefore, the availability of data in relation to storage failures is ensured, but there is no provision for data recovery in the event of accidental deletion. Therefore, it is recommended that a backup system be considered that ensures the availability of data within the defined time window, which is 30 days.

54. Section 5 of Annex B also states that «[m]ore reliability with high fault tolerance is provided for failover for this system».

The failover scenario, although mentioned, is not documented. In this regard, it should be noted that, for this scenario to exist, not just one, but two servers must be quantified, with the sharing architecture of the dedicated data storage unit. This is the only way to ensure system continuity in the event of a failure on the active server, starting to work on the passive server.

55. Finally, it is important to strengthen the control of entrances and exits of the rooms where the processing of personal data takes place. At point 4.g. of the Groundwork and in the AIPD, the system for controlling entrances to the different rooms is described, but it is important that the control mechanism - in order to be fully able to identify who, at any given moment, is in the two rooms - records, in addition to the entrances, also the outputs. Only in this way is it possible to demonstrate the subjective imputability of any event.

56. Finally, it is pointed out that there is not enough information on the procedure for extracting images for the purpose of criminal investigation. In particular, it is recommended to define rules on the procedure for the preservation of extracted images, including how these recordings are preserved to be excluded from the 30-day rotation of the system archive, and that guarantee their elimination after the completion of the process- crime.

57. Within the scope of the collection of images, the solution must include that the video surveillance system management software has mechanisms that enable the export in digital format, digitally signed, which attests to the veracity of its content. It should also allude to the presence of encryption mechanisms, if you want to protect the export with an access password or other security factor.

saw. Auditability of the processing of personal data

58. Regarding the prediction of the existence of logs (chronological records), in point 5. of the Rationale, it is noted that, for a system to be truly auditable, it is imperative to ensure that it has the detail

of the operation carried out, so that it is possible at all times to know who and what has done with the personal data.

59. In fact, in the same sense, Resolution of the Council of Ministers No. 41/2018, of March 28, points out, which also

determines the implementation of this requirement by the services of the Direct and Indirect State Administration. It provides for the obligation to record all actions that a user performs on personal data, including access attempts, as well as the obligation to guarantee its integrity, through a digital signature and TimeStamp.

60. For a better understanding of what is being said, it is exemplified that it is not enough to register that there was an action on a mask, it being necessary to specify whether it was placed, removed or changed.

61. A policy should be defined for the retention of activity records (/.e„ for how long they are retained until they are discarded) and key indicators for audit reports in terms of monitoring security in accesses and operations carried out, remembering that the function of chronological records is only achieved if they are the object of analysis.

62. In this way, it is important to point out that the person responsible for the treatment, that is, the GNR, must be endowed with human resources with sufficient technical knowledge to analyze the records and identify any incidents.

III. Conclusion

63. It is not within the competence that is legally attributed to it to pronounce on the concrete grounds for the use of the video surveillance system in the Oura and Baixa areas of the city of Albufeira, the CNPD, with the arguments set out above:

The. It believes that there are no elements that allow assessing whether the system does not have a disproportionate impact on the privacy and intimacy of people who are inside buildings or private spaces, mainly intended for housing and hotels, and thus cannot attest whether the established limits are respected. in paragraph 6 of article 7 of Law no. 1/2005;

B. Recommends that the regulation of the "voice alert" mechanism be densified, in the terms explained above, in points 16, 17 and 21;

ç. Insists that, as the person responsible for processing personal data, under the terms of the law, the GNR, must be expressly and clearly delimited in a contract or agreement, the intervention of the Municipality of Albufeira as a subcontractor of this entity, and of any subcontractors;

d. Since the applied software comprises Artificial Intelligence features that allow the tracking of citizens, the assumptions and criteria for its use not being defined from the outset, it recommends that, in any authorizing decision on the use of this video

surveillance system, activation is expressly prohibited. of these features.

64. The CNPD also recommends that measures be adopted capable of guaranteeing the security of the system and the auditability of the processing of personal data, in the terms indicated above, in particular in points 37, 38,47, 48, 51, 52 to 58 and 61 .

Lisbon, September 20, 2021

Filipa Calvão (President, who reported)