National Data Protection Commission

OPINION/2021/92

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 install a video surveillance system in the city of Funchal, submitted by the Public Security Police (PSP).

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). At the request of the CNPD, additional clarifications were provided on some technical aspects of the video surveillance system.

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 and, 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, whether, 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.

Av. D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

www.crp

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.

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 purpose of the treatment resulting from Video Surveillance in public places of common use in the city of Funchal

8. It is intended to install a video surveillance system consisting of 81 cameras, 65 of which are fixed and 16 rotating, in the city of Funchal, more specifically in downtown, on the waterfront and between the municipal park and the municipal market.

9. Implying the installation and operation of a video surveillance system in the city of Funchal, the processing of personal data which, due to its scope and extent, is likely to significantly affect the private life of people who circulate or are there, it is important to consider the purpose of using the system.

10. In the Justification accompanying the request, it is stated that the purpose "namely the "protection of people and goods, public and private, and prevention of the practice of facts qualified by law as crimes, in places where there is a reasonable risk of their occurrence", under the terms of subparagraphs c) of no. However, and because when characterizing the purpose of the treatment an adverb is used in particular, the CNPD recalls that, although the law, in paragraph 1 of the aforementioned article 2, admits other purposes, insofar as it identifies only the purpose of protecting people and property and preventing crime, the video surveillance system cannot be used for other purposes as long as it is not subject to the corresponding authorization.

11. Still regarding the general aspects of the processing of personal data, it is important to pay attention to its impact on the

privacy of citizens. Although it is intended that the cameras that make up the video surveillance system are "oriented only to areas of common use" (as is underlined in the AIPD), the truth is that there is a risk of capturing images of buildings intended for housing and, in any case, buildings and private spaces, within which people have the right and the expectation that their privacy will be safeguarded.

12. However, there is no express reference in the Justification to this risk and measures to mitigate it, other than the signaling of masks in some frames, the AIPD only mentions the creation of 'digital recording blocking zones through the programming the camera's own software'.

^ PAR/2021/38

L>

CNPD

National Data Protection Commission

13. It is recalled that, although it is not up to the CNPD, under the terms of the legal powers defined in Law no. 1/2005, to rule on the proportionality of the use of video surveillance systems in public places of common use, that competence already exists when cameras are installed in areas that are, by their nature, intended to be used as protection or to capture images or sound that directly and immediately affect people's privacy, or result in the recording of conversations of private nature (cf. paragraphs 4 and 7 of article 7 of Law n° 1/2005).

14. In this case, in addition to the extension of the processing of personal data, it should also be considered that some of these cameras have the ability to rotate and enlarge the image, which means the ability to capture, in all directions and with great acuity, images of people, in addition to the possibility of capturing sound.

15. Thus, not being sufficiently described the situations and terms in which the application of masks will take place, nor whether or not it will be possible to change or eliminate them, the CNPD cannot judge the proportionality of the processing of personal data under the terms of article 7 of Law No. 1/2005.

16. It should also be added, regarding the sound capture functionality, that it is not explained how it is guaranteed «that the system does not allow the capture of sound, except in situations duly provided for in the Law and duly authorized» - because the system does not have that functionality, or the system integrates such functionality, in which case the circumstances of its use must be specified.

17. It is insisted that the capture of sound and the capture of images of people in their homes and in spaces that deserve protection greatly impact privacy, and cannot be dependent on the subjective criteria of the agent who is currently operating the system, demanding, therefore, precise and specific guidelines.

18. Still in the context of general considerations on the processing of personal data resulting from the use of a video surveillance system, it should be noted that, despite the additional clarifications provided, there are aspects of the treatment on which the CNPD cannot conclude its assessment for lack of more precise elements.

19. This is, of course, the case with regard to the possible use of artificial intelligence technologies. Although it was stated, in the context of the aforementioned additional clarifications, that "despite the possibility presented, no facial recognition system will be used", it remains to be clarified whether the final solutions to be implemented still allow, and under what conditions, the tracking of people and vehicles. not being

Av. D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213928400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

this functionality is specifically described in the request and, therefore, it is not possible to assess its impact on citizens' rights, this possibility must be clearly prohibited.

20. Finally, it is noted that since the request, despite the additional clarifications, is still incomplete regarding the technical characterization of the solution for the system to be implemented, since it is outlined with generic references to products from manufacturers in the sector, without binding value, the CNPD is unable to conclude whether all the necessary measures will be taken to ensure the security of the video surveillance system and the integrity and auditability of the processing of personal data.

21. In view of this, some of the CNPD's observations will aim to contribute to the specification of the specifications for awarding the implementation of the video surveillance system, in order to ensure that the implementation of the technical solution does

not imply increased risks for personal data and citizens' rights.

iii. Responsible for treatment

22. The CNPD also emphasizes that the person responsible for processing personal data can only be the PSP, which is why it is strange that, in Annex C of the Justification, this responsibility is also attributed to the Data Protection Officer. Indeed, it states that the conservation and processing of data collected through the video surveillance system is the responsibility of «Data Protection Officer» (and identified there), in addition to «PSP - Head of the Operational Area of the Regional Command of Madeira».

23. It should be noted that the Data Protection Officer's intervention in all these procedures can only be advisory or control, and he does not have, under the law, decision-making powers on the processing of personal data and, therefore, , and cannot be held responsible for its implementation (cf. article 35 of Law No. 59/2019, of 8 August).

iv. subcontracting

24. Regarding the installation 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.

25. Establishing Law no. 1/2005, in paragraph 2 of article 2, that the person responsible for processing the data is the security force with jurisdiction in the catchment area or the respective security service, any subcontracting in company to ensure the maintenance or replacement of equipment has to be

formalized, contractually, with the PSP. It is not excluded that the PSP subcontracts the Municipality of Leiria, 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 PSP without the domain or control of the processing of personal data that the video surveillance system performs.

26. It is therefore important that a contract or agreement be signed that specifically regulates this subcontracting relationship,

binding the Municipality under the terms of that legal rule - which in the specific case does not seem to occur, since the text of the protocol annexed to the Rationale is insufficient from this perspective.

27. 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

28. Annex B shows two physical locations for data aggregation: the data processing center in Paços do Concelho and the PSP's Madeira Regional Command. From Annex F, it follows that there will be a conditioned access compartment for the physical media supporting the recording of recorded data. In the letter that includes additional clarifications, it is stated that "only the communication assets will remain in the City Hall, with no data capture, and the server with data processing, visualization and workstations will be located exclusively in the command and control center operational of the PSP'.

29. Therefore, it is recommended that the communication assets to be housed in the City Hall are in an infrastructure that is segregated from the rest of the Municipality's data processing center, if possible in separate racks and protected by a "cage" with a key, accessible only to authorized personnel to carry out maintenance interventions on the video surveillance system.

30. As for access control at the Command and Control Center of the Regional Command of Madeira, where the monitoring screens will be installed, it is specified that this is a space with restricted access to duly accredited communication operators, also admitting the access by others, upon request and service reason that justifies it.

31. Also specifically with regard to the conditioned compartment where data is recorded, Annex F of the Justification provides for “an access control system that only allows the entry, without supervision, of duly qualified and authorized persons; as for the remaining persons, the accompanying persons must prevent them from having access to the products stored there', providing for registration

of accesses. It is further mentioned that access to this compartment depends on a key kept in a sealed envelope, accessible

only to personnel assigned to functions in the video surveillance system.

32. In response to the request for additional clarifications, it was specified that a control system will be implemented that guarantees the «verification at all times of entries and exits of those who were present in the spaces at a given moment. The use of a key will only be a last resort if a general power outage occurs, although the Regional Command is equipped with an emergency generator set».

33. The CNPD underlines the importance of the access control mechanism being able to record, in addition to entries, exits. Only in this way is it possible to demonstrate the subjective imputability of any event. In addition, this mechanism must require two-factor authentication.

34. As for the alternative solution of keeping the access key to the compartment in a sealed envelope, it is stated, in Annex F, that "opening the envelope always implies the elaboration of information justifying the respective reason, proceeding in the shortest deadline for packaging the key in a new sealed envelope, dated and signed by the person responsible for storing and processing the data. As the replacement of the access key appears to be limited to situations in which there is a "break in security or where such a possibility is suspected", the planned measure of (re)storage of the access key in a new envelope is not sufficient to guarantee the confidentiality of the access key and, consequently, the integrity of the recorded images. Thus, the CNPD recommends that, whenever there is a need to open the envelope, the access key is replaced.

35. As for the registration of non-accredited persons, since this registration depends on the action of an accredited element, it is necessary to adopt a solution that does not allow errors or omissions in the registration of those persons.

36. Asked for clarification as to whether access to the camera console is available on the network and whether it is accessible from another device on the same network, such as at the data aggregation point located in the municipal hall, the answer was that "all the cameras will be protected with a username and password, being only accessible in the PSP's operational command and control center».

37. It is recommended that a logical network architecture be defined in which it is not possible to connect computer equipment to the communication assets and access the cameras' web consoles. A secure authentication policy must also be defined for the accesses to be assigned to each of the equipment's consoles, which prevents the possibility of a single common credential for all equipment.

38. Still in the context of the system's security, 32 telecommunications distribution cabinets are indicated, each of them aggregating several cameras in the vicinity. For further clarification, it was stated that “the lockers will have reinforced anti-intrusion protection, as well as an alert/alarm system in the event of a break-in connected to the PSP command and control center”. It is also important to ensure that telecommunications distribution cabinets - therefore installed in public spaces - are not accessible to anyone, especially due to the risk of acts of vandalism or intentional attacks on the system, such as turning off cameras to prevent filming of planned illicit acts. It is therefore essential that they are not located on the ground or at a height that makes them easily accessible.

39. Finally, it is pointed out that 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 the support and maintenance services for the video surveillance system are provided physically on site, and remote access is not admissible as it can compromise security.

saw. Integrity and auditability of the processing of personal data

40. For the purposes of criminal investigation, a process of extracting images is foreseen, «when there is notification for their preservation under the terms of article 55 Code of Criminal Procedure, and/or by direct and formal request of the Judicial Authorities».

41. In this regard, it is important to emphasize that the video surveillance system management software must have mechanisms that enable the export in digital format, digitally signed, attesting to the veracity of its content. And encryption mechanisms must also be provided if the export is intended to be protected, in the context of, with an access password or other security factor.

42. In the AIPD, contained in Annex J of the Justification, it is stated that “access to the recorded images will only be carried out by authorized and accredited police officers for the purpose and for reasons provided for in the Law. Each authorized user will have an autonomous profile on the video server that allows tracking of all actions performed on the system». In turn, Annex F states "All interventions carried out at the level of (local systems) are recorded in digital format, in an encrypted form, in real time and in a way that they can be audited, and the event recording system must be always-on, in order to allow such audit

operations'.

general@

Av. D. Carlos 1,134, I

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

WWW.

PAR/2021/38

4v.

43. It should be noted that, for a system to be truly auditable, it is imperative to ensure that it has the details of the operation carried out, so that it is possible at all times to know who and what has been done with the personal data. 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.

44. For a better understanding of what is being said, take the following example: it is not enough to register that there was an action on a mask in the captured image, it is necessary to specify whether it was placed, removed or altered.

45. In the additional clarifications, it was specified that the records will have a time stamp (timestamp) and that the encryption will be defined in the software to be acquired so that it is available only and only to accredited persons.

46. The CNPD recommends that a policy be defined for retaining traceability records and key indicators for audit reports, in terms of monitoring security in accesses and operations carried out, underlining the importance that chronological records are regularly subject to analysis, under penalty of not fulfilling their function of enabling the detection of failures and anomalies

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

III. Conclusion

48. It is not within the competence that is legally attributed to it to pronounce on the proportionality of the installation of a video

surveillance system in the city of Funchal, the CNPD, with the arguments set out above:

The. It emphasizes that capturing sound and capturing images of people in their homes and in spaces that deserve protection have a great impact on privacy, and cannot be dependent on the subjective criteria of the agent who is currently operating the video surveillance system, complaining, for this very reason, precise guidelines - in their absence, or in the absence of information to the CNPD

on them, the CNPD cannot conclude its judgment on compliance with the requirements of article 7 of Law No. 1/2005;

B. It warns against the inadmissibility of considering the Data Protection Officer (EPD) as responsible for the treatment, since in all personal data processing, the intervention of the EPD can only be consultative or control, not having it, under the terms of the law, decision-making powers on the processing of personal data and, therefore, cannot be held responsible for its execution;

ç. And it insists that, being the person responsible for the processing of personal data, under the terms of the law, the PSP, must be expressly and clearly delimited in a contract or agreement the intervention of the Municipality as a subcontractor of this entity, as well as of any subcontractors.

49. Since the request, and other information provided, is silent on some elements of technical characterization of the video surveillance system, the CNPD cannot carry out a complete assessment of the security of the system and also of the integrity and auditability of the data processing personal, so it is limited to recommending the adoption of a set of measures, in the terms specified above, in points 28 to 47.

Lisbon, July 5, 2021

Ana Paula Lourenço (Rapporteur)

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832