

National Data Protection Commission

OPINION/2022/102

## I. Order

1. By order of the Secretary of State for Home Affairs, an opinion was requested from the National Data Protection Commission (CNPd) on the request for authorization to expand the video surveillance system in the city of Olhão, submitted by the Public Security Police (PSP).
2. The request for an opinion was submitted on August 30, 2022, pursuant to Article 5(3) of Law No. 95/2021, of December 29, which regulates the use and access by the forces and security services and by the National Emergency and Civil Protection Authority to video surveillance systems for capturing, recording and processing image and sound.
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 the "Basicities", as well as the impact assessment on data protection (AIPD).

## II. appreciation

- i. Purpose of the opinion to be issued pursuant to article 5 of Law No. 95/2021, of December 29

4. Thus, pursuant to paragraph 3 of article 5 of Law No. 95/2021, of December 29 (hereinafter, Law No. 95/2021), the opinion of the CNPD, issued within the deadline set out in no. 4 of the same article (in conjunction with subparagraphs b) and c) of article 87 of the Code of Administrative Procedure), it is restricted to the pronouncement on the compliance of the request with the rules referring to the security of the treatment of collected data and with the provisions of paragraphs 4 to 6 of article 4 and articles 16, 18 to 20 and 22 of the same legal diploma.

5. In accordance with the provisions of these articles, the CNPD's opinion also includes respect for the prohibition of installing and using fixed or portable cameras in areas which, despite being located in public places, are, by their nature, intended to be used in seclusion and even the use of video cameras when the capture of images and sounds covers the interior of a house or building inhabited or its dependency or of hotels and similar establishments, and when this capture affects, directly and immediately, the sphere of the reserve of intimate and private life.

6. The collection and subsequent processing of personal data is also the subject of an opinion by the CNPD, in particular when

carried out through an analytical management system for the captured data, by application of technical criteria, as well as respect for the conditions and limits of conservation of the recordings.

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

PAR/2022/66

1v.

r

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

ii. The scope and purposes of the processing resulting from video surveillance in the city of Olhão

8. Although it is not up to the CNPD, under the powers defined in Law No. 95/2021, to pronounce on the proportionality of the use of video surveillance systems in public places of common use, this power already exists when in question are cameras installed in areas that are, by their nature, intended to be used in seclusion, or when they capture images and sound from the interior of the house or building inhabited or its dependence or from hotels and similar establishments, or when the capture of images or sound affects, directly and immediately, the sphere of the reserve of intimate and private life (cf. paragraphs 4 to 6 of article 4 of Law no. 95/2021).

9. At issue is data processing resulting from the expansion of the video surveillance system in the city of Olhão. The system is currently made up of 26 cameras installed in the downtown area of the city of Olhão, and it is now intended, according to what has been declared, to expand it with 38 additional cameras, 20 of which will be installed in the commercial/downtown area of the city of Olhão. Olhão, and the others (18) on the main road axes of the city (cf. Annexes A, point 4., p. 8, of the Grounds). It is also planned to replace 3 of the cameras already installed in the downtown area (cf. Annexes A, point 4., p. 8, and D, p. 1, of the Grounds).

10. Thus, as stated above, it is intended that the video surveillance system in the city of Olhão will include 64 video surveillance cameras, substantially expanding the area for capturing images. However, the request refers to a total of 67 cameras (cf. p. 4) and, in fact, Annex C contains 44 cameras (26 bullet type and 18 multisensors). It is therefore important to ensure the coherence of the request and the respective grounds, clarifying the number of cameras to be installed and the total number of cameras that will form part of the video surveillance system in the city of Olhão.

11. It should be noted, however, that the effective number of cameras is much higher than this, since 18 of the new cameras are multisensors, each of which is composed of 4 cameras with independent operation capacity; which means that each of the sensors works, in practical terms, as an autonomous camera and the images captured by it are processed and visualized as if it were a camera. In short, at stake are not just 18 cameras, but 72 cameras, which, in reality, implies that the video surveillance system in the city of Olhão will now integrate a total of 118, or 121 - depending on the number actually targeted with the request, which still lacks clarification - (cf. Annex C of the Grounds).

PAR/2022/66

two

National Data Protection Commission

12. In addition to the significant expansion of the territorial scope of the video surveillance system, the purposes of the system are also extended: for the purpose of protecting people, animals and property, in public places or with public access, and preventing the practice of acts qualified by the law as crimes, in places where there is a reasonable risk of their occurrence, now add not only the purpose of operational response to ongoing security incidents, but also the purposes of traffic control and safety of people, animals and goods in circulation road and the prevention and repression of road violations, under the terms of paragraphs d), f) g) and h) of paragraph 1 of article 3 of Law no. 95/2021 (cf. Annex A of the Grounds).

13. However, the chambers are not specifically linked to a purpose or set of purposes. In fact, it is stated that the 20 cameras to be installed in the shopping/downtown area of the city of Olhão have the «primary objective of protecting the safety of people and goods and preventing the commission of crimes», and the 18 cameras to be installed in the main The city's road axes (Av. João VI, Av. Heróis de 1808 and the road tunnel on Av. Bernardino da Silva) will be «mainly aimed at preventing road traffic offences»(cf. Annex A, point 4., p. 8, of the Rationale).

14. However, this confusion or indiscriminate sharing of purposes between the different chambers undermines the formulation

of a judgment of proportionality regarding their use, because such a judgment requires a careful and thoughtful assessment of the suitability, necessity and proportionality of the functionalities of each of the chambers and, in particular, the analytical data management system intended to be used, depending on each of the declared purposes - and, strictly speaking, some of these functionalities or characteristics may prove to be, in concrete terms, unnecessary and excessive, or even not suitable. From the outset, it is difficult to justify the use of video surveillance cameras on the city's main road axes with the argument of preventing or combating crime; and the functionality of reading license plates (and their tracking) in the city center appears to be an excessive compression of fundamental rights to the reserve of privacy and freedom, due to the ease of, from this information element, to identify the driver.

15. As such, and in accordance with the analysis carried out in the AIPD (cf. p. 4), the CNPD recommends delimiting the purposes of the system by the different sets of video surveillance cameras, depending on the territorial areas to which they relate and the risks detected in them, in order to allow the assessment of proportionality by the body with authorizing competence under article 4 of Law No. 95/2021, as well as the proportionality of the image analytical management system, under article 16 .º of the same legal diploma.

16. It should also be noted that the request only seems to intend to record images, therefore, without capturing and recording sound. However, in Annex G of the Grounds, it refers, twice, to suitability

Av. D. Carlos 1,134,1o

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

PAR/2022/66

2 v.

of the data analytics management system for audio analysis, in real time and on recorded data, which leaves doubt as to the intention of its use.

17. The CNPD underlines that, if there is an intention to capture sound, no information elements were made available to the

CNPD that would allow an assessment of the risk to privacy (in particular, with the use of data analysis technology), which is why it is not may it be authorized without the competent opinion of the CNPD on compliance with the limit set in paragraph 6 of article 4 of Law no. 95/2021, pursuant to paragraph 3 of article 5 of the same diploma Cool.

18. Now considering the capture and recording of images, the application of privacy masks is foreseen, whenever the cameras capture images of buildings intended for housing, which are represented in the images contained in Annex B of the Grounds. And the AIPD clarifies that, "[w]hen the mere orientation of the cameras is not enough to guarantee that private areas are not filmed, digital recording blocking zones will be created through the programming of the camera's own software", specifying noted that, in these cases, «there will be no visualization in real time».

19. It should be remembered, however, that in accordance with the provisions of Article 4(5) of Law No. 95/2021, "private zones" correspond not only to residential buildings, but also to hotel establishments or similar. In the absence of specification, in the elements provided, of the purpose for using the buildings captured in the images, the CNPD recommends that the placement of masks also be ensured in any hotel or similar establishments, under penalty of violation of paragraph 5 of article 4. ° of Law No. 95/2021.

20. It is also recalled that privacy does not have to be safeguarded only inside buildings, but also in accessing them, especially when dealing with residential buildings (for information about who enters the house itself, or who there it is received, to be, directly, information related to private life and that deserves reservation).

21. Furthermore, it is alerted to the fact that the privacy masks have to be configured in terms that guarantee that the operators cannot remove them, being essential that effective privacy guarantee measures are adopted, both at the time of their definition ( by the installer), or regarding the type of credential required for its deactivation.

PAR/2022/66

3

u \j u-

National Data Protection Commission

iii. The use of artificial intelligence for real-time analysis of personal data - "data analytics"

22. It is also intended, according to the Grounds that accompany the request, the analysis of images using Artificial Intelligence technology, with Annex G as title or alleged content the «Description of the criteria used in the analytical management system

of collected data".

23. However, what is described in Annex G of the Grounds does not correspond to criteria for analyzing personal data, but rather to the mere description of the functions of the software to be used.

24. As a matter of fact, in Annex G it is explicitly stated that «{the definition of analysis criteria or standards is the sole responsibility of the person responsible for the treatment and conservation of data, and it is not possible for system operators to change the standards created».

25. Given that the PSP is responsible for processing for the purposes of Law No. 59/2019, of August 8, and Article 17 of Law No. 95/2021-, it is all too evident that the authorization request is completely silent on the criteria for the use of this technology.

26. Only the purposes of their use are foreseen, specifying that they serve the purposes of protecting people, animals and goods, in public places or with public access, and of preventing the practice of acts qualified by law as crimes, in places where there is reasonable risk of its occurrence; the purposes of traffic control and safety of people, animals and goods in road traffic; and the purpose of prevention and repression of road violations. And it adds as a «Limit to the video analytics management system» that «[n]either the video surveillance system, nor the video analytics system, allow the capture and processing of biometric data as determined in paragraph 2 of art. 16, of Law 95/2021 of December 29" and that "[the] technical analysis criteria cannot define the profile that leads to discrimination against natural persons based on special categories of personal data, in violation of article 6 of Law No. 59/2019, of August 8» (cf. Annex G of the Grounds). It is stated in the AIPD (cf. p. 16) that the system does not allow the capture and processing of biometric data.

27. It should be remembered that the CNPD must rule on compliance with Article 16 of Law No. 95/2021, pursuant to Article 5(3) of the same law.

28. Now, the analytical criteria of the captured data - which the national legislator called "technical" - are significantly relevant in assessing the proportionality of this specific operation of processing personal data, as they are likely to impact on the rights, freedoms and guarantees of citizens. Therefore, it should be subject to a specific consideration on its suitability and necessity in view of the purposes specifically aimed at with its use, on the part of those who define them (the controller), as well as

Av. D. Carlos 1,134,1o T (+351) 213 928 400 geral@cnpd.pt

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

PAR/2022/66

3v.

and by the body that, in the context of an authorization procedure, exercises the power to authorize processing and by the body with explicit advisory power in this matter (the CNPD).

29. With the CNPD issuing an opinion on the concrete application of the technology provided for in article 16 of Law no. the Government member with authorizing competence can assess the proportionality of the processing of personal data resulting from the use of the video surveillance system and, therefore, also from this specific processing operation, in accordance with the provisions of paragraphs 1 to 3 of article 4 . of Law No. 95/2021, it would be, for this purpose, essential to identify and explain (reasoning) the criteria that will guide the application of the functionalities described in Annex G. Which does not happen.

30. There is also no information regarding data processing: where it takes place (whether in each of the chambers, or in the server/software), who manages the processing, what measures are foreseen to prevent the alteration of the criteria, etc.

31. On the other hand, it is not accurate to say that the system guarantees that there is no processing of biometric data - as referred to in Annex G, p. 5, and in the AIPD -, since the circumstance of declaring that the technology «does not have facial recognition capacity» does not mean that other biometric data is not processed.

32. In other words, the safeguards made at the end of Annex G, of a merely declarative or intentional nature, are manifestly insufficient to ensure that the data analysis operation does not imply discrimination on the basis of constitutionally and legally prohibited factors, with nothing in the description of the management system that demonstrates that such risk is removed.

33. In short, it is indispensable to present the criteria for analyzing the data, under penalty of not being able to assess whether this treatment respects the different limits and conditions provided for in the law and in the Constitution of the Portuguese Republic. And it is also essential that the source code, which will be used in this system, be auditable, under penalty of emptying the function and inspection powers legally attributed to the CNPD.

34. Thus, given the omission, in the request, in the Grounds and in the AIPD, of identifying the criteria underlying the use of the data analytics management system, the CNPD is unable to verify whether the legal and constitutional conditions and limits to which this use, nor does the body with authorizing competence have sufficient elements to assess its proportionality. The CNPD recommends, for all these reasons, that this use is not, for the time being, subject to authorization, under penalty of its invalidity due to omission of consultation imposed by paragraph 3 of article 5 of Law no. 95/2021 .

National Data Protection Commission

iv. Video surveillance system security

35. From the perspective of the security of the video surveillance system, we highlight here the aspects that are not taken care of and reinforcing measures are recommended to integrate some shortcomings of the system.

35. Starting with the physical installation of the system, it is not specified how the physical installation of the cameras will be carried out and where the communication cabinets will be located. In Annex D of the Justification it is indicated that the cameras must «have the capacity to send an alarm in case of detection of cyber-attack or physical attack» and also the protection characteristics of the standard used. The CNPD therefore limits itself to recommending that the solution to be adopted include intrusion alarms also in the communication cabinets where the cameras will be connected, it being essential that they are not located on the floor or at a height that makes them easily accessible. and that, preferably, all cables are underground.

37. Attachment D also illustrates the topology of connectivity between the cameras and the server, with the illustration showing that the local switch is provided by the Municipality of Olhão.

38. In this regard, it is recommended to review the connectivity topology to follow good security practices, for example, ensuring that only the video surveillance system server is on the cameras' network, with access to them, and that the viewing of the images on operators' computers is done from the server. In this way, all accesses will be centrally auditable in the system, as well as data communication flows.

39. From Annex H. of the Grounds it follows that there will be monitoring screens in the Olhão Control Center and also in the Main Vision Centre, located in Faro District Command. Therefore, access to the system will be done at two geographically dispersed points. There is no mention of any segregation between the video surveillance system network and the others, managed by the Municipality and by the PSP itself. This sharing of network assets and the possibility of interconnection makes the system permeable to third-party access attempts.

40. Thus, the segregation of the video surveillance circuit network must be ensured, and, in order for the network to remain segregated and isolated, it must be ensured that the video surveillance system support and maintenance services are provided



physically on site, and not remotely, because of the risk of exposing the system to vulnerabilities in an open network.

41. In Annex D of the Rationale, redundancy, high availability and disaster response mechanisms are not mentioned.

Apparently, the availability of the data in relation to storage failures is not guaranteed, nor is there provision for data recovery in case of accidental deletion. The CNPD underlines that it is essential to contemplate a backup system that ensures data availability

Av. D. Carlos 1,134,1o

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

PAR/2022/66

4v.

during the legal retention period (30 days). In fact, nothing described in Annex D corresponds to or responds to the requirement set out in Annex G: «The platform must meet high availability requirements aimed at supporting critical processes, and the solution support hardware must be protected against failures through redundancy mechanisms. The management software must maintain its operation in the event of a hardware failure, guaranteeing the continuity of the operation».

42. As for the chambers, they are described in a generic way, in Annex D, the model of the chambers not being indicated, without it being possible to carry out a concrete assessment of their characteristics. However, references to the cameras' compatibility with a given protocol and the protocol on which communication with the platform is based allow us to presume that the cameras will not send images via analogue and that they will obey a specified pre-configuration. Thus, it is based on this premise that safety recommendations are set out below.

43. Presumably the cameras contain an integrated web server for video capture and configuration available in a standard internet browser, using HTTP protocol with no need for additional software, a protocol which is known to be unencrypted. This remote administration functionality presents an access vulnerability in case of compromise of the network, as access credentials to the cameras may be captured, and, if the access password to the camera's integrated server, which by default

comes from the factory, is not changed, the system is compromised from the start. Reasons why the server integrated in the cameras must be reconfigured to HTTPS, there must be a password management policy in the cameras and a single password must not be used for all equipment.

44. Furthermore, the video surveillance circuit network must not be exposed to Internet connectivity, resorting to the use of VLAN to separate the camera network from other communications. Finally, only the doors that are strictly necessary for the operation of the equipment must remain open in the segregated network.

45. Still regarding security measures, two notes: the first, to recommend that the authentication mechanisms - access to the viewing room and access to the system - be personal and non-transferable {eg, the two authentication factors must be unique, for each PSP agent}; the second, to emphasize that image extraction must be a privileged access functionality, therefore, not recognized by all operators with permission to view the images. There must be a record of the chambers and time interval in the extraction, as well as the person responsible for carrying it out.

46. Still on the subject of image extraction, Annex H of the Grounds does not explain the image extraction process, specifically, how these recordings are preserved to be exempted from the 30-day rotation of the system file. Within the scope of image collection, it must be included in the

PAR/2022/66

5

National Data Protection Commission

solution 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. The existence of encryption mechanisms should also be foreseen, in case the intention is to protect the export with an access password or another security factor. Some of these requirements are indicated in Annex G, regarding the analytical data management system, but, strictly speaking, these are requirements to be fulfilled regardless of the use of such management system.

47. One last note, regarding synchronization with legal time, to specify that it is recommended that the service consulted to synchronize the clocks be accessible to the recording server and that this act as a synchronization service for the cameras.

v. Auditability of the processing of personal data

48. As it envisages the recording of all interventions carried out at the level of local systems, as the person responsible for the

processing of personal data, the CNPD limits itself to reinforcing the importance of providing support and maintenance services to the video surveillance system physically on site, under direct supervision and monitoring by the PSP, as responsible for the processing of personal data, remote access is not admissible insofar as it may compromise security.

49. For the purpose of auditing the processing of personal data, it is also essential to define the retention time of records of interventions and operations in the video surveillance system. Thus, the CNPD recommends the provision of a record retention policy for audit purposes, defining the period of time until their disposal, as well as the forecast of key indicators for the audit reports in terms of security monitoring in the accesses and operations performed.

saw. subcontracting

50. Regarding the installation and maintenance of the video surveillance system, because it is directly related to information security and the ability of the system to fulfill the intended purposes, it is important to underline that this obligation falls on the person responsible for data processing, regardless of who owns the video cameras and other equipment that make up the system.

51. The CNPD emphasizes, in this regard, that corresponding, under the terms of the law, the person responsible for processing the data to the requesting security force or service [...] with jurisdiction in the catchment area, eventual subcontracting in a company to ensure the maintenance or replacement of equipment must be contractually formalized with PSP. The possibility of the PSP subcontracting the Municipality of Olhão is not ruled out, which may sub-subcontract companies, under the terms regulated in article 23 of Law no. 59/2019, of 8

Av. D. Carlos 1,134,1o

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

PAR/2022/66

5v.

of August. What cannot be is a reversal of roles, leaving the PSP without the domain or control of the processing of personal

data that the video surveillance system performs.

52. It is therefore important that a contract or agreement be entered into that specifically regulates this subcontracting relationship, binding the Municipality under the terms of that legal rule - which in this specific case does not seem to occur, since the text of the protocol attached to the Grounds is insufficient in this perspective.

53. Specifically with regard to sub-subcontracting, it should be remembered that, under the terms of the same Article 23, they depend on the prior authorization of the person in charge.

### III. Conclusion

54. Since it is not within its legally assigned competence to pronounce on the concrete grounds for the substantial expansion of the video surveillance system in the city of Olhão, the CNPD, with the arguments set out above and under the competence conferred by Law No. 95 /2021:

The. Draws attention to the indispensability of clarifying the number of cameras to be installed, as well as the total number of cameras that will form part of the video surveillance system in the city of Olhão, in view of the inconsistency detected between the request and the accompanying documentation;

B. Recommends the delimitation of the purposes of protection of people, animals and goods and of criminal prevention and repression, on the one hand, and road management and prevention and repression of road violations, on the other, by the different sets of video surveillance cameras, depending on the risks by area or zone, in order to allow the assessment of the proportionality of the video surveillance system, as well as the proportionality of the intended image analytical management system;

w. Points out that blinding masks to guarantee privacy must be applied to all windows and doors in buildings intended for housing and hotel activities or similar, and must be configured as indicated above, in point 21;

d. It also recommends the adoption of measures capable of guaranteeing the security of the system and the auditability of the processing of personal data, under the terms indicated above, in points 36 to 49;

It is. It recalls the indispensability of expressly and clearly delimiting in a contract or agreement the intervention of the Municipality of Olhão as a subcontractor regarding the processing of personal data resulting from the use of the system, as well as any sub-subcontractors.

55. In particular, the CNPD recommends not authorizing the use of the data analytics management system, in view of the

ostensive absence (in the request and in the elements that instruct it, maximum in the impact assessment

PAR/2022/66

6

National Data Protection Commission

on data protection) for defining the respective criteria, due to the impossibility of verifying compliance with the legal and constitutional conditions and limits on their use, in particular, assessing the proportionality of such use.

Approved at the meeting of November 15, 2022

Filipa Calvao (President)

Av. D. Carlos 1,134,1o

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt