/• NATIONAL DATA PROTECTION COMMISSION

OPINION/2019/92

i. Request

1. On October 4, 2019, 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 Portimão, submitted by the Public Security Police (PSP).

Having meanwhile reiterated the interest in issuing this opinion within the scope of the authorization procedure within the competence of the member of the Government responsible for the requesting security force or service, the CNPD assesses the project under the terms and for the purposes of Law No. 1/ 2005, of 10 January, amended and republished by Law No. 9/2012, of 23 February, which regulates the use of video camera surveillance systems by security forces and services in public places of common use, for capture and recording of image and sound and their subsequent treatment.

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”.

II. ASSESSMENT

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

Pursuant to Article 3(2) of Law No. 1/2005, of January 10, as amended by Law No. 9/2012, of February 23 (hereinafter, Law No. 1 /2005), the CNPD's opinion is limited to pronouncement on the compliance of the request with the rules regarding the security of the treatment of the collected data, as well as on the special security measures to be implemented adequate to guarantee the entrance controls in the premises, of 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.

In accordance with the provisions of the same legal precept and in 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 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, privacy, or results in conversations of a private nature being recorded.

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.

Pursuant to paragraph 7 of article 3 of the same legal instrument, the CNPD may also formulate recommendations with a view to ensuring the purposes provided for by law, subjecting the issuance of a totally positive opinion to the verification of completeness of compliance with its recommendations.

2. Video surveillance in public places of common use in the city of Portimão for the purpose of protecting people and property and preventing crimes

2.1. previous point

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 for the purpose of protecting people and property, this competence already exists when the cameras are installed in areas that are, by their nature, intended to be used as a guard or to capture images or sound covering the interior of an inhabited house or building or its dependence or affect, directly and immediately , the privacy of persons, or results in the recording of conversations of a private nature (cf. paragraphs 4, 6 and 7 of article 7 of Law No. 1/2005).

However, the installation of a video surveillance system in the city of Portimão implies the processing of personal data which, due to its scope and extent, seems to significantly affect the private life of people who circulate or are in that city. In fact, as will be better developed below, there are several aspects and characteristics of this system that justify the CNPD's apprehension regarding a special

impact of this processing of personal data on the fundamental rights of the respective holders. Let's see.

Firstly, it is intended to install a video surveillance system in the city of Portimão, with a total of sixty-one cameras. Fifty-one cameras will be located in three areas of Praia da Rocha (west area, central area and east area), “in order to guarantee the protection and safety of people and goods, and of the economic activity of the area covered by this video surveillance system in the Municipality of Portimão, against acts of vandalism and criminal offenses». The remaining ten fixed cameras “on the main access roads to the city of Portimão with the main purpose of preventing and repressing road infractions” (cf. Annex A of the Justification, as well as Annex D).

In addition to being obvious that the video surveillance system in public places of common use cannot, under the terms of Law no. (as invoked in the grounds of the request and also in Annex A to the Grounds), and that the other grounds presented do not reflect any consideration, in the light of the principle of proportionality, other than the consideration of the effectiveness (and alleged lower cost) of the performance of the function of criminal prevention and repression, without taking into account the impact that the use of such a system results or may have on the fundamental rights of citizens, the terms in which the request for the installation of the system is presented allows us to understand that the privacy of people and others its fundamental dimensions will be significantly affected.

On the one hand, in addition to the wide scope of incidence of the cameras (practically all of Praia da Rocha), it must be considered that such cameras have the capacity to rotate and enlarge the image, which means the capacity to capture, in all directions, and with great accuracy, images of people and vehicles, in an area intended for leisure and where, during the day, people are more exposed, so greater caution is required when using this type of systems. On the other hand, it must also be considered that authorization is provided for and requested for sound capture, with an evident impact on privacy.

But above all, the circumstance that the video surveillance system presents as characteristics the «Use of technologies (hardware and software) in the state of

r

art, including intelligent video analysis in [..J' software; «the ability [to] automatically handle unusual events and present them in recorded video simply to the nv operator, «Have advanced search for physical descriptions such as clothing colors (bottom and top), gender (M/F), hair color [,.p>\

«Possibility of, in the future, having license plate reading capability (LPR)y>\ «The software platform should have video analytics of "abnormal detection movements" from the same manufacturer» (cf. Annex B of the Justification).

At stake is the use of Artificial Intelligence (AI) and soft recognition technology, which may appear to be suitable, in certain circumstances, for the intended purposes. This is the case of the license plate reading functionality that can speed up the pursuit of purposes listed in article 13 of Law No. 1/2005. Even for the prevention and criminal repression in the field of protection of people and property, the appropriateness of its use is not questioned.

However, starting with the soft recognition technology, it is not possible to achieve, through the insertion in the system of people's physical characteristics or vehicle registrations, a better traffic management or even the prevention of accidents or a more efficient provision. assistance in the event of a road accident. But, even for the pursuit of the purpose of protecting people and property, the use of technology that allows tracking of people's movement and behavior requires a specific demonstration of the need for its use, which in this case does not happen.

In fact, at no point in the reasoning is there an explanation of the need for this specific technology and functionality, for each of the two groups of cameras, which pursue very different purposes, which obviously do not justify measures restricting privacy of equal intensity.

In this diversified context of the use of the video surveillance system, with the scope and incidence of sixty-one cameras, it is up to the CNPD to highlight the need to consider the use of these types of technology, considering the impact that it may have for the people covered by the radius. camera capture.

It is not, therefore, an absolute rejection of the use by security forces of the technology that science and the market make available today. It is only intended that the use of video surveillance systems and, in particular, of software technology

recognition is preceded by a careful consideration of its consequences for the privacy of individuals, as well as for other fundamental dimensions of the human being directly put in crisis with this type of processing of personal data, such as freedom and the right to equality (here in crisis, since the risk of traceability of behaviors and habits, as well as the selection of physical characteristics for soft recognition, can generate the conditioning of freedom of action and discriminatory controls from certain

profiles).

In the same way, and even by a majority argument, the use of AI has to be preceded by especially rigorous weighting. In effect, video analytics works through an algorithm that is programmed to respond to specific stimuli and movements, a matter on which the Rationale is completely silent. In fact, nowhere in the Rationale is it clarified which algorithm to use, from which assumptions it will start and which responses (outputs) are intended to be achieved.

Note that what is now presented here is an AI and computer vision solution. To that extent, its use must, obviously, be properly framed with pre-defined assumptions and criteria (perhaps with programming of inadmissible information analysis criteria, given the current legal regime), otherwise it will not be possible to understand whether the results presented by the system, and on the basis of which the PSP will make decisions about the citizens concerned, are discriminatory and, therefore, inadmissible under the Constitution of the Portuguese Republic.

It is therefore clear that the use of AI, especially when used in an environment of systematic and large-scale control of areas accessible to the public, must be preceded by a careful consideration of the consequences of the same, not only for the privacy of the people, as well as freedom, personal identity and the right to non-discrimination.

However, these considerations can and should be made by the legislator, in a desirable regulation of these technologies, since the regime contained in Law no. , but above all it has to be done within the scope of the authorization procedure for the installation and operation of specific video surveillance systems, such as the one at issue here.

The weighting judgment is evidently guided by the principle of proportionality, not only regarding the use of the video surveillance system with this extension and incidence in the city of Portimão, but also specifically regarding soft recognition and AI technologies, so that assess its suitability and necessity (and proportionality) to the pursuit of the purposes envisaged with this use, and conclude whether or not there is an effective correspondence between the advantages or potential of using that system and that technology and the protection of personal data and other rights associated fundamentals.

When developing, it is necessary to assess, first in relation to the video surveillance system with the 61 cameras, then specifically in relation to soft recognition and AI technologies, what type of crimes or infractions justify their use and to what extent they are adequate to prevent or to repress these illicit acts, if this suitability and necessity is manifested in all the

territorial areas of the municipality covered by the system or if only in some more delimited areas, etc. Also bearing in mind that the impairment of the fundamental right to respect for private life is irreversible, and is not subject to reinstatement.

In fact, the new Law no. (EU) 2016/680 of the European Parliament and of the Council, of 27 April 2016, requires the person responsible for these processing of personal data to carry out an impact assessment on data protection when there is a high risk for the rights, people's freedoms and guarantees.

In this regard, it is important to remember that Article 2(2) of Law No. 1/2005 determines that the processing of personal data resulting from the use of the video surveillance system is governed by the provisions of Law No. 67 /98, of October 26, in everything that is not specifically provided for in this law, and that this law, regarding the treatments carried out for the purposes of prevention, detection, investigation or repression of criminal offenses or execution of criminal sanctions, was revoked and replaced by Law No. 59/2009, of 8 August. Considering also that, in paragraph 3 of article 67 of this last piece of legislation, it is determined that "All references made to the Law on the Protection of Personal Data, approved by Law n.0 67/98, of 26 October, consider made for the regime of this iei, when they concern the protection of persons

individuals with regard to the processing of personal data by competent authorities for the purpose of preventing, detecting, investigating or prosecuting criminal offenses or enforcing criminal sanctions, including safeguarding and preventing threats to public security', can only be concluded by the application of the provisions of article 29 to the processing of personal data resulting from the use of video surveillance systems.

Thus, taking into account that this treatment implies a systematic control on a large scale in the city of Portimão and that it promotes the tracking of people and their behaviors and habits, as well as the identification of people based on data related to physical characteristics, there is no denying the high risk it poses to the rights, freedoms and guarantees of individuals, in particular the fundamental rights to data protection and respect for private life, as well as freedom of action and the right to non-discrimination.

For all these reasons, the CNPD considers that article 29 of Law no. of people and the careful assessment of the measures planned to mitigate them. Moreover, taking into account that the use of a part of the cameras aims to prevent and repress road infractions (when they do not correspond to a criminal offense) and traffic management, the impact assessment on data

protection would always be mandatory under the terms of paragraph 1 and c) of paragraph 3 of article 35 of Regulation (EU) 2016/679, of 27 April 2016 (RGPD).

In particular, in this assessment, each of the intended purposes must be considered autonomously and attention must be paid to the aspects of the treatment that the analysis of the technical characteristics of the equipment and other elements contained in the Grounds allow for the time being to be highlighted and which are set out below.

The data protection principles and rules must also be applied by design and by default, pursuant to article 21 of Law No. 59/2019, of 8 August, and article 25 of the GDPR. .

2.2. The technical characteristics of the system

Before starting to assess the technical characteristics of the system, it is important to note that the application for authorization to install the video surveillance system does not describe,

strictly speaking, the characteristics of the systems on which the treatment will be carried out, but rather the technical characteristics that the PSP determined would be required for such equipment1. The two concepts differ, as the first characterizes the way in which a technology was implemented, while the second can comprise multiple different technologies and also multiple different implementation scenarios. It is, therefore, the difference between what “is” and what “can be” that makes it difficult for the CNPD to assess the system's compliance with the conditions and limits set out in paragraph 2 of article 3 of Law no. 1/2015 and Ordinance No. 372/2012, of November 16.

Furthermore, there are aspects of the data processing carried out by or based on the video surveillance system that are indicated in the description of the technical characteristics, but in relation to which there is no information that allows understanding their contours and their foundations.

This is the case of the reference, both in Annex A and in Annex B, to the functionality of «reading license plates (LPR) of vehicles». However, since there is no mention of any interconnection, whether automatic or by manual consultation, with motor vehicle registration systems or other databases, it is not understood how the purpose of detecting falsified license plates and stolen vehicles, referred to in the Grounds. Thus, the CNPD has no elements to comment on this possible autonomous personal data operation.

Likewise, Annex B states that “The software platform should also enable the integration of indoor video analytics radars with maximum radius distances of 9 meters as well as other ONV/F devices”. However, on this point too, the request for an opinion is silent on this functionality.

1 As an example, in paragraph q) of the “Video performance”, which is part of the section “Technical characteristics of the equipment”, it is mentioned that “the Chamber will allow the transport of video and audio over: HTTP (Unicast); HTTPS (Unicast); RTP (Unicast and Multicast); RTP over RTSP (Unicast); RTP over RTSP over HTTP (Unicast); RTP over RTSP over HTTPS (Unicast)". information security and that, in the way they are listed, do not allow to assess the security of the system

M/ãTone

iw

IS NATIONAL COMMISSION

' DATA PROTECTION

Special mention should be made of the use of AI and soft recognition, without specifying in what terms, under what assumptions and under what criteria these technologies will be used. Such omission prevents any type of assessment of respect for the limits and conditions relating to the protection of privacy - in the terms defined in paragraphs 6 and 7 of article 7 of Law no. part of the body with authorizing competence, the adequacy, necessity and respect for the prohibition of excess regarding the use of this video surveillance system with these attributes.

Strictly speaking, the identification of patterns such as those described in the Rationale (and transcribed above, in 2.1.) implies a video analysis with confrontation with detection algorithms. The “advanced search” functionality, for example, seems to indicate that the captured (and stored) video can be scanned to identify patterns, given that nothing prevents the technology that allows the detection of a certain color of clothing be configured to detect a certain skin color or other potentially discriminatory characteristic.

However, the Groundwork does not describe the algorithms involved in the comparison and detection of patterns, it is not specified who is responsible for defining these patterns, and the criteria involved in these patterns are not specified either {e.g., which visual patterns the system uses to differentiate a man of a woman; what are the configured tolerance rates for false positives/negatives).

Furthermore, the requirement for the system to provide the operator with 'programmed sequences of video events according to priority and according to the types of rules violated' (cf. Annex B of the Justification) is not sufficiently clear. In fact, it is not understood whether the “violated rules” refer to video detection configurations (e.g., zone entry detection) or whether they correspond to true identifications of infractions, detected by the video analysis system.

It is stressed that the lack of transparency in the information analysis process not only does not allow, exante, to understand the consequences of its use and therefore the real scope and impact of the use of this video surveillance system, but also does not allow to satisfactorily guarantee, under the terms imposed in law, the right of information to data subjects.

As mentioned above, in 2.1., in addition to not finding, in the reasoning presented, arguments specifically designed for the use of this technology for the purpose of protecting people and goods and controlling traffic, they are not established, nor is it declared that will be fixed, the situations that will justify their use, nor the assumptions and criteria that will be the basis for the insertion of physical characteristics or other information related to people, and what kind of criteria could be the basis of the intelligent analysis of the information and of profiling.

Considering that there is a set of personal data that are subject to a specially reinforced regime of protection - those provided for in paragraph 1 of article 6 of Law no. of the same article prohibits the creation of profiles that lead to the discrimination of natural persons based on these data2, the CNPD understands that the use of this type of technology must, at the very least, be preceded by a set of precise rules for its users, in order to limit the risk of discrimination and infringement of Article 6 of the aforementioned law.

In addition, it is not clear what the metadata sent from the chambers consists of, nor what type of research it is possible to carry out on this information.

Turning now to an analysis focused on the technical characteristics of the system, the following should be highlighted:

The. With regard to safeguarding privacy and the intimacy of private life, despite referring, in Annex B to the Grounds, to the application of "privacy masks" and the fact that in the images reproduced in Annex A there are buildings marked with black areas, there is no sufficient information in the request that allows the CNPD - and the body with authorizing competence - to assess compliance with the limits provided for in paragraphs 6 and 7 of article 7 of Law No. 1/2005.

And as for sound capture, strangely, no justification is found in the Groundwork. Taking into account the prohibition contained in paragraphs 6 and 7 of article 7 of Law n° 1/2005, the adequacy and necessity of this treatment is not demonstrated, the criteria to which

2 And, within the scope of the processing carried out for the purpose of traffic management, the personal data provided for in paragraph 1 of article 9 of the GDPR and the limits imposed by paragraphs 2 and 4 of article 22 thereof University Degree.

capture will not comply, nor, to be concluded by its suitability and necessity, are indicated any mitigating measures of the resulting privacy affectation.

To that extent, the CNPD can only conclude that this functionality violates the provisions of the aforementioned legal provisions.

On the other hand, it is also mentioned that the cameras must be equipped with audio output connections, for an external loudspeaker, and there is no reason for such a requirement in the Grounds, nor, once again, criteria that delimit the situations of their use. .

B. In the section “Description of the system to be implemented” in Annex B of the Rationale, the need for the system to have “high scalability and connectivity, allowing for the growth of the system and its integration with other electronic property security systems, is mentioned. Given that no interconnections are described for the processing of the data in question, it is not understood which are the possible “electronic systems of asset security” with which the possibility of integrating is proposed.

It is, therefore, essential to specify any data interconnections that the controller intends to implement, so that the CNPD can issue the appropriate ruling.

ç. Annex B requires that the system has «double authentication, one of them being a "QR Code"». In this regard, it should be noted that it is not clear what application is intended to give the QR Code in this context, since a unique QR Code is generated for each authentication, similar to what some applications do to validate access.

To this extent, it is not possible to assess whether this mechanism provides greater or lesser security until it is better implemented.

d. It is also required that the system has «export password)).

If the security of the export mechanism is based exclusively on a password, this measure alone is not enough to guarantee the

t

system confidentiality. It is also essential that access profiles for this export functionality are set in appropriate terms.

and. Annex B also mentions that the «Use of state-of-the-art technologies (hardware and software) including intelligent video analytics in the software at no cost on the same platform without adding third-party software. Intelligent video analytics must be embedded directly in cameras with intelligent video analytics by metadata and must have a minimum of 10 rules per camera, to be specified in some models below. Intelligent video analysis on cameras should be by standards and not by "motion" or "advanced motion"».

However, considering that the system is based on a centralized architecture, the reason why it is imperative that the cameras themselves be embedded in technologies, namely intelligent video analysis, is not clear. In fact, the biggest advantage of using this type of architecture is to take advantage of the configuration and control at the central level, ensuring the homogeneity and control of configurations and access.

f. Still regarding the specifications of the video cameras, it is mentioned the requirement to be equipped with SD (Secure Digital) memory cards to record video «.inside». Although this requirement is not justified, it is assumed that it is intended to guarantee a constant flow of data in case of occasional loss of connection with the server.

However, considering the risk of undue access to images stored on SD cards, the installation of local storage systems must be considered and justified.

g. Also in Annex B of the Justification, it is mentioned as a characteristic of the system «Having the possibility to integrate the access control of the same manufacturer in the future and through it to carry out advanced analytics searches such as search for appearances (face, body) in the video surveillance system» .

¥ NATIONAL COMMISSION

» OF data protection

It remains to be explained how access control - a concept traditionally associated with the control of physical access to

infrastructure - can be integrated with advanced research in a video surveillance system.

Still on access control, but now related to server security, it is mentioned that «the platform must have double authentication for viewing the recorded video». To guarantee the confidentiality of system data, the double authentication mechanism must be extended to all types of access, whether for access to recorded images, real-time images or configuration changes.

H. As for the system's audit mechanisms, only access logs are referred to.

However, paragraphs 3 and 4 of article 4 of Ordinance no. 372/2012, require logs that record all user activity, as well as changes in system configurations (e.g., change in the mask area view). This requirement is reinforced in article 27 of Law no. reasoning.

i. It should also be noted that the «Minimum computer requirements» required for the Portimão Control Center and for the Main Vision Center are the same. However, insofar as the former can only display images (in the terms stated in the Grounds), the computers destined for that location must not have the «DVD Reader/Writer» hardware and USB ports that appear in the specifications. If they exist, these interfaces must be inhibited.

2.3. Other aspects of system operation

It should also be noted that, in Annex B, it is required that the system allows "to put any camera on "stand by" with the proper credentials of the person responsible for processing the data (Data Protection Officer)".

It should be noted that such a requirement is in clear contradiction with the personal data protection regime and with the duties of Data Protection Officer (cf. article 35 of Law No. 59/2019, of 8 August , article 39 of the GDPR, and article 11 of Law No. 58/2019, of 8 August). If, on the one hand, it is not up to the latter to make changes to the processing conditions, on the other hand, it is unlawful for it to operate “with the proper credentials of the data controller”.

It is also important to pay attention to another aspect. In the Groundwork, with regard to the «mechanisms to ensure the correct use of the recorded data», it is clarified that at the Portimão Control Center, installed at the Portimão Police Station, the control of access to the monitoring screens will be guaranteed by an «element police officer who is permanently at that crossing point'. Also with regard to the Main Visioning Centre, located in the District Command of Faro, it is mentioned that

access is restricted to communications operators. In either case, measures capable of guaranteeing access control are not specified.

Therefore, it is recommended to adopt a control mechanism that allows auditing access to facilities.

2.4. The rights of information, access and deletion of data

Regarding the rights of data subjects, attention is drawn to the fact that they are currently defined in Law No. , detection, investigation or prosecution of criminal offenses or enforcement of criminal sanctions, transposing Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. The right to information is specifically addressed of data subjects, further defined in article 14 of Law No. 59/2019, of 8 August.

It is noted as positive that, in this new project now being appreciated, in addition to declaring that the warning and symbology models to be used respect the provisions of Ordinance no. information on the installation of the video surveillance system in digital media for disseminating information from the PSP (cf. Annex E of the Justification).

However, considering the AI and soft recognition technologies that are intended to be associated in the analysis of the information that the system collects, it is evident that the right to information has to be much more densified, at least when it comes to the pursuit of traffic management and prevention and repression of road infractions that do not constitute a crime - because the right to information here follows the rules of article 14 of the RGPD.

With regard to the rights of access and deletion of data, it is stated, in Annex C of the Justification, that they will be guaranteed in accordance with the provisions of paragraph 1 of article 10 of Law no. 1/2015.

III. CONCLUSION

It is not within the competence that is legally attributed to it to comment on the concrete grounds for the installation of a video surveillance system in the city of Portimão, the CNPD, with the arguments set out above:

1. It considers that the fulfillment of the duty, provided for in article 29 of Law no. .° of the GDPR, to carry out a prior assessment of the impact of the processing of personal data on the rights, freedoms and guarantees of individuals, within the scope of this authorization procedure, in particular regarding the use of Artificial Intelligence and soft recognition technologies,

2. Within the scope and following the aforementioned impact assessment, considers it particularly relevant:

i. The consideration of the different rights and interests in tension, not only regarding the video surveillance system with the declared scope, but also regarding the level of intrusion on the privacy and freedom of citizens, as well as the right to non-discrimination, resulting from the use of Artificial Intelligence and soft recognition, depending on each of the purposes pursued - namely, the protection of people and goods and the prevention and repression of road infractions and road traffic control;

ii. Understanding that compliance with the legal regime of data protection and privacy is achieved by the way data processing is designed and implemented and not by the use of a specific type of technology;

iii. The prior definition of a set of binding rules for the use of these technologies, in order to limit the risk of discrimination and violation of article 6 of Law No. 59/2019, of 8 August;

iv. The presentation of reasons and elements that make it possible to understand the real scope and impact of the use of those information analysis technologies in the context of this video surveillance system, under penalty of not being possible to judge proportionality by the body with authorizing competence, nor the CNPD judgment to issue regarding the limits defined in paragraphs 6 and 7 of article 7 of Law no. 1/2005;

3. As part of and following the impact assessment, it recommends taking into account the observations contained in points 2.2 to 2.4.

In these terms, especially considering that the use of a video surveillance system with the characteristics already highlighted represents a high risk for the privacy of citizens, not only because of the amount and type of information that can be collected from the captured and recorded images, but also due to the opacity of the process of defining analysis standards and their detection, the CNPD issues a negative opinion regarding the request for authorization to install a video surveillance system in the city of Portimão.

The need for further consultation with the CNPD is also highlighted, regarding the aspects omitted in the request now presented, and on which, under the terms of paragraph 2 of article 3 of Law no. your pronunciation.

Lisbon, December 27, 2019

Filipa Calvão (President, who reported)