í

OPINION/2021/143

I. Order

1. The Committee on Constitutional Affairs, Rights, Freedoms and Guarantees of the Assembly of the Republic asked the National Data Protection Commission (CNPD) to issue an opinion on Draft Law No. 111/XIV/2.a (GOV) , which 'Regulates the use of video camera surveillance systems by security forces and services'.

2. The CNPD issues an opinion within the scope of its attributions and competences as an independent administrative authority with powers of authority to control the processing of personal data, conferred by subparagraph c) of paragraph 1 of article 44 of Law no. 59/2019, of 8 August, as well as by subparagraph c) of paragraph 1 of article 57 and by subparagraph b) of paragraph 3 of article 58 of Regulation (EU) 2016/679, of 27 April 2016 - General Data Protection Regulation (hereinafter RGPD), in conjunction with the provisions of article 3, paragraph 2 of article 4 and paragraph a) of paragraph 1 of the Article 6, all of Law No. 58/2019, of 8 August, which implements the GDPR in the domestic legal order.

II. Analysis

3. The purpose of the proposed Law is to regulate the use of video surveillance systems by security forces and services, revoking Law no. 9/2012, of February 23 (hereinafter, Law No. 1/2005). As stated in the Explanatory Memorandum, «[...] the technological advances, which have led to significant changes in terms of the technical characteristics of the systems that the market offers at any given time, require that the legal framework be adapted to today's technical solutions. existing".

4. In this context, the Draft Law extends not only the type of media in which video cameras can be incorporated, but also the purposes to be pursued with their use and the object of incidence itself, which goes beyond the public space, starting to cover also areas of the private domain destined to the movement of people, vehicles, ships and boats. It also regulates “access by security forces and services to private surveillance systems, installed in public or private places accessible to the public” (cf. Explanatory Memorandum). In addition to the permission, without restrictions or limits, of the use of artificial intelligence technologies, in a wording that allows the use of facial recognition technologies in public or private spaces with public access.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

i. General considerations

5. Without going through the analysis of each of these changes for the time being, it should be noted that this multiple expansion of the use of video surveillance systems carries with it the obvious risk of allowing inappropriate, arbitrary or excessive use, when is not accompanied by a well-defined legal regime that sets out the conditions for the use of each type of medium used to capture and record images and sound, and the respective safeguards, taking into account the specific risks or impacts that each of them entails on rights fundamentals of citizens. And this is precisely the biggest gap in this Bill.

The. Absence of precise rules on the processing of personal data, in particular guarantees of fundamental rights

6. In the eagerness to cover all the situations that in the last decade would have, from the perspective of the security forces and services, justified the use of video cameras and the new technologies that enhance their use, the Proposal foresees all the equipment and technologies available today, almost in an alternative logic, as if there was no difference in impact on citizens' rights. And purposes for their use are listed, in an undifferentiated way, when for the pursuit of part of them only some types of means of incorporation of cameras, among those provided here, will prove suitable.

7. However, in a democratic State of Law, the mere generic provision of the use of video surveillance systems is not admissible, especially with the use of technologies that enhance their effects, without specifying the conditions, limits and criteria necessary to guarantee their suitability. for the pursuit of public interest purposes, but also essential to ensure that fundamental rights are affected to the extent strictly necessary and without excess.

8. It is recalled that the use of video surveillance systems in public spaces always represents an interference with fundamental rights, in particular the rights to respect for private and family life and the protection of personal data, enshrined in articles 26

and 35. ° of the Constitution of the Portuguese Republic, as well as in articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Private and family life also deserves explicit protection in Article 8 of the European Convention on Human Rights, and the jurisprudence of the European Court of Human Rights is known to require that legislative measures restricting those rights, especially in the context of police activity, have the degree of precision necessary to ensure the predictability of its effects and prove to be adequate, necessary and proportionate to safeguard essential Community values set out in paragraph 2 of that article 8.

9. The absence of a precise legal regime, with the definition of conditions and limits for the use of each of the types of technical means available today for capturing and recording images, impairs predictability

indispensable in a legal diploma that, in itself, with the intention of protecting public values of security and fundamental rights, foresees and implies intense restrictions on other fundamental rights. And it represents a "blank check" to the intrusion into the private life of citizens, as if the fact that they are in public spaces or with public access implies the automatic denial of this fundamental human dimension. Furthermore, it also allows, also with great openness, rectius, with no normative density, the use in this context of artificial intelligence technologies, especially facial recognition, in the apparent ignorance of the risks of error and discrimination that their use may result from.

10. It is this "blank check" represented by the Law Proposal that raises the most apprehensions in the CNPD. Above all, taking into account the effective conditions of use of video surveillance systems by the security forces and services that the CNPD has verified, in the exercise of its inspection activity, which reveal that the existing video surveillance systems, whether due to the absence of rules and criteria clear and standardized as to their use, whether due to the lack of respect for the few existing regulations, or due to the lack of means for effective control, by the security forces, of the equipment and its use, they have not shown themselves to be able to pursue the intended purposes. .

11. Thus, before analyzing each of the legal provisions that give rise to reservations from the perspective of protecting the

fundamental rights of citizens in the context of the processing of personal data, the CNPD believes that it is useful for holders of political-legislative power to list some examples that reveal the current status of data processing carried out in the context of the use of video surveillance systems under Law no.

B. The operation of already authorized video surveillance systems

12. The CNPD has been monitoring the processing of personal data carried out by video surveillance systems in public spaces by the Public Security Police (PSP) and the impact of using new tools available depending on technological developments, whose use has been authorized by the member of the Government with delegated competence in the matter. The situations presented here are described in the CNPD's interim reports regarding the inspections already carried out, and the CNPD expects to carry out further inspections, taking into account that, in the meantime, new authorizations have been issued that legitimize the use of different technology. As soon as these follow-up procedures are completed, the CNPD will issue a statement on the processing of verified personal data, of which the holders of political-legislative power will be informed.

13. Thus, so far, the CNPD has verified that the processing of personal data carried out by such video surveillance systems does not meet many of the requirements provided for either by law or in the ordinances that Law no.

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

1/2005, as well as in the systems authorizing dispatch. Next, some of the detected nonconformities are presented.

14. It should be noted that, despite the PSP being responsible for handling the inspected video surveillance systems, the installation and maintenance contracts, both preventive and corrective, of these systems are concluded by the municipalities and the companies providing the services, without any intervention. of the PSP and without the latter knowing its content. Therefore, as it is not a party to these contracts, PSP is not entitled to demand any support, correction, or updating of the

systems.

15. The analyzed contracts do not contain any data protection rules, as required by law, nor do they oblige the workers of the companies that provide support services to the system, as a rule with administration profiles, to be accredited by the National Security Office.

16. In addition, all the system administration profiles, which allow all operations to be carried out, therefore also the most sensitive, do not belong to PSP agents, who are unaware of them, but rather to people from service providers.

17. It was also found that the software of the machines and the firmware of the video surveillance cameras were not up to date, keeping the versions of the moment of installation, when these updates are essential to guarantee the security of the system.

18. As for the access control systems to the visualization rooms and data center, it was found, in one of the cases, that it was broken and, in another, that the access control system to the data center was turned off. But, even if they were all active, it was concluded that such systems have major weaknesses; it was found that access cards are used with technology susceptible to cloning by applications that can be downloaded free of charge on the Internet and that there is no second authentication factor.

19. In one of the inspected systems, the room used as a data center (with access control turned off) was the only passageway to the agents' locker room, which demonstrates the lack of conditions in the facilities to guarantee the security of the system.

20. Also in one of the verified video surveillance systems, the network of the video surveillance system was not segregated, being shared with the Municipality's network and the backstage that connected the cameras to this network were placed on the floor (of the public space), making them especially vulnerable to unauthorized access and attacks.

21. With regard to audit records, they were found to be unreliable. Indeed, they do not make it possible to identify who performed an operation in the video surveillance system (e.g. access, elimination of privacy filters), when he performed it and what type of operation he performed.

22. Audit records are not subject to analysis and there is no alarmism for situations outside of normal usage patterns. In fact, accesses by users who were not authenticated in the system, nor in the service (scale) were detected by the CNPD, which

configured a typical attack behavior, without the PSP or the contracted company having detected it.

23. None of the systems had a Disaster Recovery plan, not even backups.

24. The systems were not synchronized with the legal time. The system devices (cameras and workstations) did not show the same time.

25. In the inspected systems, it was found that there were situations in which the bus of private places (masks) did not prevent their visualization, namely doors, windows and balconies.

26. Regarding one of the video surveillance systems, the CNPD was informed that the masks are manually configured by the system administrator, in each camera, in a maximum of 24 rectangles, which does not always cover all the private spaces to be hidden.

27. In the same system, the CNPD tested the option of activating/deactivating masks by the user, verifying that they are presented according to the commands given. But it found that these operations are not recorded in the log in an identifiable way, i.e., in addition to the aforementioned, not even the type of operation performed is included in the log (audit record), preventing any internal or external audit of the legitimacy of the operations.

28. Also in the same system, it was found the installation of software that, in order to be used, implies connection to the Internet, namely FaceBook, Netflix, Recipes, Skype, Royal Revolt2, Twitter, TuneIn radio, which constitutes an inconsistency in a system that must work on an isolated network. Regardless of other considerations, the mere existence and use of this type of software presents risk vectors (e.g. cookies, device fingerprinting, malicious code) that are unacceptable in a security forces video surveillance system.

29. In another system, Internet access software (TMN Broadband) was installed on the server and, in the same location, other Internet access software (Vodafone Mobile Broadband and MEO Mobile Broadband) were installed on the server. , which is a strong indication that the system was connected to the Internet, which represents yet another vulnerability for the system.

Av. D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

30. At a workstation, searching for “.jpg" and ".jpeg” on the disks, folder listings were obtained with images totaling more than 400 folders and more than 6000 files between frames and videos since the start of operation. system.

31. In summary, what is briefly described here reveals that the use of video surveillance systems does not comply with the rules regarding the security and integrity of the processing of personal data and that the PSP has not had de facto, but also legal, conditions for its use. in accordance with the legal and regulatory framework, not having, from the outset, the indispensable control over the equipment and its use.

32. Bearing this in mind, the option made in this Draft Law to expand and make video surveillance systems more complex with new technologies, seems to reveal the lack of knowledge of the reality that security forces and services face in their day to day in the context of use of video surveillance systems.

33. The text of the Draft Law is analyzed below, in order to highlight the deficiencies that the different rules reveal with regard to the processing of personal data.

ii. Scope of law enforcement and purposes of video surveillance systems

34. Article 2 of the Draft Law states that the provisions of it apply to "video surveillance systems installed or used in public spaces or in areas of the private domain intended for the public movement of people, vehicles, ships and boats, when duly authorized, and for the purposes set out in the following article”.

35. As for the purposes of video surveillance systems listed in Article 3 of the Proposal, they have doubled in relation to those currently defined in Article 2 of Law No. 1/2005. In fact, in addition to expanding the purpose of protecting and securing animals, and making the purpose of traffic control in road traffic autonomous (already provided for in article 13 of Law No. 1/2005), there are also the following: support for the operational activity of security forces and services in complex police operations, namely in large or international events or other high risk or threat operations; operational response to ongoing security incidents-, traffic control and safety of people, animals and goods in maritime and river navigation, as well as prevention and repression of infringements of existing regimes in terms of navigation and protection of the marine environment] circulation control of people at the borders; support in search and rescue operations.

The. The purposes of criminal prevention and repression vs the purposes of mere ordering

36. Not questioning the new purposes considered here, the CNPD cannot fail to point out that, as stated in the proem of the article, if the use of video surveillance systems is limited only "to the pursuit of the purposes provided for in the Internal Security Law, approved by Law No. 53/2008, of 29 August, in its current wording» [emphasis added], then it is not understandable that it lists traffic control (in road traffic and in maritime and river navigation) and the prevention and repression of road infractions and prevention and repression of infractions to the current regimes in terms of navigation (cf. subparagraphs g), h) and i) of article 3 of the Proposal), which clearly do not fit therein. It is therefore recommended to reconsider the list of purposes presented or the express reference to the purposes provided for in the Internal Security Law.

37. In this regard, it is also important to emphasize that, if the purpose of the Draft Law is to regulate the processing of personal data arising from the use of video surveillance systems in the public space (and in the private space accessible to the public) not only for purposes of criminal prevention and repression, but also for the prevention and repression of offenses of a strictly administrative nature, as well as traffic control and detection and protection against forest and rural fires, then this Proposal cannot be limited, as to the data processing, to references to Law No. 59/2019, of 8 August, which must also include references to the RGPD and to Law No. 58/2019, of 8 August - we refer to the constant references Article 2(2), Article 18(5), Article 19, Article 22(1) and (2) and Article 27 of the Proposal.

38. Furthermore, with regard to the purposes listed in article 3 of the Proposal, the substantial change in the wording of the paragraph on the purpose of protecting personnel, animals and property in public places or with public access is highlighted, since now the subparagraph d) expands the circumstances that allow for the need for protection to be asserted (in comparison with Law No. 1/2005). Thus, the following situations are listed: /'. High probability of occurrence of facts qualified by law as a crime; ii. High circulation or concentration of people; iii. Occurrence of fact susceptible of disturbance of public order.

39. However, it is doubtful that the mere fact that, in a given public place or with public access, there is high circulation or

concentration of people is, per se, sufficient to affirm the need to protect personnel, animals and property. It is not possible to see where the danger or serious threat to the integrity of people, animals or property is due to the situation thus characterized. Even because of the imprecision of the adjective "elevated", which does not allow us to understand whether exceptional situations of movement and concentration of people on the occasion of a certain event (e.g., the night of S. João in the city of Porto) or if the situations also fit normal and recurring patterns of movement of people on the streets of a populous city.

Social

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

40. Furthermore, within the scope of that same objective, the presupposition of a fact capable of disturbing public policy appears to be too broad. It cannot be any disturbance of public order that merits the use of means that can prove to be highly intrusive in the legal sphere of citizens who are in public space or even in private areas, even if accessible to the public. The restriction of fundamental rights, in particular the right to respect for private life, which the use of a video surveillance system implies, must be justified by the need to safeguard an important community interest or a fundamental right, and any interest of mere ordering is not enough. Social. This is the reason why video surveillance in public spaces, when it involves the processing of personal data, is at the service of criminal prevention and repression or the safeguarding of people's lives (and now animals) and, only in certain well-defined circumstances, can it serve the purposes of prevention and repression of illicit acts of mere social order - but here, even so, because human dimensions or values that are especially relevant in society are considered to be at stake.

41. Moreover, it is good to see that if the illicit act has already occurred, the use of the camera is not presented as an adequate means for the purpose of protecting people, animals and property, therefore, as may be stated in this purpose thus delimited

from the list of those that justify, in abstract, the installation and use of video surveillance systems.

42. It is not, therefore, nor can any disturbance of public order justify the use of video surveillance systems, nor any alleged feelings of insecurity. Therefore, the CNPD considers that the /'/' items should be eliminated. and subparagraph d) of article 3, as they extend the use of video surveillance to situations in which there is no effective need for protection, thus revealing a restrictive legislative measure of the fundamental rights to respect for private life and the protection of unnecessary and excessive personal data, in violation of paragraph 2 of article 18 of the Constitution of the Portuguese Republic (CRP).

43. Furthermore, it should also be noted that there are purposes described in terms that do not facilitate legal certainty and predictability as to their verification. This is the case of the purpose, provided for in subparagraph c) of article 3, of supporting the operational activity of security forces and services in complex police operations, the exemplification of which leads back to events of a broad or international dimension, it is not clear whether the The breadth of the event's dimension concerns the universe of people who compose it or simply the spatial area covered by it. Despite being a terminology that the legislator has already used in the Internal Security Law, the truth is that it is a vague concept, so it would be better if, instead of replicating it, it was densified. It is also worth noting that the purpose of operational response to ongoing security incidents, set out in

r

subparagraph f) of article 3, does not appear sufficiently dense to be autonomous in relation to the cases provided for in subparagraphs a) to d) of the same article 3.

B. Video surveillance of private properties

44. The CNPD also points out that some of the purposes set out in Article 3 of the Proposal imply or may imply the capture of images of private properties, which do not coincide with the concept used in Article 2 of the Proposal to define the scope of the respective application ("areas of the private domain intended for the public movement of people, vehicles, ships and boats"),

45. This is what happens, for example, for the purpose of controlling the movement of people at borders, provided for in paragraph j) of article 3 of the Proposal. Taking into account the extension of the Portuguese land border and the means that could be used to pursue this purpose (e.g., unmanned aircraft), serious doubts remain as to whether it is compatible with the

scope of application of the Draft Law or whether same be delimited to the areas where the border control posts are located. And, even so, taking into account that within the framework of the European project an area of freedom of movement was created, it is difficult to understand the purpose of controlling movement at internal borders as lawful. If the legislator here has only external borders in mind, he must therefore define that purpose, in order to remove any doubts as to a possible restriction of freedoms guaranteed in the European legal framework.

ç. Absence of delimitation of purposes according to the surveillance means used

46. In short, Article 3 multiplies the purposes of the processing of personal data associated with the use of video surveillance systems, in an effort to cover all the situations that until now would have justified such use. But as there are also multiple means that it presents for the execution of this video surveillance, it ends up enhancing or legitimizing the use of means that are not suitable for the pursuit of these purposes (or which, if they are, are, from the outset, excessive, given the their degree of intrusion into the private sphere of citizens).

47. It would be better to autonomously delimit the purposes that certain types of means - finally, the possibility of their use - can pursue, in particular with regard to unmanned aircraft (drones) and "cameras for use individual" (bodycams).

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

iii. Principles applicable to the use of video surveillance systems

48. Article 4 sets out the principles applicable to the use of video surveillance systems, which, strictly speaking, are reduced to the principle of proportionality in its different aspects, practically reproducing the provisions of article 7 of Law no. 1/2005.

49. Nevertheless, because the Draft Law substantially broadens the scope and means to be used in this context, there are provisions that must be carefully reconsidered.

50. It is immediately the case of the ban on installing fixed cameras in areas that, despite being located in public places, are by their nature intended to be used as guards - cf. Article 4(4) of the Proposal. In fact, the provisions therein are faulty in limiting the ban to fixed cameras, because, once the legislator seeks to legitimize the use of unmanned aircraft, it cannot fail to extend the same ban to technical solutions capable of producing (at least) the same impact on citizens' fundamental rights as the capture of images and sound via fixed cameras.

51. The CNPD therefore recommends reconsidering the wording of paragraph 4 of article 4 of the Proposal, insisting on the extension of this regime to the use of unmanned aircraft.

52. Still on article 4, it was appropriate to update or improve some of its rules. First of all, paragraph 5 of this article should be taken into account, which only safeguards the interior of an inhabited house or building or its dependence, when it is certain that the interior of hotel establishments or similar establishments, gyms, , and even office buildings, especially when it comes to individual use compartments (where people spend more time active - awake - than in their own home).

53. The CNPD therefore recommends updating the wording of paragraph 5 of article 4, extending the guarantee provided for therein also to the interior of other buildings where the same reason for protecting privacy is felt with similar intensity or nearby (e.g., hotels or similar establishments and offices).

iv. The legal regime of fixed cameras

The. Limitation of transparency

54. With regard to the legal regime for fixed cameras, provided for in Articles 5 et seq. of the Draft Law, we begin by noting the shortening of the period for issuing the CNPD's opinion and the prohibition of publication in the opinion of some elements concerning to the video surveillance system when critical infrastructures, sensitive points or facilities of interest for defense and security are involved.

55. The CNPD draws attention to the fact that some of the elements specified in paragraph 6 of article 5 of the Proposal must, under the terms of the law, be included in the authorization to be issued, which, in turn, is published in the Diário da República. This is specifically what happens with the identification of the place and area covered by the system and the technical

characteristics of the equipment used - cf. subparagraphs a) and d) of paragraph 1 of article 7 of the Proposal.

56. In this regard, the CNPD also emphasizes that the criticality of the infrastructure or the sensitivity of the points or facilities must be duly indicated in the request for an opinion, because this entity does not have the information to conclude by filling in such imprecise concepts, but it has It also has to be duly substantiated, so that the CNPD can, still in a logic of extrinsic control of evidence, confirm the verification of the assumptions of the legal imposition of concealment of information in the process of publicizing its opinions.

B. The indispensability of risk assessment in the authorization request instruction

57. With regard to the authorization request, it is underlined that it is essential, according to Law No. 59/2019, of 8 August, that it be accompanied by an impact assessment on the protection of personal data .

58. In fact, prior consultation with the CNPD, imposed within the scope of the authorization procedure, presupposes that such an obligation has already been fulfilled, pursuant to paragraph 1 of article 29 of Law No. 59/2019, of 8 of August1. It should be noted that the processing of personal data associated with the use of video surveillance systems is always considered to pose a high risk to the rights, freedoms and guarantees of individuals, as it concerns a large amount of personal data and affects a large number of data subjects. , as results from recital 51 of Directive (EU) 2016/680 of the European Parliament and of the Council, of 27 April, a directive that that law transposed into the Portuguese legal system - given that the provisions of this law cannot fail to be interpreted and applied in accordance with the Directive. Therefore, given that the data controller has the duty to carry out the impact assessment and the CNPD has the duty to issue an opinion on the processing of data, it seems logical that the former is an element to be added to the authorization request statement.

59. For this reason, the CNPD considers it essential that a new paragraph be added to paragraph 1 of article 6 of the Proposal, requiring that the request be accompanied by an impact assessment on the protection of personal data. And that paragraph 5 of article 18 of the Proposal be deleted, as it restricts an obligation imposed by the aforementioned Directive (we will return to this point). It is further recommended that the paragraph to be introduced in this

1 And in Article 35(3)(c) of the GDPR, regarding the processing of personal data that are regulated in Articles 12, 14 and 15 of the Draft Law.

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

paragraph 1 on such assessment is also specifically added to the list contained in paragraph 3 of article 10 of the draft law (regarding the ordering instruction concerning portable cameras).

ç. The restriction of the authorizing competence of the member of the Government

60. Also with regard to article 6, it is important to point out the absurdity of limiting the competence of the member of the Government responsible for the requesting security force or service to verifying the provisions of paragraphs 1, 2 and 3 of article 4 .° of the Draft Law - where the use of cameras is linked to the principle of proportionality, in terms of adequacy and necessity because compliance with the limits set out in paragraphs 4 to 6 of that article - relating to the specific respect for privacy - it also has to be verified by that body, as holder of authorizing power, since they are legal, negative presuppositions of authorization. And because the opinion of the CNPD, which has to focus on paragraphs 4 to 6 of article 4 (see paragraph 3 of article 5 of the Proposal), is a mere legal act of opinion, without force binding legal system, which serves to support the exercise of the authorizing authority of the member of the Government, therefore, serves to support the verification of compliance with these assumptions defined in article 4 - being especially relevant as it creates in the member of the Government the duty to state reasons if he decides in a different sense from the opinion (cf. article 151(1)(c) of the Code of Administrative Procedure).

61. The CNPD recommends, therefore, the reformulation of the provisions of paragraph 3 of article 6 of the Proposal, in the sense of not excluding from the competence of the member of the Government the verification of the assumptions provided for in paragraphs 4 to 6 of article 4, even with the support of the opinion of the CNPD.

d. Reduction of deadlines

62. One last note, now on deadlines, especially on the duration of the authorization. In article 7, the novelty of setting a maximum period of 5 years is highlighted (as opposed to the 2-year period of Law No. 1/2005), which represents a substantial

extension of the same.

63. It is important here to consider, from the outset, which criteria may be the basis for the forecast of a maximum period of 5 years, more than double the current one, given that the Explanatory Memorandum is regarding such omission. It should be noted that the period of 2 years, currently in force, changed the period initially provided for in Law No. 1/2005, which was 1 year.

64. It is recalled that this legislation was based on the assumption that both fixed and mobile cameras would be used to meet specific and exceptional situations that required video surveillance for a specific event or to deal with a certain phenomenon. If the extension to 2 years was a first sign of simplifying the verification of such circumstances, the setting of a period of 5 years reveals the abandonment of any judgment of exceptionality or temporally delimited necessity of the

video surveillance. It therefore means the assumption that video surveillance systems must exist regardless of the demonstration of their need, suffice it with an initial judgment (sometimes summary) on the proportionality of their use, disregarding the interference in the private life of the people who such means.

65. Furthermore, this period jeopardizes the timely reassessment of the need to use video surveillance systems, also taking into account that, due to technological developments, the technical equipment and security measures adopted may, over such an extended period, become markedly obsolete.

66. For all these reasons, the CNPD recommends reconsidering the maximum period set out in Article 7 of the Draft Law, as it does not find reasons to support it, or in view of the essential requirement of regular reassessment of the adequacy, necessity and proportionality of the use of video surveillance systems, or in view of the tendency to obsolescence of the systems in such a long period of time.

67. At the same time, it should also be considered whether the period of 30 days before the expiry of the authorization for renewal of the application is not insufficient to guarantee the prior consultation of the CNPD whenever the renewal request incorporates changes in relation to the initial authorization, in particular considering the period - also 30 days - that the CNPD

has for issuing its opinion.

68. It is therefore recommended that the deadlines set out in paragraphs 3 and 4 of article 7 of the Draft Law be reconsidered.

v. Exceptional and special regimes

The. The installation or use of cameras without the prior authorization of the member of the Government

69. Article 9 exempts from the need to obtain prior authorization for the installation of fixed cameras, by decision of the top leader of the security force or service, when there are duly substantiated urgent circumstances that constitute a danger to the defense of the State. or for security and public order.

70. A similar exception is provided for in paragraph 5 of article 10, regarding the use of portable cameras, although here the respective legal requirements are relaxed, with the formula 'when it is not possible to obtain authorization in good time [...]».

71. In both cases, it is necessary to obtain the authorization ex post, prescribing the duty to destroy the recorded material in case the authorization is not issued.

72. This exceptional regime was provided for in Law No. 1/2005, but only for the use of portable cameras (cf. Article 6 of that law).

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

73. It should be noted that, in comparison with the provisions of Article 6(3) of Law No. 1/2005, which requires the destruction of recorded material also in the event that, within the scope of the subsequent authorization procedure, the CNPD issues a negative opinion, in this draft law the opinion of the CNPD is no longer binding. There are, therefore, many changes introduced in the exceptional procedure for the use of portable cameras without prior authorization, in order to streamline the procedure and reduce the impact of the prior consultation of the CNPD. This cannot fail to be apprehensive, especially since this regime

of portable cameras also covers the processing of data made using cameras incorporated in unmanned aircraft (aka, drones), as will be discussed below.

74. In any case, what is at issue is the use of fixed or portable cameras in which the prior control of the member of the Government is dispensed with, and the decision of the top leader of the security force is sufficient, based on particularly imprecise assumptions. . Experience shows that urgent circumstances or the impossibility of obtaining authorization in good time end up referring to events scheduled well in advance, in relation to which the need for surveillance is foreseeable from an early age, only occasionally invoking supervening facts revealing the need the use of video surveillance (e.g., festivities in public spaces on New Year's Eve, carnival processions, football matches, international summits or similar events, such as the Web Summit).

75. The lack of prior control and the weakening of a posteriori control, on the one hand, and the imprecision of the assumptions for the use of these exceptional procedures, where there is no express reference to the need to use video surveillance, cannot fail to cause concern as to the to the concrete application of these legal precepts.

B. The use of portable cameras, especially drones

(i) Exclusion of prior consultation with the CNPD

76. As for the procedure for authorizing the use of portable cameras, regulated in Article 10, it is important to note, from the outset, that nowhere in that article refers to the authorization regime provided for in Article 5 of the Proposal (but already contains a partial reference to Article 6, concerning the elements that must support the application). Such omission allows the interpretation that the opinion of the CNPD is not necessary here.

77. However, the CNPD draws attention to the fact that it is precisely the use of this type of camera that has revealed the greatest difficulties in complying with the regulatory requirements (currently in force) that aim to guarantee the security of the video surveillance system and the integrity , confidentiality and auditability of the

processing of personal data resulting from its use2. For this reason, the law must, for the avoidance of doubt, explain the need in this type of procedure for obtaining a prior opinion from the CNPD in paragraph 1 of article 10, by express reference to such

prior consultation or by reference to Article 5 of the Draft Law.

78. Otherwise, and in the absence of prior verification by those with specialized knowledge and experience in this matter, with the aggravating factor that the use of unmanned aircraft (idrones) may be involved, there is a serious risk of not being considered in the authorization process eventual insufficiencies of the video surveillance system to be able to fulfill the intended purposes with its use or aspects of the treatment that imply the unlawful restriction of the privacy of the citizens.

(ii) Lack of elements necessary for the authorization decision

79. It should be noted that the selection of elements that must be included in the request for authorization of the use of portable cameras, contained in paragraph 3 of article 10 of the Proposal, has not yet been achieved. In fact, with the exception of the rules contained in subparagraphs a) and c) - although the provisions of subparagraph a) must be applicable with the necessary adaptations, because this type of request must be accompanied by a specific justification regarding the suitability and necessity of its use -, it is not achieved because the procedure for informing the public, the identification of the biometric data subject to collection and the mechanisms to ensure the correct use of the registered data are excluded (cf. paragraphs f), h) and i) of Article 6(1) of the Proposal).

80. We insist: the use of portable cameras, not only regarding the collection of images and sound, but also regarding the conditions of their transmission and subsequent treatment, requires special attention with regard to the confidentiality, integrity and auditability of the treatment . In addition, if portable cameras are attached to unmanned aircraft, special public information duties are warranted. It is, therefore, inexplicable and inadmissible not to refer to the aforementioned instructional elements, and the CNPD recommends that such a gap be integrated, in the terms set out above.

(iii) Absence of regulation of the use of drones

81. Finally, attention is focused on Article 10(2) of the Proposal, which provides for the use of portable cameras through any means of portability, with a special focus on the use of unmanned aircraft (drones).

2 Cf. the opinions of the CNPD, available at: Opinion/2021/141, of October 29, Opinion/2021/51, of April 27, Opinion/2020/139, of November 19, Opinion/2020/41, of 1 of April, available at https://www.cnnd.pt/decisoes/historico-de-decisoes/?vear=2021&tvoe=4&ent= and https://www.cnpd.Dt/decisoes/historico-de-decisoes/?vear =2020&tvpe=4&ent=

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

82. The simplified, one might even say simplistic, way in which the use of unmanned aircraft is provided for in the Draft Law cannot fail to be surprising. As if the mere legislative attestation of the general possibility of its use was sufficient to fulfill the role of the law of guiding the conduct of public entities, and specifically, of the security forces, and the function of predictability that a restrictive law of rights, freedoms and guarantees always have to guarantee the holders of these rights.

83. There are no specific conditions or limits for the use of portable cameras when incorporated into drones, as if the impact on the private life of a camera carried by an agent that circulates on a street or carried in a vessel on the high seas, and a camera that flies over a certain altitude, and with no or very little perception of this fact by passers-by, the streets of a city, beaches, public gardens and, perhaps, private gardens and terraces . In fact, with the ability to fly on a level plane with buildings, capturing images of the interior of buildings, which can be dwellings.

84. And yet, in the explanatory memorandum of the proposed law, one can read the intention to «[...] accommodate the use of cameras incorporated in unmanned aircraft systems [...] by the forces and services of security, in their daily activity" (italics added), which clearly shows that the purpose of this draft law is to popularize or generalize the use of drones to monitor citizens, without limiting their use to specific purposes and regardless of their effectiveness. suitability and necessity, secondary to the impact on fundamental rights resulting from its use.

85. One cannot resist transcribing here recital 33 of Directive (EU) 2016/680, of 27 April, which Law No. 59/2019, of 8 August transposes, where it can be read, as to the legal basis or the national legislative measure to which the directive itself refers, that these “[...] must be clear and precise, and their application must be foreseeable for individuals, as required by the case law of the Court of Justice and the European Court of Rights Man. The law of the Member States governing the processing of personal data within the scope of this Directive should specify at least the purposes, the personal data to be processed, the

purposes of the processing and the procedures aimed at preserving the integrity and confidentiality of the data. personal data, as well as the procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness'. As can easily be seen, this diploma, regarding the use of drones, clearly does not meet this requirement of legislative density and predictability, remembering that, under the terms of the Portuguese Constitution (cf. article 18 and paragraph b) of no. Article 165(1) of the CRP), these rules and guarantees must be defined at the legislative level and not at the regulatory level.

0

86. The CNPD therefore considers it essential that this law regulates the use of cameras incorporated or coupled to unmanned aircraft in terms that guarantee that, unless authorized by the judge in the context of a criminal proceeding, images and sound of the inside buildings, balconies, terraces, gardens and any other spaces in the private domain. As for public spaces and public access, the indispensability of guaranteeing that the restriction of fundamental rights, in particular the right to respect for private and family life, is appropriate, necessary and not excessive in relation to the purpose pursued in the specific case, specifying if in the legal diploma the specific purposes that can justify its use. It should not be forgotten that article 3, as it is written, encompasses purposes of different relevance, since, alongside the prevention and repression of criminal offenses, the protection of secondary goods is also allowed, the aggression of which constitutes an offense of mere social order. It is therefore imperative that the law reflects the balance between the legal interests in tension, only legitimizing interference in private life with the intensity that drones potentiate if the threatened or injured legal interests deserve the reinforced protection of criminal legislation.

87. The CNPD also stresses that it is essential to impose the adoption of adequate forms of compliance with the duty to inform the public, as provided for in article 14 of Law no. , at points 145 to 148.

88. Furthermore, it is essential to define the conditions for the collection, transmission and use of the captured images and sound, precisely in order to prevent the risk of external interference, of manipulation of the captured images and sound, thus guaranteeing the integrity, confidentiality and, in particular, the auditability of the processing of these data. The regulation of these aspects of data processing in more specific and technical terms can be done at the regulatory level, but it is up to the law

to provide for this referral or delegation, while reserving for itself which safeguards apply to the defense of rights, freedoms and guarantees, the which Article 10 of the Draft Law clearly does not.

89. Otherwise, the mere general provision of the use of portable cameras in drones, in paragraph 2 of article 10, without providing for conditions that demonstrate the need for such use, nor measures that reveal the weighting and safeguard the impact differentiated and more intense processing of data in the legal sphere of citizens, implies a disproportionate restriction of fundamental rights to respect for private and family life and the protection of personal data, in violation of Article 18(2) of the CRP.

Av. 0. Carlos 1,134, Io

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

ç. Using body cams

90. It is now important to consider the use of portable cameras for individual use, regulated in Article 11 of the Draft Law, for the purposes of recording the individual intervention of an agent of the security forces in police action (cf. no. 1).

91. The use of a video camera by each agent of the security forces and services poses the specific challenge of reconciling the protection of the privacy of the agents themselves and of all the citizens they come across in the exercise of "police action" with the protection of of the interest that its use aims to protect. It is true that this interest is not made explicit, and it seems that the agent's individual intervention is registered as an end in itself. In fact, this prediction will be based on recent cases in which the conduct of agents was recorded by citizens through their cell phones and smartphones and disseminated on social networks, which generates the conviction that agents must be equipped with similar tools that give them allow you to demonstrate your version of the same event.

92. Understanding this interest - which will correspond to the collection of evidence relating to the conduct of agents and

citizens who interact with them -, however, it is still necessary to safeguard the rights and freedoms of citizens and, from the outset, to ensure that the regime defined in Article 11 is capable of achieving the objective pursued. Let's see.

93. The solution enshrined in the Draft Law makes the use of the chamber dependent on the authorization of the respective top manager, and information is provided to the member of the Government responsible for the security force (cf. paragraph 1 of article 11 of the Proposal).). This first provision is not, from the CNPD's point of view, clear as to the purpose and scope of the authorization: if in question is the authorization to place the camera on the agent's uniform or equipment whenever he goes into police action (and subsequent information from the member of the Government), or if it is the first time that an agent is assigned a chamber for such purposes. The CNPD therefore recommends its clarification.

94. As for the assumption that underlies the possibility of activating the camera, and subsequent capture and recording of images and sound, paragraph 3 of article 11 of the Proposal states that it is "in case of intervention by an element of the security forces" , an assumption that is then exemplified with various circumstances, characterized through imprecise concepts. Not making the precept explicit who makes the decision to activate the camera, seems to be the security forces agent and, therefore, the law is attributing to him a discretionary power to turn on the camera when one of those circumstances occurs (which are, repeats themselves, merely illustrative).

95. Now, if it is understood that this discretionary power of decision, thus delimited, regarding the activation of the camera limits the impact that a camera recording image and sound during the entire shift of the agent would have on the private life of the agent himself and everyone citizens who could cross paths with it, the truth is that the solution found does not seem suitable for fulfilling the intended purpose.

96. In fact, the first aspect of the principle of proportionality seems to fail here: this measure, defined in this way, leaves the agent with the option of activating or not activating the chamber, even when it is 'in intervention', and leaves it with the power to conclude if it is a situation that legitimizes its activation. In other words, the solution found here does not take into account the

risk or probability that the agent does not want part or all of his action to be captured and recorded, being of doubtful use for the purpose of proving his intervention. From the outset, it is not determined whether the images and sound are transmitted in real time, or if they are recorded on the equipment in the agent's possession and, therefore, if there is a risk of manipulation or elimination of the recordings. In fact, in the terms in which it is thought, the use of these cameras does not seem to be suitable or suitable for fulfilling the purpose, stated in paragraph 1, of 'recording the individual intervention of an agent of the security forces in police action'.

97. In addition to these two aspects, the article is only concerned with ensuring the transparency of this processing of personal data - referring to a sign indicating the purpose of its use (which, it is reiterated, was explained in the law as "registration of individual intervention of an agent of the security forces in police action») - and a verbal warning, it is assumed, that the recording will be started «whenever the nature of the service and the circumstances allow» (cf. n. 2 and 3, in fine).

98. However, the article stops at this point, regulating nothing else; it was decided to refer the definition of the «characteristics and rules of use of the cameras [...], as well as the form of transmission, storage and access to the collected data» to the government decree.

99. And here lies the CNPD's second main concern. In addition to the lack of adequacy of data processing for the intended purpose, if this were to be surpassed, there would still be a need to provide for rules regarding the moment in which the capture and recording of images and sound must cease, as well as the possibility of being issued. a higher order of recording of the intervention, and that prevent the risks of deletion, manipulation or dissemination of the recorded material. Rules that, from the perspective of the CNPD, must be defined in a legislative framework, precisely because they serve to guarantee the fundamental rights of citizens.

100. Otherwise, we will have the provision of yet another processing of personal data that implies the restriction of fundamental rights of citizens, without this being accompanied, at least, by the imposition of adequate guarantees to protect the rights and interests of all citizens , which also includes the agents of the security forces themselves.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

101. In short, as it is not able to pursue the intended purpose, the legal provision for the use of cameras for individual use, as written in article 11, violates the first manifestation of the principle of proportionality, in contradiction with the provisions of paragraph 2 of article 18 of the CRP.

d. Other special regimes

102. As for the maritime and river navigation surveillance systems, regulated in article 14 of the Proposal, attention is drawn to the need for their installation to ensure that images of private properties are not captured, and should also provide for measures are taken that, while ensuring the intended purpose, eliminate or reduce to the bare minimum the impact on people's privacy in public spaces where people are more exposed, as in the context of the use of sea and river beaches.

103. The CNPD also recommends that a note be specified regarding the need, in all special procedures regulated herein, to comply with the procedure provided for in article 5 of the Draft Law, which includes prior consultation with the CNPD. This observation is related to the fact that in article 15 of the Proposal, concerning fire surveillance and detection systems, when consultation with the National Emergency and Civil Protection Authority is required, the opinion of the CNPD is expressly referred to. However, when the need to consult the CNPD is made explicit (wording that is already found in Law no. if other surveillance systems are specifically regulated (12th and 14th), it is possible to interpret that this consultative procedure would be dispensed with in these cases.

104. If, prima facie, this does not appear to be the ratio legis, nor is there an objective and reasonable basis for rejecting the instruction of the procedure with an opinion of the administrative authority that has powers of prior (today, essentially advisory) and successive supervision with regard to the protection of personal data, the CNPD takes the liberty of insisting on the need to clarify this duty of prior consultation.

saw. A new special image capture regime

105. Within the scope of chapter IV, entitled Access to other video surveillance systems, article 17 of the Proposal appears,

under the heading Capture of images without recording, providing for the possibility of capturing images, using fixed or portable cameras , exclusively for real-time viewing.

0

PAR/2021/103 11

CNPD

National Data Protection Commission

106. It should be noted, in the first place, that this rule, as it is written, does not correspond to access to video surveillance systems, but rather to a specific use of such systems, so it is recommended to reconsider its systematic insertion in this chapter, or change its name.

107. More important, however, is the substantive regime established here. The use of fixed or portable cameras for viewing images is permitted provided that the purposes set out in subparagraphs c), e), f) and l) of article 3 are at stake, which seem to relate, roughly, to interventions operations of the security forces.

108. However, firstly, as regards the use of fixed cameras in this context, it is not possible to achieve any degree of autonomy in relation to the regimes for the installation and use of fixed cameras regulated in Articles 5 to 9 of the Proposal. In fact, if the cameras are already installed, then it is always possible to use them just for viewing. If, on the other hand, access to third-party video surveillance systems is intended here, then the rule must expressly say so, for reasons of legal certainty. But this raises another question - which will be analyzed below (see below, points 116 to 119) - and which concerns remote access to such systems.

109. With regard to the use of portable cameras for viewing, the CNPD does not understand why this use is not regulated in Article 10 of the Proposal, or in any case in Chapter III on special regimes, here a simplified procedure is foreseen, depending solely on the authorization of the top leader of the security forces and services.

110. It is recalled that real-time visualization can include (and it would be said to include here, to be of some use) the transmission of images for visualization in a command and control center, which implies the need to adopt measures of security regarding the transmission process, which, in itself, already implies data processing. And, as then, in paragraph 2 of article 17, the possibility of recording is foreseen, then it is essential to legally impose special measures that guarantee the security, confidentiality and integrity of the treatment, as well as its auditability, as in any other processing of personal data

resulting from the use of portable cameras.

111. However, it should be noted that the provisions of article 17 also cover the use of drones (or unmanned aircraft), which means the possibility that, only by determination of the top leader of the security forces and services, the use of portable cameras incorporated in drones. And this possibility is stated in this way, to be implemented in a simplified decision-making procedure, without any densification of conditions or material limits for making such a decision.

112. The CNPD insists that this type of rules, merely illustrating the possibility of using equipment with an enormous intrusive potential in private and family life, without defining any

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

guarantees the fundamental rights of citizens, does not comply with the most basic requirements of the Rule of Law, relying exclusively on the affirmation of a public (or private) interest as a greater good, without being previously obliged to undergo a rigorous process of weighing the adequacy, necessity and proportionality (in the sense of non-excessiveness) of the use of that type of equipment. And without requiring the adoption of measures that mitigate the evident impact that this use has on the private life of citizens. We refer, therefore, to the recommendations and conclusions left above, in points 86 to 89, in view of the evident unconstitutionality of a legal norm with this restrictive scope of rights, freedoms and guarantees, for not delimiting the restriction and, therefore, it thus presents itself, without further presuppositions, as unnecessary or, at least, excessive, in clear violation of paragraph 2 of article 18 of the CRP.

vii. Remote access to video surveillance systems of public or private entities

113. In the aforementioned chapter IV, article 16 of the Proposal regulates access to video surveillance systems of any public

or private entity, installed in public or private places with public access, for the purposes set out in article 3. ° of the Proposal.

114. In this regard, the CNPD makes two observations. The first, to point out that, according to the Explanatory Memorandum, through the Proposal "the special regimes are clarified and the procedures related to the use, by security forces and services, of video surveillance systems created by the municipalities, as well as access to private video surveillance systems installed in public or private places with public access', when strictly speaking the provisions of article 16 do not clarify or strengthen the access that was already provided for in paragraph 7 of article 31 of Law No. 34/2013, of 16 May, amended by Law No. 46/2019, of 8 July (which sets the legal regime for private security). And that, for video surveillance systems in restaurant and beverage spaces with spaces or rooms intended for dancing, paragraph 5 of article 5 of Decree-Law no. 35/2019, of 24 May, already provides for the viewing of images in real time at the command and control centre.

115. Therefore, it is not envisaged that densification will be carried out here, in addition to extending this possibility to all video surveillance systems of any public or private entity, installed in public or private places with public access.

116. The CNPD has already commented on this matter regarding the legal amendments of 201 93, maintaining the need to establish that the possibility of remote access must be contextualized, through the

3 Cf. Opinion 52/2018 and Opinion 53/2018, both of November 13, accessible at https://www.cnpd.pt/decisoes/historico-de-deçis,Qes/?year=2mS.tya£541e.nt=0

demonstration of its suitability and necessity for a specific purpose - which appears to exist, prima facie, in relation to establishments where, in legal terms, there must be a video surveillance system (e.g. goldsmiths, banks) - and drawing attention to the risks that remote access may result in for the video surveillance systems of public and private entities, when remote access is not carried out through a secure channel. The risks are not only related to the security of such systems, as they may potentially potentiate improper access, deletion and manipulation of images by third parties, but also, as a consequence, those related to privacy that will result from the dissemination and manipulation of images by third parties.

117. Furthermore, in addition to not seeing that this rule results, without further ado, in a duty of all these entities to create a safe channel - and, therefore, such a duty would fall on the security forces -, it is not possible to see which channel could be created that guarantees secure access to all video surveillance systems covered here.

118. Furthermore, it remains unclear at what level - centralized at national level, or rather delimited at local level - access to such systems takes place.

119. The CNPD therefore considers that the provision for the possibility of remote access must be reconsidered and, if it remains the final one, it must be accompanied by the imposition of adoption of measures that mitigate the resulting risks.

viii. Use of Artificial Intelligence technologies and treatment of biometric data

120. Chapter VI of the Draft Law, under the heading Data Processing, brings important novelties to the video surveillance regime in public space and also in the private space with public access, insofar as this is also covered by the scope of application of the Proposal of Law.

The. Artificial intelligence

121. In fact, it is accepted in paragraph 1 of article 18 that the visualization and processing of data may be based on an analytical management system of captured data, by applying technical criteria according to the purposes for which systems are intended.

122. Once again, the generic forecast of the use of technology that implies an impact on the legal-fundamental sphere of citizens of different intensity, depending on the type of data analytics tool to be used, proves to be manifestly insufficient for the law to comply with the its function of guiding the security forces and services regarding this use is, objectively, insufficient to allow citizens to understand under what conditions it will be used and what impact it may have on their fundamental rights. From the outset, without realizing whether these tools can be used for any of the purposes provided for in article 3 of the Proposal, therefore, also for the purposes of protecting interests of mere social order.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

v.

í

B. Covert prediction of facial recognition technology

123. And if this mere generic provision is added to the permission, in the following paragraph of the same article 18, of the processing of biometric data, then we have a legislative norm that, in this subtle and hidden way, opens the door to the incorporation of technology of facial recognition in video surveillance systems in public spaces. Furthermore, as mentioned above, given the scope of application of the Draft Law, defined in its article 2, such incorporation will also be possible in video surveillance systems in a private space with access to the public, if in paragraph 1 of article 18° its scope is not restricted.

124. The covert prediction of the use of facial recognition technology is confirmed later in the article. In fact, Article 18(4) leaves no doubt as to what is meant by capturing biometric data: it is not just about capturing the person's image, and analyzing biometric data {e.g., the gait), but creating a biometric template of your face.

125. The fact that the national legislator, in this Proposal, incorporates in the same article the permission to use data analytics technology and the permission to process biometric data, without expressly stating the permission to use facial recognition technology, does not it is no longer surprising, when in a democratic State governed by the rule of law, restrictions on rights, freedoms and guarantees must be clearly and definitively determined by law.

126. The CNPD does not know whether the national legislator is aware of the real consequences of the use of this type of technology in video surveillance systems in public spaces and in private spaces with public access. It is, in fact, giving the green light to mass surveillance by security forces and services, denying any dimension of privacy that might still remain in the public space (and in the private space open to the public). It allows the tracking of citizens, boosted by the possibility of linking the information available in the video surveillance systems of public and private establishments and other private spaces open to the public, in addition to the use in the daily activity of the security forces and services of portable cameras as well. through the use of drones.

127. The impact that such control can have on any democratic society is evident, due to the ease with which this tool is used

as a means of repressing freedom of expression, demonstration and assembly, as recent examples in other parts of the world have demonstrated.

128. It is certainly not necessary to recall here the jurisprudence of the Constitutional Court and the jurisprudence of the European Court of Human Rights, or even the Court of Justice of the European Union, all of which affirm a right to respect for private life in the public space. Jurisprudence that has insisted on the indispensability of, in a democratic State of Law, the law precisely delimiting the restrictions on the rights

and liberties of citizens, when they prove adequate to pursue certain fundamental public values, under penalty of having such restrictions as disproportionate or even as affecting the essential content of these rights.

129. However, Article 18 of the Proposal is absolutely devoid of conditions and criteria for the use of data analytics technologies and, in particular, facial recognition. It confines itself to referring in paragraph 1 to the application of technical criteria according to the purposes for which the systems are intended. Not even specifying who defines such criteria.

130. It is also worth recalling that the European Parliament's Motion for a Resolution on artificial intelligence in criminal law and its use by police and judicial authorities in criminal cases «[d]escores that the use of biometric data is more broadly related to the principle of the right to human dignity, which forms the basis of all fundamental rights guaranteed by the Charter; Considers that the use and collection of any biometric data for remote identification purposes, for example through facial recognition in public spaces, as well as at automated border control barriers used in border control at airports, may pose specific risks for fundamental rights, the implications of which can vary considerably depending on the purpose, context and scope of use; also highlights the disputed scientific validity of recognition technology, in particular cameras that detect eye movements and changes in pupil size, in a police context; believes that the use of biometric identification in law enforcement and judicial contexts should always be considered “high risk” and therefore subject to additional requirements, in line with the recommendations of the Commission’s High Level Expert Group on AI”4.

131. And even though, at the end of the Explanatory Memorandum of the Proposal for a Resolution, it reads: “Finally, the rapporteur requests a moratorium on the implementation of facial recognition systems for police purposes. The state of advancement of these technologies and their important impact on fundamental rights require a deep and open debate in society, in order to examine the different questions that arise and the justification for their implementation» (italics added), which is well sign that the option of using this technology in public space for police purposes is not yet mature enough.

132. Furthermore, there are many studies showing that the use of facial recognition technology in video surveillance systems generates high rates of false positives in the identification of people. In particular,

4 Cf. § 30 of the Proposed Resolution, accessible at https://www.euronarl.euroDa.eu/doceo/document/A-9-2021-0232 PT.html#title6

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

when the images are of people with a specific ethnic or racial origin, in particular women5 6. However, given such error rates and especially with the relevance of ethnic or racial origin in their promotion, the risk of discrimination is too much to be taken lightly in our legislation.

ç. Technical and legal inconsistencies in the wording of article 18

133. Without prejudice to all that has been said, the regime provided for in Article 18 will now be analyzed, in order to highlight its different inconsistencies and shortcomings.

134. First of all, Article 18(1) chooses to differentiate between visualization and data processing, for the purpose of applying data analytics technology, when the actual transmission of data for the purpose of visualization and further analysis, on the central server, always involves a data processing operation; so, right here, the reference to the visualization process would lose meaning. But the incongruity thickens when one understands that the application of that technology cannot occur in a

simple process of mere visualization.

135. Next, Article 18(2) and (3) are provisions that are difficult to interpret and articulate. Biometric data, in the sense given in paragraph 4 of the same article, cannot be captured - therefore, for the purpose or through the creation of a template -, without such data being subject to the necessary treatment for the creation of the biometric template, so talking about capture in paragraph 2 and processing these same data in paragraph 3 is completely devoid of logic and reveals little technical rigor.

136. Therefore, what seems to be foreseen is the processing of biometric data of all those who are or circulate in public space or in spaces open to the public - in a logic of mass collection

5 Cf. Leslie, D. (2020). Understanding bias in facial recognition technologies: an explainer. The Alan Turing Institute, in https://doi.Org/10.5281 /zenodo.4050457. and Joy Buolamwini / Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research 81:1-15, 2018, in http://proceedings.mlr.press/v81/buolannwinn8a/buolamwini18a.pdf

6 Cf, Peter N. Schuetz, Fly in the Face of Bias: Algorithmic Bias in Law Enforcemenfs Facial Recognition Technology and the Need for an Adaptive Legal Framework, 39(1) LAW & INEQ. (2021), accessible at http://scholarship.law.umn.edu/cQÍ/viewcontent.cai?article=1656&context=lawineQ.and especially the reference made there to a study carried out in July 2018 by American Civil Liberties Union (ACLU), within which it ran Amazon's Recognition software, advertised as offering "highly accurate facial analysis, face comparison, and face search capabilities', on photographs of members of the 115th Congress of the United States of America and compared it with a public database of 25,000 photographs of prisoners; although none of the congressmen was among this universe of prisoners, the software presented the result of 28 matches, after which it was verified that the error concerns a number disproportionate number of African-American congressmen.

of biometric data. But the standard does not define what, in this context, would be crucial: whether biometric data will be included in a centralized database and who will be responsible for such an information system.

137. Furthermore, on this basis, it is not clear whether paragraph 3 is intended to limit access to that database for the purpose of preventing terrorist acts, in which case access depends on a judicial authorization, which is presumed, although the legislator does not say so, it occurs in a specific judicial process, or if, with the same paragraph 3, it is intended to make access to such biometric data subject to a judicial authorization only when the purpose of preventing terrorist acts is at stake . Which would mean that, for the other purposes of Article 3, it would still be possible to access such a biometric database - many of which, as mentioned, do not even concern criminal prevention and repression.

138. Finally, this article ends with a provision that, by limiting the performance of impact assessments to cases of use of artificial intelligence technologies, restricts the scope of the obligation under EU law to carry out an impact assessment. Such an obligation is provided for in the RGPD (cf. subparagraph c) of paragraph 3 of article 35) when the video surveillance systems regulated in articles 12, 14 and 15 of the draft law are at stake, and, as regards the use of systems for the other purposes provided for in Article 3 of the Proposal, also in Article 27 of Directive (EU) 2016/680, which provides for the obligation of Member States to bind controllers to the carrying out the impact assessment on the protection of personal data, read in the light of recital 51, in fine (where processing involving a large amount of personal data and affecting a large number of data subjects).

139. In this sense, paragraph 5 of article 18 of the Proposal should be deleted, as it restricts an obligation imposed by the GDPR and the aforementioned Directive.

140. In short, Article 18 of the Proposal provides for a mass surveillance system using generic data analytics and facial recognition technologies, which represents a restriction of citizens' fundamental rights, without complying with the dictates of the State. of Law, not even with regard to the essential clarity and transparency regarding the provision of these restrictions, and without providing for any guarantees of those rights, and for this reason it proves to violate the requirements set out in paragraphs 2 and 3 of article 18 of the CRP, being liable to affect the essential content of the right to respect for privacy and manifestly infringes the principle of proportionality.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

ix. Responsibility for the processing of personal data and subcontracting relationships

141. With regard to article 19 of the draft law, the CNPD would like to highlight the importance of providing in this article that any subcontracting of installation and maintenance services for video surveillance systems or the supply of software to be incorporated in them must comply with the provisions of article 23 of Law no. . of the Proposal).

142. And this point is stressed because, in its activity of monitoring the processing of personal data carried out by the security forces in the context of the use of video surveillance systems, the CNPD has noted the lack of means and adequate training of the security forces to precisely determine the operations to be carried out and monitor their execution (cf. above, points 14 to 30).

x. Recording procedures

143. In relation to Articles 20 and 21 of the Proposal, it is important to clarify what seems to be the legislative option of providing that the images extracted for submission to the Public Prosecutor's Office must be kept beyond the elimination period provided for in paragraph Article 21.1. In the latter case, the deadline for its elimination must be determined and, if this is not a certain deadline, a procedure must be foreseen - under the responsibility of the Public Prosecutor - of notifying the person responsible for the treatment of the moment from which it must proceed. up to its elimination.

144. Also with regard to article 21, it is recommended that the wording of paragraph 4 be corrected, as the expression 'the code [...] is in charge [...]' is not appropriate. Therefore, it is suggested to replace it with the indication that the encryption code or key must be known exclusively to the data controller.

xi. Lack of transparency in the use of portable cameras, including in drones

145. One cannot fail to look with concern at Chapter VII, since Articles 24 and 25 only concern the provision of information regarding the installation of fixed cameras, having opted for a total absence of disclosure the use of portable cameras.

146. The CNPD underlines that article 13 of Directive 2016/680 (and article 14 of Law no. 59/2019, of 8 August) grants data subjects the right to information on the processing of personal data, the CNPD having doubts that all processing of personal data carried out using portable cameras is covered by the exceptions provided for therein.

147. The CNPD recommends, therefore, that consideration be given to extending the provisions of Articles 24 and 25 of the Proposal to portable cameras, especially when their use in areas or because of well-defined events is at stake, and especially when they are incorporated in unmanned aircraft (drones), where the demands of publicity are placed with greater intensity, because the citizens may not be aware of them.

148. It further recommends that article 24 be updated in light of the provisions of paragraph 2 of article 13 of the aforementioned Directive - and regarding the treatments carried out in the context of the systems provided for in articles 12, 14 and 15 of the Proposal, in view of the provisions of article 13 of the RGPD -, under penalty of national law being in disagreement with such regimes. Eventually, with the definition of other instruments for the dissemination of this added information, such as, for example, on the website of the security forces and services.

xii. Restriction of the CNPD's prior and successive supervisory powers

149. Finally, in addition to the aforementioned restrictions resulting from the elimination of the CNPD's intervention in the context of prior consultation in the exceptional procedures of article 9 of the Proposal and of the special procedures regarding the use of portable cameras (articles 10 and 17. 2 of the Proposal), also when incorporated in drones, it is important to highlight here two apparent restrictions on the powers of the CNPD arising from the provisions of paragraph 2 of article 23 and paragraph 2 of article 26 of the Proposal.

150. Article 23(2) gives the General Inspectorate of Internal Administration (IGAI) the power to issue recommendations aimed at improving procedures for collecting and processing personal data, through video surveillance systems.

151. Since the CNPD has no objection to the IGAI issuing recommendations on this matter, it nevertheless notes that, both

under Article 57(1)(d) of the GDPR, as to the treatment of personal data regulated in the Proposal that are subject to it, as per Article 46(1)(d) of Directive (EU) 2016/680, which Law No. 59/2019 of 8 of August, transposed the (cf. article 44.º), it is up to the CNPD to give guidance to those responsible for the treatments on their obligations, and this function cannot be pinched by the Portuguese legislator as long as the CNPD is considered by national law to be the national authority of data protection also in this area of public activity.

152. Thus, the CNPD suggests that the provision in paragraph 2 of article 23 be added to the proviso without prejudice to the attributions and powers of the CNPD.

153. Also the wording of paragraph 2 of article 26 of the Proposal, when it requires that "[the] supervision is carried out through periodic verifications of the video surveillance systems and processing of data collected, by sampling",

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

1/

seems to be conditioning the inspection activity of the CNPD in terms that are not fully in line with the discretionary space recognized by the RGPD and by the aforementioned Directive to the national supervisory authority regarding its inspection function. Although the legislative intention may not have been that, the imposition that the inspection be carried out by sampling limits its inspection competence, precluding an eventual exhaustive inspection of the video surveillance systems of the security forces and services.

154. In this regard, paragraph 4 of article 26 must be corrected, when it refers to the CNPD's duty to order the "cancellation" of data, since the appropriate term will be deletion or erasure of data.

III. Conclusion

155. On the grounds set out above, the CNPD understands that the Draft Law, in all its provisions, introduces a very restrictive legal regime for the fundamental rights of citizens, in particular the rights to respect for private and family life and the right to protection of personal data, liable to affect the essential content of the right to respect for private life, by allowing mass surveillance in public space and in private spaces accessible to the public.

156. The broad and imprecise terms with which security forces and services use surveillance systems through fixed cameras and portable cameras - the latter may be incorporated into unmanned aircraft (drones) and agents' equipment (bodycams) indefinitely for any of the purposes admitted in the Proposal, with the generalized possibility of using artificial intelligence and facial recognition technologies, does not meet the minimum requirements in a democratic State of Law for the legislative restriction of fundamental rights.

157. What permeates throughout the diploma is the option to lighten the video surveillance regime for police purposes, both procedurally and substantially, to facilitate its use regardless of an effective and detailed assessment of its suitability and necessity to the guarantee of public safety or the safeguarding of goods especially deserving of protection. The underlying reason is that it is not necessary to verify a special risk or danger for such goods to justify the interference, to a high degree (especially when combined with certain technologies also generally accepted here), in the rights, freedoms and guarantees, the allegation of a supposed feeling of insecurity suffices.

158. The use of equipment and technologies that enhance the impact of the use of video cameras is not foreseen for specific purposes, and it seems to be indifferent to the national legislator whether they are used to prevent or repress crime or to prevent or repress any minor disturbance. gives

public order. This is the case with drones, bodycams and data analytics or facial recognition technologies.

159. Exceptional and special procedures proliferate, leaving the decision to use portable cameras (also with drones) to the

security forces and services themselves (irectius, their top manager) without any prior independent control. And without effective subsequent independent control.

160. Just enumerate here the:

i. lack of definition, at the legal level, of the conditions and limits of the use of video surveillance systems, in particular of portable cameras, in relation to which simplified and largely discretionary decision-making procedures are foreseen;

ii. the absence of setting criteria for the application of artificial intelligence technologies, and specifically in relation to biometric data;

iii. the opacity of the legal provision for the use of facial recognition technology in public spaces and also in private video surveillance systems that affect the private space accessible to the public;

iv. the lack of transparency regarding the use of portable cameras, especially when coupled to drones, as the duty of publicity is limited to the installation of fixed cameras;

v. the 5-year period for authorisations, which thus dispenses with an up-to-date assessment of the suitability and need for the use of video surveillance cameras;

to understand that this diploma does not make the use of video surveillance systems dependent on a concretely detailed judgment of suitability and necessity regarding the intended purpose, nor does it manage to fulfill the function of guiding security forces and services regarding their use, not preventing the possibility of its arbitrary use, nor fulfilling the function of predictability regarding the processing of personal data and likely consequences for the fundamental rights of citizens.

161. In this way, and in particular, the CNPD highlights that, as they represent restrictions on rights, freedoms and guarantees, in particular the fundamental rights to respect for private and family life and the protection of personal data, in gross violation of the principle of proportionality, the following rules of the Draft Law appear to be unconstitutional: the items //. and iii. of subparagraph d) of article 3; Article 10(2), Article 11, Article 17 and Article 18.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

v.

162. Finally, the CNPD takes the liberty of pointing out that, in its perspective, the impact that this Draft Law has on the fundamental rights of citizens and the structural deficiencies that it presents in the alleged regulation of processing of personal data highly restrictive of rights , freedoms and guarantees call for a deep and broad debate of the different legal provisions.

Approved at the meeting of November 4, 2021

Filipa Calvão (President)