(

O

National Data Protection Commission

OPINION/2021/99

I. Order

1. The Secretary of State for the Presidency of the Council of Ministers asked the National Data Protection Commission (CNPD) to issue an opinion on the Draft Decree-Law No. 956/XXII/2021, which “changes the alternative system and voluntary authentication of citizens in the portals and websites of the Public Administration called Chave Móvel Digital».

2. The CNPD issues an opinion within the scope of its powers 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 57, subparagraph b) of Article 58(3) and Article 36(4), all of Regulation (EU) 2016/679, of 27 April 2016 - General Data Protection Regulation (hereinafter GDPR), in conjunction with the provisions of article 3, paragraph 2 of article 4 and paragraph a) of paragraph 1 of article 6 of Law No. 58/2019, of 8 August, which implements the GDPR in the domestic legal order.

II. Analysis

3. The Draft Decree-Law in question introduces three main changes to Law no. 37/2014, of 26 June, last amended by Law no. from the Digital Mobile Key (CMD) to authentication to electronic systems and websites, allows the use of biometric identification features of the citizen's mobile device and introduces the possibility of associating facial recognition technology with the CMD.

4. As for the change mentioned in the first place, it results from the wording now designed for subparagraph a) of article 1 of Law no. and Internet sites of the Public Administration, now extends to any portals and sites on the Internet, therefore, also to those under the responsibility of private entities - although, strictly speaking, paragraph 11 of article 2 of the same law already admitted the possibility of regulating the use of the CMD as a means of authentication on Internet sites.

5. Added to this change is the possibility that authentication can be carried out using the biometric identification features of the citizen's mobile device, under the terms set out in subparagraph d) of paragraph 1 of article 3 of Law no. 37/2014, introduced

by the Project.

6. The same functionality is provided for the qualified electronic signature, in accordance with the projected subparagraph d) of paragraph 1 of article 3, A of Law no. 37/2014.

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

f

i. Facial recognition technology associated with CMD and the relevance of AIPD

7. From the perspective of protecting the rights, freedoms and guarantees of citizens in the context of processing personal data, the new regime for associating facial recognition technology with CMD for the purpose of obtaining it, provided for in the new wording of article 2, deserves special attention. .°, no. 6, subparagraph e), and no. 17 to 19 of Law no. 37/2014.

8. The first observation that must be made in this regard is related to the indispensability of an impact study on the protection of personal data resulting from this new data processing, in order, from the outset, to allow the taking of options at the legislative level - cf. no. 4 of article 18 of Law no. 43/2004, of 18 August, introduced by Law no. 58/2018, of 8 August (CNPD Organization and Functioning Law).

9. And while it is true that, although at the request of the CNPD, an impact assessment on data protection (AIPD) was sent on the CMD system, this assessment refers only to the part of the processing of personal data to referred to in the Project, being silent on the use of biometric secure identification functionalities as a second authentication factor. In this way, the presented IAPD fails to provide an effective explanation of the personal data processing operations and an assessment of the risks arising from them in sufficient terms for a considered decision, by the holders of political-legislative power, on the regulatory legal framework. to give to the new processing of personal data.

10. In fact, the entire process surrounding the regulation of the use of this technology for the purpose of processing personal data is an expression of persistence on a path that is certainly not desirable in a rule of law: the elaboration of laws that are

limited to a mere reflection of the de facto reality, harming the function of guiding the conduct (of the citizens and, of course, of the Public Administration) that the Law and the legal norms are required.

11. Indeed, the Agency for Administrative Modernization, I.P. (AMA), within the scope of an investigation process, declared in 2020 that it had not carried out any AIPD related to facial recognition technology, for, allegedly, having acquired the licensing of a software without any solution that made use of the software being implemented. even and only for the purpose of evaluating the possibility of carrying out the Simplex measure #50 and without having to worry about sending it to the CNPD when, finally, it was carried out.

12. And before the possible approval of a legislative diploma that legitimizes the use of facial recognition technology - prohibited under the terms of paragraph 1 of article 9 of the GDPR and only exceptionally allowed under the terms of paragraph 2 of the same article - , the National Security Office (GNS) published a dispatch in the

Diário da República1, with rules - issued, therefore, by an administrative body - legally binding for those responsible for processing personal data in the use of facial recognition technology and which impact on citizens' rights, without having previously consulted the CNPD and without being based on an IAPD. Corresponding, obviously, to an administrative regulation, this order was subject to the rules mentioned above, in point 2, and it should also be noted that its requirements are not merely technical, including rules on the processing of personal data - as is the case with the prediction of the possibility of conservation of biometric data within a certain period and with compliance with conditions such as pseudonymization.

13. For only in the legislative procedure, and after the request of the CNPD, the aforementioned AIPD has been presented.

14. The CNPD insists on this point because the need for prior and subsequent monitoring, by the supervisory authorities, of the regulation of the processing of biometric personal data, especially using facial recognition technology, has been highlighted at European level, given the impact that they can have in people's lives2. It also insists because, in the subsequent assessment of the provisions contained in the Project, it will highlight some of the inconsistencies between these and the aforementioned AIPD, inconsistencies that could have been avoided had the process followed.

ii. The insufficiency of the Project's rules in the definition of data processing and rights guarantees

15. Regarding the legal regime for the processing of personal data resulting from the use of facial recognition technology in the request to obtain the CMD, provided for in article 2 of Law no. the rules in question are limited to little more than providing for the processing, without densifying the elements and conditions for its implementation, nor defining guarantees of the rights of data subjects.

16. In fact, it is not immediately defined who is responsible for the processing of personal data. It should be noted that the indication, which appears, in the version still in force, of paragraph 8 of article 2 of Law n.° 37/2014, that AMA, IP., is responsible for the management and security of the technological infrastructure that supports the CMD, namely the system for generating and sending numerical codes for single and temporary use, is not elucidative as to the

1 Cf. Order No. 2705/2021, of 11 March, on the “Identification of natural persons through remote identification procedures using automatic biometric facial recognition systems”.

2 Cf, for example, the Council of Europe guidelines on facial recognition: Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data - Convention 108, Guidelines on Facial Recognition, January 28, 2021, P. 8, accessible at httos://rm.coe.int/ciuidelines-on-facial-recocmition/1680a134f3

who is responsible for the processing of data, under the terms set out in paragraph 7) of article 4 of the GDPR3, and says nothing about this new operation of processing personal data.

17. Furthermore, the personal data being processed are not defined and, specifically, which face images are collected electronically in real time (cf. subparagraph e) of paragraph 6 and also paragraphs 17 and 18 of article 2): if the image displayed in real time on the citizen's mobile device, if a photograph (.selfle) taken at the moment and sent by the citizen, if it also includes biometric details, if eventually the image of the face which appears on the citizen's card (which is only implicitly referred to in Article 2(19), when the image of the citizen's card is expected to be collected). Note that the AIPD (cf. 5.1.1.3. and 5.1.5.) foresees the collection of selfies and the collection of photographs of the face and the respective biometric

template.

18. Moreover, what is described in those rules does not seem to coincide and, therefore, does not seem to give legal coverage to the operations on personal data described in the IAPD presented - it should be noted that only in paragraph 19 of article 2 is spoken of the 'image of the citizen's card», which is characterized, in the AIPD, as corresponding to the photograph of the front and back of the citizen's card, therefore with all the personal data visible on it. This is one of the incongruities that must be corrected.

19. Furthermore, in the Project, there is no explanation of the process of processing personal data, apart from the reference to the comparison of the enigmatic images of the face collected electronically in real time with the facial image contained in the information system responsible for the life cycle of the citizen's card, in an automated way, using life detection software (cf. paragraph 17 of article 2). When in the AIPD (cf. 5.1.13 and 5.1.1.3.) another biometric comparative operation is described between the photograph visible on the citizen's card and the constant of that information system and it also refers to the use of Deep Learning algorithms for verification veracity of the Citizen Card.

20. Now, for reasons related to the predictability for citizens of the processing of personal data to be carried out by the Public Administration, the legal instruments must define the main elements of the treatment, among which the person responsible for the treatment, the data subject to treatment and storage periods. If this is indicated, in paragraph 3 of article 6 of the RGPD, for the processing of personal data in general, it becomes more pressing when personal data that integrate the special categories defined in paragraph 1 of article 9 of the GDPR, as is precisely the case with biometric data to uniquely identify a person. Even more so when the treatment is based, according to the

3 Since the responsibility for the management and security of a technological infrastructure is not equivalent to the responsibility for the processing of personal data that takes place in the context of the same.

determined in the Project, in the consent of the data subject - cf. paragraphs 17 and 19 of article 2, introduced by the Project.

21. It is recalled that - in fact, also in accordance with the general rules of law - consent presupposes that the expressed will is free and informed, for which it is essential to provide clear information regarding operations on personal data - cf . Article 4(11)

of the GDPR.

22. As the facial recognition system implies, a self-learning Artificial Intelligence technology, which therefore autonomously analyzes, through a deep neural network system (Deep Learning), the biometric data of each citizen's face , the explanation of what this system does is essential - how biometric data are processed «automatically» (e.g., which images are analyzed, the rationale or logic underlying the treatment, the consequences and risks for the data subject, etc. .) so that any citizen can freely choose to use it and consent to the operations to be carried out. Furthermore, the Project says nothing about the technology for detecting life and, as mentioned above, point 19, the AIPD states the use of Deep Learning algorithms to verify the veracity of the citizen's card.

23. Although the data controller is responsible for providing the information, as required by Article 13(2)(f) of the GDPR, the truth is that there is a risk that, specifically, if claiming that such information already derives from the law and to that extent the person is exempted from the fulfillment of the duty (cf. knowledge of the information), when in fact the elements of the treatment that the law reveals are scarce for a full understanding of it and its implications.

24. Also because, as regards one of the purposes provided for the processing (in paragraph 19 of article 2), it is not the mere reference to a 'data retention policy' that guarantees the right to information expressly imposed in the cited article 13 of the GDPR.

25. Furthermore, the reference to a government ordinance, contained in paragraph 14 of article 2, of the regulations necessary for the development and security of the CMD infrastructure is clearly not, in the context of the processing of biometric data using Deep Learning, capable of replacing the definition of the essential elements of that treatment in the proper headquarters, which is the law, when the ultimate purpose of authenticating citizens before public and private entities is at stake.

25. Therefore, the CNPD understands that the main elements and the process (the logic, if you prefer) of the automated processing of biometric data should be defined in more detail in the text of the Draft Decree-Law

within the scope of the technology used for facial recognition and for the verification of other personal data, so that the citizen

can be sufficiently informed for the purpose of issuing his consent.

27. Still regarding the Project's omissions regarding this processing of biometric data, it is important to mention that the periods for the conservation of personal data must also be defined in the legislative diploma and with exactitude, so that there can be no doubts as to the period during which its conservation is necessary.

28. Indeed, it could be said that the formula used in Article 2(18), that the images of the face are deleted after the completion of the procedure for obtaining the CMD, does not clarify the citizen - he is unaware whether this is the moment in which the validation of the elements necessary for the issuance of the CMD is concluded, or if it is the moment of delivery of the CMD. However, it should be noted that the AIPD refers to the automatic daily deletion of the photograph of the face and the respective biometric template. In addition, as for the front and back photograph of the citizen's card and the personal data visible therein, the AIPD states (cf. 5.1.11.) to be kept for 30 days, in accordance with the provisions of the GNS Order mentioned above. , in point 12. Therefore, once again, what the legal norm provides does not coincide with the description of the system contained in the IAPD presented.

29. In any case, it is essential that Article 2(18) extends automatic deletion to all personal data collected in that operation and not just face images. Thus, and in order to fully comply with point e) of paragraph 1 of article 5 of the RGPD, it is recommended to specify that all personal data collected for the issuance of the CMD are automatically deleted after the validation of the necessary elements for the effect.

30. Also with regard to retention periods, it is suggested to change the wording of paragraph 9 of article 2. There, the permanent recording of all interactions between citizens with the Public Administration or other entities processed through CMD is prohibited, when, strictly speaking, what the legislator seems to want to prohibit is the full registration of authentications. In fact, Ordinance No. 77/2018, of March 16, in its current version, provides in article 12 for one year as the retention period for authentications with the CMD. In other words, there is strictly a permanent record, but not complete, of the authentications while the CMD is active, which is updated over time.

31. Under any circumstances, it is not reasonable that the time limits for storing personal data relating to the use of the CMD for authentication before public and private entities are not currently defined by law, as they are essential elements of the processing of personal data through CMD. It is therefore recommended that the definition of the retention periods for this personal information be introduced in Law No. 37/2014.

iii. 0 use of videoconferencing for joining the CMD and confirming identity

32. Also among the alternative means of obtaining the CMD, the Project introduces in article 2, no. ordinance provided for in paragraph 14.

33. The CNPD does not question the possibility of resorting to such a mechanism, but insists, in this regard, that greater normative densification at the legislative level is imperative, since, as it stands, paragraph 6(f) of article 2 does not offer any guidance on administrative regulation, first of all, with regard to guarantees of citizens' rights.

34. This legal provision cannot, therefore, be limited to the mere delegation in an administrative regulation in a matter that has such an impact on the identity of citizens, on their subsequent authentication and on the different legal acts in which such authentication is necessary.

iv. The reuse of biometric data for another purpose

35. Paragraph 19 introduced by the Project in article 2 also provides for the collection of the image of the citizen's card by AMA, IP., and its storage for 10 days, for the purposes of the evolutionary development of the CMD, with prior consent of the citizen.

36. At stake will be the reuse of the image of the citizen's card for a different purpose: the evolutionary development of the CMD.

37. The question then arises whether by image of the citizen's card it is intended to refer to the photograph of the citizen presented on the card or if the image of the entire card, therefore, comprising the personal data visible in this identification document. And whether the treatment can also include the corresponding details of the citizen's face. The note, left above in point 18, is reiterated here, that the IAPD seems to assume that this is the reproduction of the front and back of the citizen's card - which, if confirmed, may be unnecessary and excessive for the intended purpose, unless it is related not only to the improvement of the facial recognition algorithm, but also to the improvement of the citizen card verification algorithm. Therefore, under penalty of violating the principle of minimization of personal data, enshrined in subparagraph c) of paragraph

1 of article 5 of the GDPR, the wording of paragraph 19 of article 2 must be changed, limiting processing the given face image or specifying the purpose and scope of the new treatment.

38. Continuing with the assumption that by image of the citizen's card it is intended to refer to the reproduction of the citizen's card, front and back, the provision in the legal norm that the stored data [...]

associated with the citizen raises the greatest perplexity. In fact, the fact that the different elements of identification of the citizen are visible in that image were not enough, even if it were only the image of the face of the citizen, the disassociation of the citizen is of little use in this context. Precisely, biometric data are sufficient to identify the citizen, as they allow to establish a univocal relationship with the citizen, which is why this pseudonymization announced here does not substantially mitigate the risks that a database of this nature always implies4

39. In any case, it is intended to carry out tests on real personal data, as well as biometrics, to improve the algorithm, with the consent to be provided by the citizen based on information that, under the terms of its designation "policy of retention of data", is insufficient. This is because it is not just the collection and conservation of personal data that are at stake; more than that, a database is created for the analysis of this data by the Deep Learning algorithm.

40. Thus, the law has to explain what the processing of personal data it is providing for, in its main elements, since, in addition to the foreseen period, the characterization of the treatment that paragraph 19 of article 2 makes is inaccurate. From the outset, it will be necessary to define which personal data are processed (only the photograph of the face? also the corresponding details? the other data contained in the citizen's card visible in the image of the same?); and what are the exact processing operations to which they are subject.

41. Regarding this last point, it should be noted that the collection and conservation of the image of the citizen's card, per se, does not allow the declared purpose to be achieved, so that, if the legal norm says nothing more, it can only be concluded due to the lack of adequacy of the treatment for the purpose of “evolutionary development of the CMD” and, to that extent, due to the manifest disproportionality of its legal provision.

42. Added to this are data protection issues that the standard does not address at all.

43. No guiding rules are established regarding the location of storage of personal data, especially biometric templates, first of all, if the database is maintained directly by the controller - which, according to the wording presented, appears to be the AMA, IP - or if there is a possibility of subcontracting this data processing operation.

44. Recalling that biometric data are at stake, especially protected under Article 9 of the GDPR, due to the risk that access and misuse entails for the legal sphere and for the lives of the respective citizens, the CNPD warns of the relevance of the national legislator to consider the option of requiring the conservation

4 It is not understood, therefore, the provision of this condition for the conservation of biometric data in the aforementioned GNS Order (cf. Annex A, 5.3.1.3.)

of these data in national territory - since the person responsible for this treatment is a public administrative entity - and to allow or exclude the possibility of subcontracting (aspect that will be developed below, points 47 et seq.).

45. The only requirement for security of personal data that the legal provision in question provides is the encryption of the image of the citizen's card. But the encryption of personal data by the controller, or by one of its processors, does not guarantee the use by any of them for different purposes.

46. For the above reasons, the CNPD recommends reviewing paragraph 19 of article 2, specifically and expressly providing for the personal data processed and the processing operations to be carried out, and also defining rules regarding the creation and storage of this biometric database, both in terms of its location and of direct responsibility for it.

v. subcontracting

47. Finally, it is important to highlight here the issue of subcontracting in the context of the processing of biometric data and other personal data using Deep Learning technology for facial recognition and for verification of the citizen's card. The issue is all the more important when it comes to the voluntary availability, by citizens, of their biometric data to an administrative entity for the ultimate purpose of using authentication mechanisms and qualified digital signature, a will that is formed on the

assumption - not expressly excluded by the law that provides for the treatment - that it is the administrative entity that collects, analyzes and stores such data.

48. The hypothesis that the public entity responsible for the processing subcontracts a third party - e.g., a private company - to carry out, in fact, the aforementioned processing raises new questions from the perspective of data protection, which may not be irrelevant either in the decision-making process. by the citizen.

49. Among these issues, the location of the database stands out in the first place - whether the data are stored in national territory, or in the territory of a Member State of the Union, or even in the territory of a third State that provide an adequate level of data protection. If, in the light of the GDPR, any of these solutions is admissible, it is not indifferent, even so, the question from the perspective of political choice and the option of each citizen.

50. Indeed, even if that biometric database is located in the territory of a Member State of the Union or of a third State that offers an adequate level of protection, it is essential to ensure that the subcontractor (or subcontractor) does not is subject to binding legal rules of a third State that may affect the protection guaranteed in the territory where the

database - this is what will happen, for example, if the company hosting the biometric database is part of a corporate group whose parent company is headquartered in a third State with legal rules that bind it to make available to the public authorities of that State the data stored or processed by you, as is clear from the jurisprudence of the Court of Justice of the European Union - cf. Schrems II judgment of 07.16.2020 (C-311/18).

51. The CNPD leaves this alert because the IAPD presented (cf. 5.1.13 and 5.1.17) refers to the subcontracting of the treatment described in point 47 (with biometric data and access to the life cycle database of the citizen's card) to a Portuguese company that has the platform and database hosted in another company based in Ireland, which, in turn, is part of a corporate group (Amazon) whose parent company is based in the United States of America. However, this situation, taking into account the European jurisprudence cited, unless the adoption of additional protection measures is demonstrated, is not admissible under the GDPR.

III. Conclusion

52. The CNPD understands that a legislative act that intends to regulate facial recognition in the context of the use of the Digital Mobile Key, because the treatment of biometric data using the Artificial Intelligence technologies of deep neural networks, has to define more detail the main elements of the processing, as well as the process (the logic) of the automated processing of biometric data within the scope of the technology used, so that the citizen can be sufficiently informed to be able to choose its use and give an informed and free consent.

53. Thus, and based on the grounds developed above, in II, the CNPD recommends:

The. The review of paragraph e) of paragraph 6 and paragraphs 17 and 18 of article 2 of Law no. 34/2017, introduced by the Draft Decree-Law, identifying the main elements of the treatments with Deep Learning technology for facial recognition, technology for life detection, Deep Learning technology to verify the veracity of the citizen card (e.g., the person responsible for the treatment, the personal data being processed - specifying the collected face images), as well as the process (the logic) of automated processing of biometric data within the scope of the technology used;

B. The specification, in article 2 of Law no. Public Administration and other entities, in full compliance with Article 5(1)(e) of the GDPR;

ç. The revision of paragraph 19 of article 2, on the collection and storage of the image of the citizen's card by AMA, IP., for the purposes of "evolutionary development of the CMD", specifically and expressly providing for the personal data processed and the processing operations in view, as well as defining rules regarding the creation and storage of this biometric database, both in terms of its location and in terms of direct responsibility for it.

54. With regard to the confirmation of identity by videoconference, the CNPD recommends the densification of subparagraph f) of paragraph 6 of article 2, since this provision does not offer any guidance on administrative regulation by ordinance, from the outset , with regard to guarantees of citizens' rights.

55. Finally, the CNPD draws attention to the inadmissibility, in the national legal system, of subcontracting the processing of

personal data, including biometrics, that prevent access to them by third States, in accordance with the jurisprudence of the Court of Justice of European Union.

Approved at the meeting of July 22, 2021

Filipa Calvão (President)

Av.D. Carlos 1,134.1° 1200-651 Lisbon

I (+351) 213 928 400 F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt