National Data Protection Commission

OPINION/2021/152

I. Order

1. The Minister of State Modernization and Public Administration asked the National Data Protection Commission (CNPD) to issue an opinion on the Draft Ordinance on the “Second amendment to Ordinance No. 77/2018, of 16 March , which makes the necessary regulations for the development of the Digital Mobile Key (CMD)'.

2. The request for an opinion is accompanied by an impact assessment on data protection (AIPD).

3. 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

4. This Draft Ordinance amends Ordinance No. 77/2018, of March 16, implementing the changes introduced by Decree-Law No. 88/2021, of November 3, in Law No. 37 /2014, of June 26th.

5. The CNPD notes that the provisions of the Draft Ordinance, with occasional exceptions, reproduce or are supported by the rules contained in that Decree-Law, without the inconsistencies and most of the omissions therein having been corrected or integrated, notwithstanding the CNPD for them to have drawn attention in the Opinion/2021/991, of July 22, which it issued on the draft of that legal diploma. To that extent, the CNPD will reiterate here part of the observations and recommendations that it left in the aforementioned opinion. Let's see.

i. Inadequacy of regulation of the processing of biometric data through facial recognition technology

6. First of all, it should be noted that essential elements of the processing of biometric personal data, which the CNPD, in its opinion, recommended to be fixed in the legal diploma, not only were not translated into this, but also are not determined in the Draft Ordinance .

1 Available at https://www.cnpd.pt/umhraco/siirfaoe/cnpdDeci.sion/download/121905

Av. D. Carlos 1,134,10

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

7. In fact, regarding 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. 37/2014, in its current version, the elements and conditions of its realization and for defining guarantees of the rights of data subjects.

8. In fact, Articles 4-A and 4-B, now added by the Draft Ordinance, do not define, from the outset, who is responsible for the processing of personal data. It should be noted that the indication, contained in paragraph 8 of article 2 of Law no. 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 numeric codes for single and temporary use, does not clarify who is responsible for data processing, under the terms set out in paragraph 7) of article 4 of the GDPR2.

9. Furthermore, the Draft Ordinance, like the legal diploma that regulates it, does not define the personal data being processed and, specifically, does not specify which face images are collected electronically in real time (cf. subparagraph e) of n. 6 and also paragraphs 17 and 18 of article 2 of Law no. 37/2014): if the image viewed in real time on the citizen's mobile device, if a photograph (if/f/e) taken at the moment and sent by the citizen, if it also includes the biometric details and if eventually the image of the face that appears on the citizen's card. It is not understood why the specification of the personal data being processed is considered unnecessary, when this is an essential element of the processing, especially when the processing of biometric data is at stake.

10. Furthermore, in the Draft Ordinance, there is no explanation of the process of processing personal data, apart from the reference to the comparison of the face images collected electronically in real time with the facial image contained in the

information system responsible for the cycle of life of the citizen's card, in an automated way, using life detection software (provided for in paragraph 17 of article 2 of Law no. 2 of article 4-A, now introduced in Ordinance No. 77/2018, stating that "[t]he registration [...] is carried out in accordance with the procedures established by the National Security Office on identification of natural persons through remote identification procedures using automatic biometric facial recognition systems'.

11. Now, neither the legal diploma, as required, nor the ordinances that regulate it offer the least amount of predictability for citizens regarding the processing of personal data to be carried out by the Public Administration, among which are the person responsible for the treatment, the data object of treatment

2 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.

and retention 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.

12. In the Draft Ordinance, as, incidentally, it would have happened at the legislative level, it seems to be assumed that, as the legal basis for the processing of biometric data is the consent of the data subject (see paragraphs 17 and 19 of article 2 of Law No. 37/2014), it is unnecessary to identify in the respective legal and regulatory documents the elements essential to the perception that personal data are processed and what the consequences or risks are, when, in fact, the consent to be legally relevant must be informed.

13. 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. But the Project says nothing about the technology for

detecting life and, however, the AIPD states the use of Deep Learning algorithms to verify the veracity of the citizen's card.

14. Although the data controller is responsible for providing the information, as required by subparagraph f) of paragraph 2 of article 13 of the RGPD, the truth is that a diploma whose purpose is to regulate this specific processing of personal data must assume the degree of predictability and density required in a Rule of Law and, therefore, contain elements that allow citizens to make an informed and conscious choice.

15. Also because there is a risk that, specifically, it is claimed that such information already derives from the law and the ordinance and to that extent the person is exempted from the fulfillment of the duty (cf. paragraph 4 of article 13 of the RGPD , which admits this exemption when and to the extent that the data subject already has knowledge of the information), when in fact the elements of the treatment that the law and the Ordinance Project reveal are scarce for a full understanding of it and its implications .

16. Therefore, the CNPD understands that the main elements and the process (the logic, if you prefer) of the automated processing of biometric data within the scope of the technology used must be defined in more detail in the text of the Draft Ordinance for facial recognition and verification of other personal data,

insisting that an uninformed consent is not sufficient to legitimize the processing of special or sensitive data that are the subject of provision.

ii. Subcontracting and reusing biometric data for another purpose

17. It is also important to insist on the provision for the reuse of the image of the front and back of the citizen's card for a different purpose, the evolutionary development of the CMD, provided for in paragraph 19 of article 2 of Law No. 37/2014 .

18. As the CNPD drew attention in its Opinion on the Draft Decree-law that this provision lacked normative densification, which only partially occurred in the approved version of Decree-Law No. 88/2021, it is very strange that the Ordinance Project is regarding this new treatment of personal data totally omitted.

19. The only requirement for security of personal data that the legal precept in question provides is the encryption of the image

of the citizen's card3. 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.

20. Specifically in this regard, but with considerations that are relevant for the entire processing of biometric data, the CNPD insists on the need for the Draft Ordinance to frame the subcontracting regime within the scope of the processing of biometric data and other personal data using Deep Learning technology for facial recognition and citizen card verification.

21. The issue is all the more important when at stake is the voluntary availability, by citizens, to an administrative entity of their biometric data for the ultimate purpose of using authentication mechanisms and qualified digital signature, a will that is formed on the assumption - no expressly excluded by the law that provides for the treatment - that it is the administrative entity that collects, analyzes and stores such data.

22. The hypothesis that the public entity responsible for the processing subcontracts a third party to carry out, in fact, the aforementioned processing raises new questions from the perspective of data protection, which may not be irrelevant in the decision-making process by the citizen either. Among these questions, in the first line, is the question of who ensures the storage of biometric data.

3 It is reiterated that the statement in paragraph 19 of article 2 of Law no. 34/2017 that the stored data [...] is not associated with the citizen raises the greatest perplexity, since even that only the image of the face of the citizen is at stake, the disassociation of the citizen is of little use in this context. Precisely, biometric data are sufficient to identify the citizen, as they allow a univocal relationship with the citizen to be established, which is why this pseudonymization announced here does not substantially mitigate the risks that a database of this nature always implies.

23. Indeed, even if that biometric database is located in the territory of a Member State of the Union, it is essential to ensure that the subcontracting company and the subcontractor are not subject to binding legal rules of a third State that could affect the protection guaranteed in the territory where the database is housed.

24. This is precisely what happens in this case, as stated in the AIPD (cf. 5.1.17): the company where the platform that performs the validations associated with the remote identification procedures is hosted is AWS (Amazon Web Services , Inc),

headquartered in the United States of America, which is a third State that presents legal rules that bind this company to make available to certain public authorities of that State the data stored or processed by it, as follows from the jurisprudence of the Court of Justice of European Union - cf. Schrems II judgment of 07.16.2020 (C-311/18).

25. However, this situation, taking into account the European case-law cited, unless it is demonstrated that additional protective measures have been adopted, does not appear to be admissible in the light of Articles 44 and 46 of the GDPR, in particular in view of the sensitive nature of of information that, it is insisted, even if it could be encrypted - and it cannot, as it would prevent the pursuit of the purpose -, always allows the identification of the data subjects. And there is not, in the presented IAPD, any risk assessment specifically on this processing of personal data, in contradiction with Article 46(1) of the GDPR.

26. It is reiterated that the consent to be legally relevant and, therefore, to be able to legitimize an operation that involves or is likely to involve the international flow of sensitive personal data to a third State without adequate protection, must fulfill the attributes of paragraph 11) of article 4 of the GDPR, which, under the terms of Law No. 37/2014 and the Draft Ordinance, is not guaranteed, given the omission of all aspects relating to subcontracting and subcontracting relationships.

27. Thus, the CNPD recommends that the Draft Ordinance take care of the risk of transferring biometric data to third States that do not guarantee adequate protection, in accordance with the jurisprudence of the Court of Justice of the European Union.

iii. Changes introduced by article 2 of the Draft Ordinance

28. Finally, it is important to point out an aspect of the legal regime contained in the Ordinance and in the Draft Ordinance on personal data processed for the purpose of registration. Pursuant to article 2 of Ordinance No. 77/2018, in the new version now designed, registration implies the association of the civil identification number, tax identification number or passport number, adding that it can also be associated the email address.

Av. D. Carlos 1,134,10

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

29. However, the CNPD only questions the final part of paragraph 1 of article 2 because the provision that the address does not have to be associated makes or may make the provisions of paragraph 3 of article 7 unenforceable. .° of the Project. Indeed, unless another alternative means of communication is indicated, it is not possible to change the mobile number in the event of loss of access to the registered number.

30. Moreover, in the AIPD (cf. 6.1.3.2) it is stated that membership of the CMD is terminated if the holder does not enter the email address; however, the Draft Ordinance identifies this data as optional when referring to "the email address may also be associated".

31. To that extent, it is recommended to consider the optional nature of providing the email address, in the final part of paragraph 1 of article 2, or to explain in paragraph 3 of article 7 that the possibility of changing the mobile number depends on the prior provision by the data subject of an alternative contact. And, above all, that this information is made available on the website, so that the citizen can make a decision in complete freedom as to whether or not to provide this personal data.

32. Finally, with regard to paragraph 6 of article 6, what constitutes 'mediated telephone service', which has no legal provision, and which represents a new means of processing personal data, is not achieved. Nor does it seem to have assessed the specific risk posed by the use of this medium, since the IAPD refers to the registration official (mediator) only for videoconferencing situations.

III. Conclusion

33. The CNPD understands that this Draft Ordinance suffers from omissions that had already been noted in the draft legal diploma that amended Law no. Artificial Intelligence technologies of deep neural networks, does not define in detail the main elements of the treatment, as well as the process (the logic) of the automated treatment of biometric data within the scope of the technology used, so that the citizen can be sufficiently informed to be able to opt for its use and give informed and free consent.

34. Thus, and with the foundations developed above, the CNPD recommends the prediction of the main elements of treatments with Deep Learning technology for facial recognition, technology for life detection, Deep Learning technology to verify the veracity of the citizen card (eg, the controller, the personal data being processed - specifying the collected face

images), as well as the process (the logic) of the automated processing of biometric data within the scope of the technology used;

35. The CNPD also draws attention to the impact that the subcontracting of operations or part of the operations for the processing of biometric data can have on the legal sphere of citizens, underlining the inadmissibility, in the national legal order, of subcontracting the processing of personal data , including biometrics, which imply or involve access to them by third States, in accordance with the jurisprudence of the Court of Justice of the European Union, noting that the information contained in the IAPD points towards this possibility, so it is recommended that in the Draft Ordinance, such a consequence is taken into account.

36. Finally, it is also noted:

The. The difficulty of reconciling the provisions of paragraph 1 of article 2 with the provisions of paragraph 3 of article 7 of the Ordinance, in the wording given by the Draft Ordinance, recommending the consideration of the optional nature of the supply of the email address, in the final part of paragraph 1 of article 2, or the explanation in paragraph 3 of article 7 that the possibility of changing the mobile number depends on the prior provision by the holder data, an alternative contact;

B. The indication in paragraph 6 of article 6 of the "mediated telephone service", which is not provided for in the legal diploma that the Draft Ordinance intends to regulate, and which reflects a new means of processing personal data, not revealing to have there has been any assessment of the specific risk posed by the use of that medium.

Lisbon, December 3, 2021

Filipa Calvão (President, who reported)

Av.D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt