AVG/2019/356

_ _ J

National Data Protection Commission

Opinion/2021/30

I. Explanation of the object of this Opinion

1. This opinion is based on the inspection carried out by the National Data Protection Commission (CNPD) of the in-person electronic voting system in the 2019 European Parliament elections, based on the technical report, to highlight a set of aspects related to the processing of data. personal data resulting from the use of electronic voting systems that lacks legal regulation.

2. This opinion is issued by the CNPD, as an administrative authority with powers to monitor and control the processing of personal data, to raise awareness, both of citizens and organizations, as to the risks and guarantees associated with the processing of personal data, as well as advice to the political power regarding legislative and administrative measures related to the defense of rights and freedoms in the context of data processing, under the powers conferred by subparagraphs a) to d) of paragraph 1 of article 57, in conjunction with paragraph 1(b) and article 58(3)(b), both 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 b) of paragraph 1 and paragraph 2 of article 6, all of Law no. .° 58/2019, of August 8, which implements the GDPR in the domestic legal order.

3. The CNPD's option of only now commenting is related not only to the complexity of the matter and the constraints and challenges regarding data protection caused by the pandemic situation over the last year, but also with the understanding that , on the one hand, a pronunciation of this type immediately after the two 2019 elections could be interpreted as a claim to validate or invalidate the electoral results - leaving it expressly noted that this is not the purpose of this pronunciation - and, on the other hand On the other hand, its publicity before an electoral act in which its use was not considered (the presidential elections) would produce noise and, eventually, would bring the risk of generating the erroneous conviction that such an act would be based on that system.

4. As alternative ways to the voting system established by law are now being considered for municipal elections, and the need to reassess the electronic voting solution is understood, after more than fifteen years have passed since the CNPD Deliberation on Privacy Electronic Voting, of 14 November 20051, with all the regulatory and technological changes that have

taken place in the meantime, and with sufficient time distance to contribute to the public debate and political consideration of the different solutions, the CNPD believes that this is the opportune moment to adopt this opinion.

1 Deliberation available at https://www.cnnrl.nt/media/0y3dvime/delib voto electronico.pdf

Av. D. Carlos 1,134,1o 1200-651 Lisbon

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

geral@cnpd.pt

www.cnpd.pt

5. The analysis that follows is divided into two parts: the first focuses on the electronic voting system used in the elections to the European Parliament in the municipality of Évora, within the scope of the pilot project; the second addresses the use of this (and, incidentally, other) system(s), in the light of the legal framework for data protection, the intended purpose and considering the existing information on electronic voting processes.

II. In-person electronic voting system in the 2019 European Parliament elections

i. CNPD intervention framework

6. Organic Law No. 3/2018, of August 17, came, in paragraph 1 of article 8, to provide for the possibility for the General Secretariat of the Ministry of Internal Administration (SGMAI) to promote the implementation, on an experimental basis, of face-to-face electronic voting, in at least 10 national councils, with votes being counted in the tabulation of results, in the 2019 European Parliament elections. The CNPD was not consulted within the scope of the legislative procedure within which the aforementioned law was passed.

7. On May 3, 2019, about a month before the elections, it was known from the media that the pilot project would be carried out in the district of Évora, but until then the CNPD had not been consulted on this implementation , which, as will be explained further below, involves new processing of personal data, the CNPD requested, by letter addressed to the Ministry of Internal Administration, the remittance of the impact assessment on the protection of personal data which, in compliance with no. 1 of article 35 of the GDPR, would have to have been prepared, taking into account that the processing of personal data resulting from the implementation of the pilot project was likely to generate a high risk for the rights of citizens, either by virtue of the use of innovative technology, whether by context, nature or extent of it. Assessment, dated May 17, 2019, which was delivered to

the CNPD on the same day, therefore, on May 17, 2019.

8. Indeed, it is important to note that the entire electoral process is based on the processing of personal data, based on the Electoral Census Database (BDRE), in order to organize and keep the information of all voters registered in the census, as well as in the Electoral Registration Management Information System (SIGRE), which centrally ensures the updating and consolidation of information derived from interoperability with the different information systems that feed the voter registration2. As the entity responsible for the processing of

2 Legal Regime for Voter Registration, approved by Law No. 13/99, of 22 March, lastly amended by Organic Law No. 4/2020, of 11 November.

data, the General Secretariat of the Ministry of Internal Affairs (hereinafter, SGMAI) released the following information about the experimental project:

/. As part of the electronic voting pilot project, to ensure the uniqueness of the vote of voters in the District of Évora, Dematerialized Electoral Registers were designed, and their constant information was obtained through SIGRE (Electoral Census Information and Management System) based on the BDRE (Electoral Census Database) registration information. The voters' personal data contained therein come from the Electoral Census Database (BDRE), collected by the census entities and by the identification services, which operate through interoperability platforms with SIGRE, by virtue of legal provisions that establish the mandatory and official registration in the voter registration, for Portuguese voters residing in national territory.

9. The CNPD, in the exercise of the powers provided for in paragraphs b), e) and f) of paragraph 1 of article 58 of the RGPD, in conjunction with the provisions of article 3, paragraph 2 of article 4, and in paragraph b) of no. 1 and in paragraph 2 of article 6, all of Law no. 58/2019, of 8 August, and also within the competence provided for in no. 2 of article 11, of Law No. 13/99, of 22 March, last amended by Organic Law No. 4/2020, of 11 November, carried out several investigations to verify whether the voting process face-to-face electronic voting involves, at the time of voting, processing of personal data, and monitoring the processing of personal data relating to the electoral rolls on which its execution was based.

10. Within the scope of the investigation carried out, in particular with the aim of verifying whether this electronic voting system did not involve the processing of personal data at the precise moment of exercising the right to vote and at a subsequent moment, the CNPD detected facts with relevance to the electoral legal regime, but for the assessment of which (their compliance with the law) this Commission has no competence. In order to contribute to the improvement of the electoral system and to a more detailed legal regulation of electronic voting processes, as these facts are in apparent contradiction with legal provisions and, in some cases, do not offer sufficient guarantees of the integrity of the vote, the CNPD feels that it should point out them here, as well as the norms and principles that may be in crisis.

ii. Description of the electronic voting system

The. Creation of Dematerialized Electoral Books for the District of Évora

11. For the download of voters in the suffrage (/.e„ to indicate those who exercised the right to vote), SIGRE allows the issuance, by SGMAI, of electoral rolls in electronic format, with a view to printing and

use in the electoral act by polling stations or sections (cf. no. 2 of article 58 of Law no. 13/99, of 22 March, as amended by Law no. 47/ 2018, of August 13)3.

12. In the case of elections to the European Parliament, at the time they were held, each parish corresponded to a polling station and the polling stations of parishes with a number of voters significantly greater than 1000 are divided into polling stations, so that the number of voters is adequate to the geographic reality and the places where the electoral act is carried out, seeking, whenever possible, that it does not significantly exceed this number (cf. paragraphs 1 and 2 of article 40 of the Electoral Law of the Assembly of the Republic4 - Law No. 14/79, of 16 May, as amended by Organic Law No. 3/2018, of 17 August, as this was the version in force at the time of the electoral process in cause). Each electoral roll contains the identification of the set of voters who vote in that polling station - cf. Article 51(2) of the Electoral Law of the Assembly of the Republic.

13. Now, in the operation of electronic voting in the district of Évora, to allow each voter to choose the section where they would cast their vote, the necessary conditions were created to ensure that voters could vote in any assembly or section

related to electronic voting. : through the creation and availability of Dematerialized Electoral Records (CED), which included all voters in the district with active electoral capacity, which made it impossible to respect that legal command.

14. Even for the traditional polling stations (where there was no electronic voting), since it is necessary to guarantee the uniqueness of the vote, the SGMAI gave instructions for the polling stations in these sections to download both the printed electoral rolls and the in the CED.

15. In fact, through the CED system it is guaranteed that a voter can exercise the right to vote in any polling station in their registration district, ensuring that they only vote once and that the information5 in the digital electoral rolls is kept intact.

16. The CED system consists of a web interface that allows access, in a distributed way6, to a central database and has the purpose of consulting and downloading the electoral rolls in digital format.

3 After the electoral act under analysis, Organic Law No. 4/2020, of November 11, amended this No. 2, which now reads as follows: The electoral administration of the General Secretariat of the Ministry of Administration Internally makes available, with a view to its use in the electoral act or referendum, electoral rolls in electronic format or, alternatively and provided that the necessary technical conditions are met, dematerialized electoral rolls. On this legislative amendment, see below, points 109 to 113.

4 Applicable ex vi article 1 of the Election Law for the European Parliament - Law no. 14/87, of 29 April, last amended by Organic Law no. 1/2014, of 9 January.

5 Information on who voted, in which section they voted and which form of vote (traditional or electronic) they performed.

6 Where users access a centralized system from different points.

17. All polling stations in the district, whether or not they were involved in electronic voting, had access to the electoral rolls with all the voters and the voters' discharges were registered in the CED, in an auxiliary table called CEDJDBJ.VOTACAO, which aggregated all voters who voted.

18. Envelopes with the credentials assigned by the SGMAI, unalterable, were delivered to the members of the polling stations

for access to the CED and electronic voting machines. SGMAI generated random passwords for each of these users, which were printed and delivered, in a sealed envelope, to each chairperson on election day. As a form of redundancy, each vice chairperson also received an envelope with the same credentials as the chairperson.

19. To the presiding officer and to the tellers, the CED system makes available the functions of polling the voter, admission of the voter (the polling station confirms the identity and informs the voter that he can vote), finalization of voting (discharge in the electoral roll, after the voting) and cancellation of voting (elimination of electronic voting due to irregularity in the procedure or the voter's will).

20. Support to polling stations for problems that might occur with the CED was provided by a subcontractor that was available through a call center to support the polling stations. The support took place following the contact and express request of the elements of the polling station. Access by the subcontractor's employees was carried out with the profile of the polling station member, thus having the possibility of carrying out operations on behalf of that user. The CED system log recorded these accesses as "user impersonation".

B. Electronic voting procedure

21. In the absence of procedural rules, electronic voting in the district of Évora followed the procedures contained in a PowerPoint presentation and the so-called "Practical Guides" that served as a basis for training the members of the board. These documents were made available to the CNPD.

22. These only result in instructions for the opening and closing of polling stations and the steps to be followed for voting by voters.

23. As these documents do not include a description of the architecture of the electronic voting system, it was useful for the CNPD, for the purpose of monitoring the system, to have at least access to the implementation reports on the development of the application to support the CED, which did not happen.

24. Indeed, the services for the development of the application to support the CED and its implementation and operation were awarded in contract No. 12/2019, signed on 02/14/2019, which had as its object

r

such operations, on an experimental basis, in elections to the European Parliament and to support the counting of votes by Portuguese residents abroad.

25. In Clause 4.a, with the heading Deadline and phases of execution, three phases were established, namely: Phase 1 -Development of the application to support the CED, with an estimated duration of three months; Phase 2 - European Elections 2019 (configuration and monitoring of the electoral act); and Phase 3 - 2019 Legislative Elections (configuration and monitoring of the process of counting the votes of residents abroad).

26. Paragraph 6 of Clause 8.a provides for the delivery of a Phase Report at the end of the provision of services for each of the phases, with the payment due for each phase (paragraph 1 of Clause 6 .a) dependent on the delivery and acceptance of said Phase Report.

27. By email dated 05/22/2019, the CNPD requested the phase 1 report, having received as a response that the document was still being prepared, as it was awaiting approval from the SGMAI.

28. Already after the election date, the CNPD requested access to the reports, having obtained as a response that the Phase 2 report did not exist because the first phase was not completed.

29. Thus, based solely on the documents indicated above, in point 21, the act of voting involved the following steps:

The. the voting citizen identifies himself at the table with the respective identification document;

B. the teller polls the voter in the CED7 and activates voter "admission";

ç. the voter is given a smart card containing a token for single use by that voter, which enables the activation of their voting session;

d. the voter goes to the electronic voting booth, inserts the smart card and signs his/her vote on the voting machine's touch screen;

and. the voter gives the printing order of his vote, which reproduces the ballot paper displayed on the screen with his choice marked;

f. the voter returns the smart card and places the printed proof of vote in the traditional ballot box;

g. teller 1 unloads the vote in the CED and teller 2 confirms end of voting.

7 Available on two portable computers, assigned to each of the tellers.

30. Also, the traditional polling stations in the district of Évora, as they have to use the CED and the paper-based electoral roll, have adapted their procedures with regard to the unloading of voters in the two types of rolls.

31. As regards the electronic voting system, each voting booth was equipped with a computer with a smart card reader (ECO), a printer and a touchscreen with two compact flash memory cards (one of them installed inside the drive and another accessible through the front cover) for data storage.

On the internal card (only accessible by removing the ECO component), only the operating system and the voting system software would be stored.

32. The voting systems were configured so that, in each electronic voting section, two voting booths were installed, connected to each other8.

33. In situations where the voter was unable to print the cast ballot (most of the time, because the printer ran out of paper), the polling station president had a mechanism to give a new order for printing the vote.

34. This mechanism makes it possible for the presiding officer to always reprint the last vote, i.e., the vote of the citizen who has just voted.

35. During the electoral act, a technician from the subcontracted company was present in each electronic voting section, to provide support in the opening and closing of the electronic voting system, as well as during the electoral act whenever there were events that required technical support.

36. Once the chair was closed, it was up to the subcontractor's technician to ensure the dismantling of the different components of the voting systems. A seal was placed on the ECO component, and the components of the electronic voting system (ECO, compact flash, VIA and smart cards) were stored in boxes and a new seal was placed. The sealing process of the ECO machines and the respective transport boxes consisted of the simple affixing of a sticker with the description "Portuguese Republic - Early Vote".

ç. Mechanism for verifying the reliability of the vote in the pilot experiment

37. The electronic voting system covered the process of printing and placing the cast vote in a traditional ballot box, which aimed to make it possible to compare and validate electronically registered votes, in order to create confidence in the citizen as

to the integrity of their cast vote9, and allow, through the opening of the

8 In direct communication, without using network equipment.

9 Guarantee that the vote marked on the screen of the electronic voting machine corresponds to the printed vote.

Av. D. Carlos 1,134.1° T (+351) 213 928 400 geral@cnpd.pt

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

f

polls, the polling stations could confirm the number of votes cast and consequently the number of voters in the section, as well as the correspondence between the results recorded in the machine (on the memory card) and the printed votes in the box.

38. However, the SGMAI gave express instructions to the tables not to open the polls.

39. In fact, several minutes of the electronic polling stations contain requests, complaints or protests from delegates to count the paper votes in the ballot boxes. In all of them, the request or complaint was rejected because the Assistant Secretary for Internal Administration had given express instructions for these boxes not to be opened.

40. This instruction was documented to the CNPD by the person responsible for the electoral process at the Évora City Council.

iii. Facts found with legal relevance in the light of the electoral legal regime

41. It is noted, as highlighted above, in point 10, that, within the scope of the investigation carried out, some of the facts found by the CNPD refer to rules and principles of the electoral legal regime for which this Commission is not competent. But, as they are in apparent contradiction with legal provisions and, in some cases, do not offer sufficient guarantees of the integrity of the vote, the CNPD believes that it should point out these facts here, as well as the norms and principles that may be in crisis.

The. Presence of non-voters in polling stations

42. As mentioned above, point 35, during the electoral act, a technician from the subcontracted company was present in each electronic voting section, to provide support in the opening and closing of the electronic voting system, as well as during the electoral act whenever events that lack technical support may occur, which appears to contradict the prohibition on the presence of non-voters in electoral assemblies established by article 93 of the Electoral Law of the Assembly of the Republic (here applicable ex vi article 1 of the Electoral Law for the European Parliament).

B. Transport and storage of electronic votes

43. The delivery by the SGMAI of an external storage device (USB flash drive) to the Intermediate Tabulation Assembly, containing the files with the lists of voters who voted at the electronic and traditional polling stations in the district of Évora10, was carried out without security measures to prevent the improper access

10 These lists included the voters' full name, the polling station of origin, the polling station where they voted, the identification number and the corresponding page and line of the (traditional) electoral roll.

to its content; in fact, they corresponded to PDF listings stored on a removable medium, without any physical or logical protection measure that would guarantee the confidentiality and integrity of the information.

44. As for the transport of electronic votes, no pre-defined security measures were taken, and in fact, adequate and sufficient measures were not adopted.

45. Indeed, as described above, in point 36, the sealing process of the ECO machines and the respective transport boxes is limited to the simple affixing of a seal with the description "Portuguese Republic - Early Vote". This procedure hardly offers security guarantees, especially since seals, as self-adhesive, do not truly isolate the systems from undue access, and it is conceivable that a careful removal and replacement of the breast would allow access to the interior of the components, without visible signs of this violation11; in addition, the CNPD detected machines without a seal or with a torn seal;

46. There was also uncertainty as to where the voting machines should be sent, and under what conditions, for the purpose of storing them, with no adequate place being provided for their conservation, nor any indication of the appropriate time period for this purpose.

47. Finally, the boxes with the components of the electronic voting system of each section (with the memory cards where the electronic votes are registered) were collected by elements of the National Republican Guard and the Public Security Police and transported to the premises of the District Command of the Évora Public Security Police.

48. It is recalled that the law determines that votes are sent and are kept by the judge of the section of the local instance or, as the case may be, of the section of the central instance - cf. Article 12 of the Election Law of the European Parliament and

Article 104 of the Election Law of the Assembly of the Republic.

ç. Registration of access and changes to electronic voting machines after the election

49. After the elections, on the 6th and 17th of June, with the presence of the President of the Assembly of Intermediate Tabulation of the District of Évora and technicians from SGMAI, the CNPD identified the machines it intended to verify and proceeded with the forensic copy12 of the compact flash of the voting systems of these machines.

11 In this regard, note is made of the study by Andrew W. Appel, from Princeton University, which, as would be expected, concludes that a traditional seal system does not provide sufficient security guarantees - cf. Security seals on voting machines: A case study. ACM Trans. info syst. Security 14, 2, Article 18 (September 2011), available at http://doi.acm.ora/10.1145/2019599.2019603

12 The forensic copy was performed using the Tableau Forensic Duplicator tool, having proceeded to a bit-by-bit copy from the source support (compact flash) to the destination support (formatted USB stick), guaranteeing two fundamental requirements: that the original media information is not changed; that the target medium becomes a full copy of the original medium. After the cloning process, the corresponding report was printed with the digital signature of a hash associated with the image of the copied support,

50. After analyzing the collected elements, it was found that the compact flash stored inside the machines, intended to have the operating system and the voting system software, had an internal copy (replica) of the votes cast.

51. From the analysis of the Windows Event Logs, it was possible to verify that the operating system of several voting machines had files altered on June 1st and files accessed on May 28th, dates after the vote.

52. However, given that the machines had to be sealed - and that they actually had the self-adhesive seal - and that their integrity had to be guaranteed, the operating system cannot produce records that allow that integrity to be doubted.

53. Considering a pilot project in which electronic votes count for the electoral result, this type of incident is not at all admissible.

d. Discrepancies between the number of voters discharged in the CED and the number of votes held in the machines

54. The CNPD found that, in at least three polling stations13, there was no coincidence between the number of votes registered in the compact flash machines and the number of CED downloads.

55. For this reason, it requested the minutes corresponding to those sections and verified that the discrepancies were reflected in the minutes. In these minutes, several situations are reported that may have given rise to this result, in particular those arising from voters' statements that they had not exercised their right to vote because the system informed that the smart card had already been used, as well as a voter who , after voting, stated that the impression did not correspond to the vote expressed. In both situations citizens were allowed to vote again.

56. These situations were not addressed in the training documentation and, consequently, there were no indications for their resolution.

57. In several minutes of the electronic polling stations, there are also requests, complaints or protests from delegates to count the paper votes in the ballot boxes. In all of them the request or complaint

document that proves that that copy has not been altered. All proofs were delivered to the President of the Intermediate Tabulation Assembly.

13 In Polling Section no. 3 of the Union of Parishes of Bacelo and Senhora da Saúde, in Section no. 6 of the Union of Parishes of Malagueira and Horta das Figueiras and in Section no. 1 of the Parish of Santiago do Escoural.

was rejected because the Assistant Secretary for Internal Administration had given express instructions for these polls not to be opened.

58. Protests/complaints were also presented to the Intermediate Tabulation Assembly so that the ballot boxes with the prints of the electronic votes could be opened. These requests were rejected. However, this Assembly decided to open and count the printed votes in the three polling stations where there were discrepancies between the number of discharges in the CED and

the number of votes indicted by the electronic voting machines.

59. Despite the fact that, in these cases, it was proved that there was a coincidence between the number of voters discharged in the CED and the number of printed votes introduced in the ballot box, the votes contained in the electronic voting machine report were considered, as it was understood that «in against the provisions of art. 101.o, no. 3 of the Electoral Law of the AR (applicable by the provisions of art.0 1 of Law 14/87 of April 29, with the wording of Law no. 4/94 of March 9), which The "number of ballot papers counted" will prevail, in other words, the number of electronic ballot papers counted by the machine'.

60. Bearing in mind the objective of this pilot experience, these are facts that could not fail to be reported and from them consequences for solutions to be adopted in the future.

61. With this, the printing of electronic votes and the corresponding conservation of the forms proved to be practically useless, since there was no place to count them, frustrating the objective of the legal provision of a pilot project - cf. above, points 37 to 40. In fact, there was no verification, by comparing the printed votes and the votes recorded in the machine in each polling station, whether the electronic voting system presented the same numbers of voters and the same number of votes by lists than those in the one where the printed votes were cast. In conclusion, therefore, that the legal purpose of the experimental implementation of this system was not fulfilled.

iv. Electronic vote of 2019 in light of the legal regime for the protection of personal data

The. Dematerialized Electoral Books

i. Too much information in the CED

62. In this regard, it is important to note that the CED contain much more information than the electoral rolls provided for by law, both in terms of the universe of voters and the categories of data accessed. Indeed, the electoral roll only contains the identification card number, whether identity card, citizen card or other, and the full name of the voter (cf. articles 52, 53 and paragraph 2 of article 58 of Law No. 13/99, of 22 March, with the wording given to it by Law No. 47/2018, of 13 August), while the CED

present the data contained in the public part of the citizen card and allow searches to be carried out, using the citizen card chip or identification number, name or affiliation, without this being or currently being specifically provided for by law.

63. This reflects the disregard for the principle of minimization of personal data provided for in subparagraph c) of paragraph 1 of article 5 of the GDPR.

ii. Inexact search criteria that produce multiple results

64. In addition, the system admits a search criterion indicating only a voter's name. In meetings with the CNPD, the SGMAI highlighted the problem that there are still voters with only one (proper) name on the electoral roll - which is why the CED system seems to be designed to carry out free searches by voter's name. The CNPD admits that this is due to the lack of quality of the data that exists in the SIGRE system and in the electoral roll, which needs to be corrected. The development of systems, such as CED, that circumvents the problems of lack of quality in the databases, not only does not solve the source of the problem, but also helps to perpetuate it, tolerating it. This vicious cycle of adapting to incorrect data means that data are never truly corrected - which, strictly speaking, is an obligation of the data controller.

65. In fact, by analyzing logs from the CED_OBJ.LOG_EVENTO table, voter surveys were identified, carried out only with the indication of a voter's name (e.g. "Nuno", "Inês", "Luis", "tomas", "flora ", "amelia", "Pilot", "MANUEL", "Antonia", "Andreia", "Epifanio") - a search criterion that is clearly insufficient to guarantee a correct (and unambiguous) voter identification.

66. From the subsequent event recorded in the table, it is possible to state that those polls returned results, which would correspond to all voters who had one of these expressions in their full name. However, such a situation is contrary to the requirement of Article 25 of the GDPR, which requires the adoption of data protection mechanisms by default, since it allows access to more personal data than is necessary in this case. .

67. It is therefore essential that the BDRE be updated and, in the meantime, ensure that the poll by voter always implies, in addition to a name, the respective civil identification number.

iii. Duplication of personal data

68. As mentioned above, the CED support application consists of a web interface that allows access, in a distributed way, /.e., in which the various users access a centralized database at the SGMAI from different points.

69. SGMAI developed the CED system, which has several tables14 Having analyzed these tables, the CNPD raised doubts about the need for an auxiliary table (CED_OBJ.ELEICAO_ELEITOR_DADOS_AUX) when the database model already provided for a table for registration voter data (CEDJDBJ.ELEICACLELEITOR), which would correspond to a duplication of personal data. It was clarified that there was a need to temporarily store voter data while they were in the voting process and that the data would be deleted when the vote was terminated.

70. The existence of duplication of voters' personal data, given the principle of minimization provided for in subparagraph c) of paragraph 1 of article 5 of the GDPR, is only admissible if its indispensability is demonstrated. Not discussing the need to indicate voters who are, at any given moment, in the voting process, there are doubts that the solution found is the one that respects the principle of data minimization and data protection from conception and by default, as defined in Article 25 of the GDPR.

iv. Real-time knowledge by SGMAI of voters who are voting

71. In any case, it should be noted that through this solution, described above (in points 68 to 69), the SGMAI, therefore, a ministerial service, knows at all times, i.e., in real time, the identity of voters who are exercising the right to vote throughout the district of Évora.

v. Knowledge by SGMAI of voters who voted and those who did not vote

72. It should also be noted that the information of all voters who exercised their right to vote was recorded in a table called CEDJDBJ.VOTACAO. However, this table centralized in the SGMAI also allows this service to know the identity of citizens who exercised the right to vote as well as those who did not.

73. In addition, as with any other operation within the scope of electronic voting, there were no written rules regarding the use and destruction of the CEDJDBJ.VOTACAO table, responsible for registering all voters in the district of Évora who exercised the right to vote.

74. The CNPD was told that this table would be eliminated at the end of the publication of the data, on the third day after the vote.

75. The solution found of centralizing information on who exercised the right to vote in the MAI's General Secretariat, indicating themselves in the CED, allows this service, which obviously integrates the ministry and, to that extent and in legal terms, is

directed by the Minister of Internal Administration, knowing in real time the identity of

14 CED_OBJ.ELEICAO_ELEITOR; CED_OBJ.ELEICAO_ELEITOR_DADOS_.AUX; CED_0BJ.L0G_EVENT0; CED_OBJ.USER; CEDJDBJ.VOTACAO; and, CED_OBJ.VOTACAO_TIMELINE

Av. D. Carlos 1,134.1o T (+351) 213 928 400 geral@cnpd.pt

1200-651 Lisbon F (+351) 213 976 832 wwvccnpd.pt

votes and having at his disposal the table that allows him to know the identity - and the moment - of who exercised the right to vote and who did not exercise it.

76. It is not a question of questioning the impartiality of the holders of the executive body and of all those who, within the scope of the SGMAI, exercise the legally imputed functions, but it is nevertheless a matter of concern that sensitive information such as that relating to the identity of each citizen who votes, and who is voting at an exact moment, is directly aware of a ministerial service, therefore, hierarchically dependent on a minister.

77. In short, regardless of the degree of trust that we all place in the democratic system of the Portuguese State, it cannot fail to cause the greatest apprehension, regarding the act that constitutes the pillar of the functioning of democracy, that such sensitive information - with personal data of voters actually voting, and transmitted in real time - is available to an administrative service that is hierarchically dependent on a member of the Government, whatever the composition of the Government at each historical moment. Ensuring respect for the democratic rule of law requires, and cannot fail to demand, the definition of clear legislative rules that prevent any risk of distorting the principle of separation of powers, especially in the context of electoral processes.

saw. Intervention of third parties in place of members of the boards

78. With regard to the CED audit measures, the CNPD analyzed the CED_OBJ.LOG_EVENTO table and verified the existence of seven events recorded as "user impersonation", a term already mentioned in point 20. These events were compared with the minutes of the polling stations that would have triggered them. The contextualization of the events with episodes reported in these minutes was verified. The justification for these accesses resided in users' difficulties in accessing the CED.

79. It cannot, however, fail to be noted that a subcontracted private entity had access to the CED and that it discharged voters,

as voters, under an apparent delegation of powers by members of the board that has no provision or regulation in the law.

vii. Records of access to CEDs outside the electoral period

80. The logs of the application servers that supported the publication of the CED system interface were also analyzed. From this analysis, it should be noted that voter surveys carried out outside the opening period of the polling station were identified.

81. In fact, polls were carried out in the CED system on May 24, between 8:42 am and 4:36 pm, on May 25, between 6:39 am and 5:24 pm, and on the election day itself, May 26, from from 5:52 am.

__ W?

National Data Protection Commission

82. A possible explanation for such access would be to carry out tests of electronic voting, but it cannot help but be surprised that, nowadays, the practice of carrying out tests with real personal data persists. The CNPD has repeatedly insisted on this point, also with the Electoral Administration (cf. Deliberation no. 488/2009, of 1 July15), due to the risk that the tests may pose to the integrity of the database.

viii. System Auditability

83. Regarding this matter, it is also worth noting that the application servers were configured with circular logs (i.e., the oldest events are replaced by the most recent ones). However, given the high volume of accesses and consequently of logs, in the inspection carried out by the CNPD, the logs of the morning of the election day no longer existed on the application servers.

84. In an electoral process, it was essential that all election day logs were safeguarded, in the event that IPs (Internet Protocol) had to be identified, for example, in the event of an external attack.

85. This obviously calls into question the auditability of the system.

86. Finally, the process of attribution by the SGMAI of access credentials to the CED and electronic voting machines to each chairperson on election day does not comply with basic security principles, since, even if generated randomly, the credentials are unalterable by the president, thus being known to the SGMAI.

87. Furthermore, by handing over the exact same credentials to the vice-president, any possibility of, in an audit or inspection of the voting system, being able to conclude who specifically accessed the CED and, above all, the voting machines electronic

voting, with evident damage to democracy.

B. Impact Assessment on Data Protection

88. The main obligation of those who process personal data is to verify in advance, and be able to demonstrate, that it respects the principles and rules contained in the legal regime of data protection, in particular the RGPD - cf. Article 5(2) of the GDPR.

89. In a treatment of this nature, which covers a wide universe of data subjects and which implies the use of technology in a new context and with a special impact on the exercise of the fundamental right to vote

15 Available at httDs://www.cnpd.ot/media/oikixadw/20 488 2009 d.pdf

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

f

and, therefore, with an impact on the functioning of democracy, the duty to carry out the impact assessment on the protection of personal data provided for in paragraph 1 and in paragraph 3 b) of article 35 of the GDPR

90. It is important, first of all, to point out that the security measures suggested by the CNPD in the Deliberation on the Privacy of Voters in Electronic Voting, already mentioned, were adopted. But, taking into account that such recommendations date back more than a decade, the technological evolution that has taken place in the meantime and the change in the legal regime for the protection of personal data cannot fail to oblige the person responsible to carefully investigate the risks and vulnerabilities of the system. electronic voting system and its weighted assessment.

91. It is therefore regretted that the data protection impact assessment (AIPD) was only carried out on May 17, 2019, after a request by the CNPD, therefore, a few days from the execution of the treatment, when its function is precisely to help the person responsible to detect possible risks to the rights of data subjects and, by applying the precautionary principle, to adopt

the necessary measures for their elimination or mitigation.

92. It is further regretted that the document presented represented the mere fulfillment of a formality, without reflecting a real assessment of the risks and the identification of the measures adopted to correct them, bearing the curious result of all the risks listed being qualified as "not relevant "; above all, when it does not include the risks and vulnerabilities detected, as stated by the SGMAI, in the report prepared by the Judiciary Police.

93. In fact, the IAPD presented did not analyze all the processing of personal data that this face-to-face electronic voting system entailed, in particular the new processing operations; the electoral process was not analyzed until the moment of the vote, and therefore there was no analysis, nor evaluation, of the guarantees of anonymity or confidentiality of the vote; there does not appear to have been an effective analysis, nor justification provided, for the claims that each identified risk is "acceptable" - this impact assessment clearly does not meet the requirements of Article 35(7) of the GDPR. And this conclusion is reached without the need to transcribe what was declared here, for example, regarding the lawfulness of the data processing - invoking laws that the electronic voting process cannot, at all, comply with (as will be shown below). will explain16) - and the requirement of transparency of treatment, which would allegedly be fulfilled by the publication of electoral laws, which are silent as to the new operations of processing of personal data that this voting process implies.

16 Cf. below, points 96 to 101.

94. It is reiterated: the impact assessment is a legal instrument that aims to help those responsible for the treatment to comply with legal requirements, so the presentation of a document that does not reflect a real investigation and consideration of risks and measures is of little use. however adopted. Failure to do so while the technical solution for carrying out the treatment is being designed and, in particular, carrying it out without a significant period of advance in relation to the date of execution of the treatment, proves to be useless in terms of compliance with the obligations imposed. either by article 35 or by article 25 of the RGPD and, in these terms, it is reflected in the non-compliance with this legal regime.

95. 0 which is all the more serious as it would be essential in relation to a processing of personal data carried out by an

administrative body without legal or regulatory norms that safeguard the rights and interests of data subjects.

v. Conclusion

The. Lack of legal regulation of the in-person electronic voting system

96. The only legislative rule that supports the use of the electronic voting system is Article 8(1) of Organic Law No. 3/2018, of 17 August, which recognized "In the next electoral act for the European Parliament, [to] the electoral administration of the General Secretariat of the Ministry of Internal Affairs" the possibility of implementing, "on an experimental basis, face-to-face electronic voting, in at least 10 national councils"] and the only regulated aspect regarding such a system is the determination, in the final part of that provision, that votes are counted in the tabulation of results.

97. Therefore, nothing else was regulated regarding the electronic voting system, and the other pieces of legislation that regulated the electoral procedure were clearly not adequate to regulate electronic voting17.

98. In an effort, at the administrative level, to comply with the mandate of Article 8(1) of Organic Law No. 3/2018, of 17 August, and in view of the failure of the national legislator to regulate the procedure electronic voting, a procedure was in fact adopted that did not comply with the legal regime then in force.

99. The option for the creation, in fact, of a procedure that combined procedures foreseen in legal rules regarding early voting and voting by residents abroad, was not accompanied by any formalization of the applicable legal rules.

17 Just think, for example, of the impossibility of complying with the legal duty to display the number of voters, number of voters and electoral results by polling station, since the electronic voting system refers to the universe of all voters.

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

100. Even if the non-approval of an administrative regulation is explained by the fact that this is a matter reserved for the legislative competence of the Assembly of the Republic, under the terms of article 164 of the Constitution of the Portuguese

Republic, it is difficult to understand that, with this constitutional framework , if it had opted for de facto administrative actions without any written definition of precise and detailed guidelines.

101. Thus, the most basic principles inherent to the democratic rule of law are violated, disregarding the principles of predictability and transparency of the electoral process, by promoting informal administrative action in a matter in which the activity of the Public Administration is exhaustively and exhaustively regulated by law, leaving those who had the task of executing the procedure on election day and on subsequent days left to their own discretion and to impromptu solutions, not coincident in all polling stations18.

102. With regard specifically to the legal regime for personal data, in addition to the creation and use of CEDs without foundation in law and without regulation of the respective processing of personal data, the fact that articles 25 were not materially complied with .° and 35.° of the RGPD, as well as the failure to adopt adequate security measures in the transport of electoral rolls, thus promoting the risk of personal data breach (due to improper access or loss of data).

B. secret of the vote

103. It is important to emphasize that, following the analysis of the databases of the in-person electronic voting system, no evidence was found that the electronic voting system implemented for the 2019 European Parliament Elections made it possible to relate, in the voting machine, identification of the voter with the direction of the vote.

104. However, there were circumstances in the electronic voting process - foreseen in the documents indicated above, in point 21 - that prejudice the guarantee of anonymity of the vote.

105. In fact, in situations where the voter was unable to print the cast vote (most of the time, because the printer ran out of paper), the president of the polling station had a mechanism to give a new order for printing the vote. .

18 This was verified, for example, in the writing of the minutes by the polling stations: in the absence of rules regarding the relevance, and consequent duty of recording, of different incidents during the electronic voting process, only a few register the fact that the paper in the printer, although the system logs show that the same happened on other tables. This is a pertinent fact, as it implies the reprinting order by the president, which makes it possible, as will be explained below, to know the voter's vote.

106. This mechanism makes it possible for the presiding officer to always reprint the last vote, i.e., reprint the vote of the citizen who has just voted. What, in the limit, allows the chairman of the board to know the direction of the vote of the electors.

III. In-person electronic voting and the personal data protection regime

107. In addition to the case-by-case analysis of a particular face-to-face electronic voting system in the context of an experimental operation, it is also important to systematically consider the use of electronic means of voting at the borders of the personal data protection regime, as well as the creation and use of Cadernos Dematerialized Electoral Offices (CED).

108. In this regard, it is pointed out that the changes introduced in the Law on Electoral Census by Organic Law No. 4/2020, of 11 November, to finally give the CED a legal framework, did not contribute to the certainty and legal certainty in the processing of personal data19.

109. In fact, the new paragraph 2 of article 58 of the Voter Registration Law assumes that there is a difference between "electoral records in electronic format" and the CED. Since article 58,°-A, introduced by Organic Law No. 4/2020, defines the CED as "electoral records in electronic format based on information from the registrations contained in the BDRE and include all voters with electoral capacity for each election or referendum'.

110. In other words, the CED are distinguished from the "electoral registers in electronic format" only in that the former include all voters with electoral capacity for each election or referendum, unlike the electronic format registers, which are organized by constituencies (see article 53 of the Voter Registration Law).

111. Apart from the provision of its existence («provided that the necessary technical conditions are met») and the specification of the possibility of downloading votes, nothing else is regulated regarding the processing of personal data that the CED presuppose. It should be noted that, by their nature, the CED cannot respect, in their creation and use, most of the rules relating to census records provided for in the Law on

19 One cannot fail to point out and regret that a diploma that regulates the processing of personal data with the relevance that it has for the Portuguese democratic system, such as the Law on Electoral Census, is once again subject to legislative changes with right in the fundamental right to the protection of personal data without the political-legislative power having requested the CNPD's pronouncement, under the legally established terms.

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

r

Electoral Registration, as manifestly and exemplified by Article 52(2), Article 53 or Article 55.

112. Therefore, the regulation of CEDs, which is essential, is still not found in the electoral legal regime, under penalty of continuing to verify all the situations indicated above, in points 62 to 87.

113. The omission, or insufficiency, of legal regulation on CED is incomprehensible in a matter in which the transparency of personal data processing operations is essential, in order to provide predictability and legal certainty to the electoral process.

114. In addition to the issue of legal regulation of the processing of personal data within the scope of the CED, the CNPD believes, in order to contribute to a more adequate legal regulation of electronic voting systems, it should then systematically assess the use of electronic means of voting in the light of the personal data protection regime, and this, naturally, without prejudice to the powers of the sovereign bodies that may determine their use, as well as the entities controlling the legality of electoral processes - in the Portuguese case, the Commission National Elections and the Courts.

115. However, in terms of the protection of personal data, and because we are dealing with data included in the special categories of data20, the structuring principles that condition the performance of any processing are known and are currently listed in Article 5 of the GDPR. We refer to lawfulness, loyalty and transparency; limitation of purposes; data minimization; to its accuracy; the limitation of conservation; and integrity and confidentiality (not to mention the innovative principle of responsibility introduced by paragraph 2 of this article).

116. It is therefore with reference to those principles that the appropriate use of these means will be analyzed below.

i. Lawfulness, loyalty and transparency

117. To ensure compliance with this principle, the data controller must limit himself to what is permitted by law, ensuring that the data subject is perfectly aware of the operations that affect his personal data.

118. In this context, at first sight, we would consider the dimension of legality to be fulfilled, since it would be enough for the intervention of the Assembly of the Republic to guarantee this option, legislating accordingly. But it is not

20Cfr. Article 9(1) of the GDPR and Article 35(3) of the CRP.

sufficient that the diplomas that deal with the electoral processes that take place in Portugal foresee this means as legally admissible for the exercise of the vote.

119. In fact, it is important, from the outset, to define what type of electronic voting is intended to be enshrined in the law - in person voting (e-voling) or remote voting (i-voting) - and to regulate concretely and exhaustively the electoral process that frames the exercise of voting rights.

120. It should be recalled that, in Portugal, this possibility does not apply to all electoral processes without distinction, since voting in elections for the President of the Republic has a constitutionally established discipline. In paragraph 3 of article 121 of the CRP, it is established, beyond any doubt, that «The right to vote in the national territory is exercised in person>. This means that, except for a constitutional revision that modifies the precept, only the vote of Portuguese residents abroad can be exercised in a different way in terms of location, although it can be admitted that the alteration of the precepts of Decree-Law No. 319-A/ 76, of 3 May, in its current wording, would be sufficient to allow the use of electronic means in face-to-face voting.

121. In any case, the issue of transparency listed in Article 5(1) of the GDPR has to be read in the light of the possibility that data subjects (read "voters") can understand, in a complete (although not exhaustive), how the processing operations that affect your personal data take place, among which is the vote.

122. This question was, moreover, the subject of a decision by the German Federal Constitutional Court21 (German TC), which considered the use of a face-to-face electronic voting system unconstitutional whose popular union was not proven. In short, the court considered that the system did not allow a complete understanding of the process by which the voter's vote is expressed, counted and confirmed without the citizen having specific knowledge regarding the technological process by which this process takes place. In addition to this dimension of transparency, linked to the public nature of the elections, the factor of

potential risks in terms of electoral fraud committed through technical means or in terms of programming errors only possible in an electronic environment makes, from the court's point of view, necessary to existence of special precautions to safeguard the democratic principle underlying elections.

123. Without this meaning the denial of the use of these means, the judgment of the German TC led to a complete regression in the implementation of electronic voting systems in that country. This tendency to match the level of transparency and apprehension needed between the paper and electronic electoral process makes

21 Bundesverfassungsgericht, Second Senate Judgment of March 3, 2009 - 2 BvC 3/07 -, para. 1-166, available (in English) at http://www.bverfa.de/e/cs20090303 2bvc000307en.html.

Av. D. Carlos 1,134,10

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

gerai@cnpd.pt

www.cnpd.pt

It is frankly difficult to introduce means whose functioning depends on a minimum of knowledge to understand how one passes from the moment of the expression of the vote to the conclusion of the process, which includes the sequential phases of counting, investigation by the tabulation stations, until the publication of the final results .

124. It could be argued that the expression of the vote is already a moment in which anonymity prevails, with no personal data, but this lacks full confirmation and competent technical support to guarantee it, being also one of the moments whose understanding should be easily grasped by voters.

ii. Limitation of purposes

125. This principle is linked to one of the essential constraints for the protection of personal data. Basically, its translation reflects the need to limit the use of personal data to the purposes for which they were collected. Such purposes must necessarily be determined (specific), explicit (uncontroversially declared) and legitimate (which rules out illicit or abusive purposes).

126. Now, if no comments are offered on the determinability and explicit character of the purpose of the electronic vote, as for the legitimacy some considerations should be noted.

127. It should be noted that the motivation for introducing additional technology and, concomitantly, processing additional personal data for a given purpose must be guided by a rigorous consideration of its usefulness and indispensability. In fact, useless or redundant personal data should not be processed, because any additional operation on that information represents an additional interference with a fundamental right and is a factor of an almost automatic increase in the risk to its integrity.

128. That is why the legitimacy of the purpose should not be determined only by reporting to those who intend to process personal data, but rather and primarily on the reason for this operation.

129. And the use of face-to-face electronic voting appears as an operation of dubious legitimacy when faced with the traditional option of voting on paper. It is not ignored that the use of these means can speed up the reporting of results of electoral acts, since the counting of votes is carried out immediately. However, it is necessary to consider whether or not there should be, apart from the electronic counting of votes, another one, as it currently exists, in which a meeting dedicated to it, inspects and verifies, a posteriori, all reported incidents and decides on what resolution to give them. In the pilot project, the Electoral Administration (SGMAI) chose to implement a model in which the vote, in addition to being electronically validated, was still (and

well) supplemented by a copy of the bulletin printed by the voting machine (ECO) so that the voter could confirm their choice, placing this proof in a ballot box specifically created for this purpose. The legislative option taken regarding the validation of results by reference to the votes registered electronically, instead of the option for those placed in the ballot box, within the scope of a pilot project, is debatable, but the determination not to proceed with the confrontation between the electronically recorded votes and a paper copy thereof, at least as a sample.

130. Even so, it is recognized that this objection conflicts with the specific role of the authorities that ensure the regularity of electoral processes22.

131. The use of these electronic voting systems should, therefore, be based on criteria of indispensability and on the proven

benefits resulting from the substitution of paper votes. And this indispensability is far from being uncontroversial, especially in face-to-face electoral processes (is the greater speed in the calculation of results reason enough to opt for these means and accept the risks they entail?).

132. This mention of face-to-face processes does not want to legitimize an even more radical option for voting through electronic means at a distance. Also because, in this domain, there are several recommendations for its non-use. At this point, it is worth remembering that, in 201623, the Venice Commission - European Commission for Democracy through Law, consultative body of the Council of Europe - maintained that only in-person voting ensures that the vote is personal, since the guarantees of identity recognition associated with mobile voting (postal or over the Internet) do not extend to the non-transferability of voting credentials.

133. In addition, only face-to-face voting guarantees the freedom to vote at the time of its exercise, since in remote voting no guarantee is offered against the possibility of the voter being coerced when exercising his right.

134. In summary, it is concluded that the legislative option should not disregard other fundamental rights, nor the legal regimes specifically applicable to them, as provided for in the GDPR.

22 In Portugal, the National Elections Commission (CNE) and the Courts. For this purpose, see the CNE opinion, available at httDs://www.parlamento.Dt/ActividadeParlamentar/Paoinas/DetalheIniciativa.asox?BID=41351.

23 At the April 2016 conference (Bucharest).

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

iii. data minimization

135. The aim here is to ensure the proportionality of the use of personal data, both in terms of the universe that is intended to be collected and of the actors who may access them.

136. In the Portuguese case, there is a wide range of information dealt with under Law no. 13/99, of 22 March, in its current wording, with Article 12(1) listing a wide range of of data that must be included in the Electoral Census Database. In any case, as this list stems from the legitimate option of the legislator, it will be, above all, necessary to guarantee the security of information (which we will return to) and limit its knowledge to the people who have the duty to manage, change and consult that information.

137. As noted in the CNPD's analysis of the voting process in the 2019 pilot project (see above, points 64 to 67), the possibility of carrying out searches based on a single name resulted in the return of information on sets of voters in nothing related to the citizen object of the research. This is an example where the present principle seems to suggest a narrowing of the consultation possibilities through the obligation to use, at least, the civil identification number.

iv. Accuracy

138. With regard to the exercise of the right to vote, and by virtue of its essentiality in the architecture of democratic systems such as the Portuguese one, it is essential to ensure that the information contained in the voter registration files is up-to-date.

139. The use of electronic voting does not have significant impacts within the framework of this principle, since it is upstream that the operations of updating the databases must take place, avoiding the evasion of this right to voters, guaranteeing the uniqueness and, at the same time, ensuring that those who cannot vote do not do so (in case of errors or fraud). In any case, concerns about information security and the correctness of all phases of the electoral process, from the registration to the calculation of the final results, are also taken into account here, avoiding the intrusion of third parties and the alteration, tampering or corruption of information by third parties or by the system itself.

v. Conservation limitation

140. In this context, the law determines the information retention periods24, and it is important that the electronic systems supporting the electoral process or on which this process is based (if only electronic voting is used) scrupulously comply with what is defined.

141. It should be borne in mind that electronic voting systems are very different, so the definition of the information retention periods should not depend on the nature of the systems used, but on the essentiality of maintaining information for the determination of electoral results.

142. As noted in the evaluation of the pilot project, the inconsistencies between what had been declared and what was actually in the system (duplication of tables - cf. supra, points 69 and 70) is a factor of concern and undermines the compliance with principles such as the limitation of conservation, but above all it can give rise to the existence of duplicated and non-validated information, as well as to improper access and potential biases of these initially unknown sources of information.

saw. Integrity and confidentiality

143. The greatest concern of any citizen and of any person responsible for the electoral system will reside here - to provide for the «security [of information], including protection against its unauthorized or unlawful treatment and against its accidental loss, destruction or damage, adopting appropriate technical or organizational measures> - cf. Article 5(1)(f) of the GDPR. If it is true that traditional (paper-based) voter registration systems are not immune to fraud, it is no less true that their use over several decades (if not, centuries) made it possible to know their weaknesses and build an electoral system where existing safeguards25 are capable of guaranteeing a very high level of security.

144. On the other hand, the use of technological means in the expression of popular vote presents new and perhaps insurmountable challenges26 that must be addressed before the introduction of these novelties.

24 As an example, see what is provided for in paragraph 2 of article 104 of Law no. once these have been definitively decided, the judge promotes the destruction of the bulletins».

25 Such as the structuring of polling stations, the presence of delegates from the different candidacies and international observers, the review of results and even the repetition of elections.

26 For a summary approach to these risks, see https://epic.orQ/cvbersecuritv/election/. And as for the guarantee of this robustness, again, reference is made to the investigation of Andrew W. Appel, cited above note 11.

Av. D. Carlos 1,134.1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

145. Remember that, all over the world, cases of failure in the implementation of electronic voting27, face-to-face and non-face-to-face28 were known, many of them linked to the security weaknesses detected, which called into question fundamental dimensions of the democratic process , including voting secrecy, a factor in which the right to protection of personal data is fundamentally affected. As mentioned by Boehme-NeBler29, «privacy is (...) a psychological and anthropological necessity», precisely adding that «free thought is the foundation of free societies. It is not surprising, therefore, that the secret ballot is an important instrument of democratic elections - and a symbol of democracy. It guarantees that people can vote freely and autonomously without being observed, coerced or intimidated".

146. Integrity and confidentiality must, therefore, be understood in their broadest dimension, encompassing all the moments in which the electoral process takes place, from the electoral roll, to the counting, passing, of course, through the specific moment when the right to vote is exercised. And its implementation cannot dispense with the use of the concepts and guidelines provided for in article 32 of the GDPR.

IV. Non-face-to-face electronic voting and the personal data protection regime

147. As per article 8 of Organic Law No. 3/2018, of 17 August, the pilot project was limited to face-to-face electronic voting, although its no. «Within 12 months, (...) to carry out the studies and steps necessary to enable the Assembly of the Republic to legislate on the introduction, in cases where the vote is exercised by correspondence, of electronic non-face-to-face voting with validation of identity via digital mobile key or equivalent electronic identification means-'. As far as the CNPD is aware, this last modality of electronic voting has not seen developments since the date of the 2019 European Parliament elections, even though Organic Law No. amendments to the laws that govern the main electoral acts and procedures at the national and local levels.

27 The report contained in the European Parliament Research Service document «Digital technology in elections. Efficiency vs. Credibility', (available at https://www.europarl.europa.eu/ReaData/etudes/BRIE/2018/625178/EPRS BRIÍ20181625178 EN.pdfl. where it is observed that European countries either did not adopt these systems, or, having adopted them, decided to reverse this decision,

abandoning their use.

28 See the study (white paper) of the International Foundation for Electoral Systems (IFES) Considerations on Internet Voting: an

overview for Electoral decision-makers, available at

https://www.ifes.orQ/sites/default/files/considerations on internet voting an overview for electoral decision-makers.pdf.

29 Volker Boehme-NeBler, «Privacy: a matter of democracy. Why democracy needs privacy and data protection', in International Data Privacy Law, V. 6, no. 3, 2016, pp. 222-229.

148. Although this opinion has been briefly and atomized, it is worth mentioning the possible introduction of the remote electronic voting modality, using the Internet (i-voting).

149. Notwithstanding the aforementioned incompatibility with the constitutional norm that prevents remote voting30, it is important to highlight the particular risks posed by the use of non-face-to-face electronic voting. And specifically to point out the challenges that arise in terms of protection of personal data and which are also reflected in the essential core of safeguarding electoral processes - the free and correctly counted vote.

150. As mentioned above, the freedom to vote is only fully guaranteed in face-to-face voting, since, in cases of remote voting, there is no guarantee, from the outset, that the voter is not being coerced.

151. If such mention were not enough to discourage this type of voting, the white paper of the International Foundation for Electoral Systems (IFES), of April 202031, is clear about the failure of electronic voting over the Internet to stimulate popular participation, giving as an example the cases of Estonia and Norway, where the problem of abstention remained substantially unchanged after the adoption of these alternative means.

152. Accepting the premise (also advanced in the study we have just cited) that the introduction of technologies in electoral processes must find its justification in the resolution of a previously identified issue or problem, it is not clear what the difficulties are. they aim to overcome with the potential use of remote electronic voting. Understanding the particular situation of nationals residing abroad, where physical distance from polling stations is, not infrequently, an obstacle to the fulfillment of a

civic duty and fundamental right, it will also be necessary to consider whether this is the best solution. for a situation that will deserve specific answers32, even in the light of the conclusions already pointed out by the Venice Commission and cited by the CNE.

153. Reference has already been made to the view that organizations specifically devoted to reflection on electoral processes have expressed on some of the critical aspects associated with them. Among them, it is important to highlight, as it directly and necessarily involves the processing of personal data, the criterion of personality.

30 Cf. As for presidential elections, art. 121, of the CRP.

31 Cf. the aforementioned Considerations on Internet Voting: an overview for Electoral decision-makers

32 In the case of France, the news that became public show that the use of this method has been abandoned due to security concerns (https://www.reuters.com/article/us-france-election-cvber/france-drops

-electronic-votina-for-citizens-abroari-over-cvbersecuritv-fears-id[JSKBN16D233).

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

154. This criterion is only fully guaranteed by the presence of the voter at the polling station or, when at a distance, it can only be ensured with specific technological conditions that are not, from the outset, intelligible, nor above all accessible to the general population.

155. It is now intended to address the risks associated with the introduction of this option, taking into account the history of its (embryonic) use in some countries.

156. The first risk is of a formal nature and relates to the degree of legal certainty that can be built up through national legislation. As noted by Driza Maurer33, «As demonstrated by the experiences of several countries (USA, Germany, Netherlands, France, etc.), the inherited regulation of mechanical or low-tech solutions is not appropriate to regulate digital,

even when it has been improved»34. This also means, in Portugal, that legislation that limits itself to stating that «machines [or automatisms] may be used as long as the secrecy of the vote is guaranteed» (Article 35 of the German Federal Electoral Law)35 36 will not comply with the requirements minimum requirements to fully frame the introduction of technological means in electoral processes.

157. This aspect of the formality of introducing adequate legislation represents only the first (albeit indispensable) step towards safeguarding compliance with electoral principles and the protection of personal data in the electoral act.

158. Added to this is the finding that the degree of maturity of remote electronic voting solutions may not be, even today, enough to prevent disproportionate risks and, above all, increased and insurmountable when compared to traditional face-to-face voting .

159. It has already been expressed, and here it is reaffirmed, the need to match the introduction of new technologies to the resolution of duly identified concrete problems, since «introducing technologies just for the appearance of modernity generated by the electorate is not recommended»35. However, in the Portuguese case, only the vote of emigrants can justify the consideration of this hypothesis and, even so, concretely equating the advantages and risks to democracy arising therefrom - and only if specific security measures capable of guaranteeing confidentiality and the integrity of the vote.

33 Ardita Driza Maurer, «Digital technologies in elections - Questions, lessons learned, perspectives» (2020), available at https://edoc.coe.int/en/elections/8956-eDub-diaital-technoloaies-in-elections- questions-lessons-learned-DersDectives.html.

34 Idem, op. cit, p. 20.

35 also.

36 Id, ob. cit, p.16.

160. The truth is that suitable technical studies37 always seem to return a non-negligible degree of risk, regardless of the solutions adopted. Furthermore, the conclusion appears to be constant that it is not possible to guarantee the total security of a remote voting operation (either by post or via the Internet).

161. In this context, among the main problems related to the protection of personal data, highlights the «impossibility [or, at

least, great difficulty] of maintaining the separation of the identity of voters and the votes cast by them when the act of voting takes place via the Internet»38. In fact, from the analysis carried out in 2016, in the United States of America, it is evident the distrust of multiple official entities regarding the inviolability of votes expressed in this way and the ability to guarantee the anonymity of voters. For this reason, the US Department of Homeland Security and the US Department of Defense concluded that it was not advisable to use the Internet to vote, even in the case of military personnel who are regularly deployed in locations other than those in the census39.

162. Even in countries where the adoption of remote voting by electronic means is generally considered to be successful, technical assessments have shown that the risks remain and cannot be ignored, with conclusions indicating that potential threats of interference from third States , or individuals (external or internal to the body responsible for the electoral act) can overcome either technological or procedural controls in order to manipulate the outcome of the elections40.

163. It should be noted that the introduction of highly complex technological means leads, at the same time, to the reinforcement of human, technical and financial resources which, in addition to the possible burden they represent for the State, imply a decreasing perception on the part of voters about how the the voting process; in fact, the lack of transparency and predictability of the processing of personal data involved in these operations generates a lack of trust on the part of voters in the electoral system.

164. The combination of risks - of information security (and with it of its accuracy), threat to anonymity and deficiency or unintelligibility of existing information - necessarily endangers a

37 Cfr., at this level, the study by Véronique Cortier /Joseph Lallemand / Bogdan Warinschi, Fifty Shades of Ballot Privacy: Prívacy against a Malicious Board (2020), available at https://eprint.iacr.ora/2020/127. ddf

38 Caitriona Fitzgerald / Ramela Smith / Susannah Goodman, The Secret BallotAt Risk: Recommendations for Protecting Democracy ("2016), p. 5, (study developed on behalf of, respectively, the Electronic Privacy Information Center, Verified Voting Foundation and Common Cause Education Fund,) available at https://secretballotatrisk.org/Secret-Ballot-At-Risk.pdf

39 Cf. "Appendix I, The Risk of Internet Voting" from The Secret Base at Risk: Recommendations for Protecting Democracy, cited in the previous note

40 Cfr. Drew Springall /Travis Finkenauer / Zakir Durumeric /Jason Kitcat / Harri Hursti / Margaret MacAlpine / J. Alex FHalderman, Security Analysis of the Estonian Internet Voting System, p. 11, available at

https://dl.acm.om/rioi/10.1145/2660267.2660315

Av. D. Carlos 1,134,1st

1200-651 Lisbon

I (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

set of crucial dimensions linked to the basic principles of data protection, namely: lawfulness, loyalty and transparency; of accuracy; of integrity and confidentiality.

165. The lack, firmly assumed and scientifically proven, of the reliability and robustness of remote electronic voting systems is, therefore, an obstacle that appears, at the present moment, as insurmountable or, at the very least, strongly discouraging the decision to embark on implementation of these means in the various electoral processes. Ignoring this fact can represent severe damage to trust in the democratic system, which is combined with the strong probability of violation of the fundamental right to the protection of personal data.

V. Conclusion

166. In addition to the conclusions specifically referring to the electronic voting system implemented in the 2019 European Parliament elections, highlighted above, in paragraphs 96 to 106, the CNPD presents the following final considerations regarding the possible use of electronic voting systems in future processes electoral.

167. The evaluation of the introduction of electronic means of voting in electoral processes in the light of data protection rules indicates the insurmountable need to carry out a consideration of the risks and merits that may result from it, first of all because special categories are at stake data, pursuant to Article 9(1) of the GDPR, also listed in Article 35(3) of the CRP.

168. Specifically regarding the Dematerialized Electoral Registers, the CNPD warns of the need for detailed regulation of the processing of personal data that their creation and use presupposes, since, apart from the legal rules that provide for their existence and the possibility of downloading of voting rights, that treatment cannot comply with the rules relating to the registration books provided for in the Law on the Electoral Census. The omission, or insufficiency, of legal regulation on the

CED is incomprehensible in a matter in which the transparency of data processing operations is essential, to provide predictability and certainty to the electoral process.

169. Given that the electronic electoral process is divided into several phases, it is also important to ensure, in all of them, effective supervision by independent entities, which implies ensuring, from the outset, the syndication of the information system (in particular, that the source code is auditable) and that those entities are equipped with the necessary technological knowledge for an efficient and effective inspection.

170. Now, if regarding the first phase - i.e., the one relating to the processing of personal data within the scope of electoral rolls - supervision is the responsibility of the CNPD, which has specialists in information technology and

communication, in relation to the phases of voting and counting of electoral results, it is essential to provide the CNE and the Courts with adequate technical knowledge for the control of electronic voting systems. In fact, as has been underlined by the doctrine and even by the Venice Commission, it is not enough for independent entities that supervise the electoral process to know the electoral law, it is still necessary to understand the functioning of the electronic process in order to verify the security, reliability and completeness, efficiency and technological robustness of electronic voting systems.

171. As the robustness of electronic voting systems is still controversial and relevant weaknesses were detected during the pilot project conducted in 2019, the CNPD recommends that any evolution towards the implementation of electronic voting be preceded by a rigorous prior scrutiny the technology to be used and the security measures (technical and organizational) envisaged. In this area, it is also essential, as defined in the RGPD, to conduct an effective and exhaustive impact assessment on data protection that allows for anticipating the challenges that may arise in safeguarding this fundamental right.

Approved at the meeting of March 16, 2021

Filipa Calvão (President)

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