□I

PAR/2022/41

1

B WEER

CNPD

National Data Protection Commission

OPINION/2022/50

I. Order

1. The Commission on Constitutional Affairs, Rights, Freedoms and Guarantees, of the Assembly of the Republic, submitted to the National Commission for Data Protection (hereinafter CNPD), for opinion, Draft Law no. 11/XV/1 .a (GOV), which "regulates access to metadata relating to electronic communications for criminal investigation purposes".

2. The CNPD issues an opinion within the scope of its attributions and competences as an independent administrative authority with powers of authority to control the processing of personal data, conferred by subparagraph c) of paragraph 1 of article 57, in conjunction with subparagraph b) of paragraph 3 of article 58, and with paragraph 4 of article 36, all of Regulation (EU) 2016/679, of 27 April 2016 - General Regulation on Data Protection (hereinafter, RGPD), in conjunction with the provisions of article 3, paragraph 2 of article 4, and paragraph a) of paragraph 1 of article 6, all of Law no. 58/2019, of 8 August, which enforces the GDPR in the domestic legal order.

II. Analysis

3. In accordance with Article 1 of this Draft Law, it «establishes the rules for access, for the purposes of criminal investigation, to data processed by companies that offer electronic communications networks and/or services» and «proceeds to the second amendment to Law No. 41/2004, of 18 August, amended by Law No. 46/2012, of 29 August [...]».

4. Understanding the need to access personal traffic and location data for criminal investigation and prosecution, the CNPD welcomes the intention to strike a prudent balance between, on the one hand, the public interest in public security and peace and, on the one hand, on the other hand, the fundamental rights to respect for private life, to informational self-determination and to the free development of the personality.

5. In particular, the concern expressed, in the explanatory memorandum of the Draft Law, with the serious and violent crimes committed by criminal organizations which, as highlighted there, "often resort to the Internet (namely the dark web) and to mobile telecommunications, under encryption and possible anonymity'. What cannot fail to be noted is that to monitor communications and collect evidence in the context of the dark web, the regime presented in this Law Proposal is of little or no use, because it is the nature of the dark web that, precisely, prevents the identification of the access destination, which is why it is necessary to use a software/browser to mask the communications. It is not clear, therefore, why the dark web is invoked to motivate the provision of a regime of access to personal data in the context of electronic communications that, clearly, does not allow the monitoring of communications; otherwise

as Law No. 32/2008, of 17 July, will not have allowed either. The same reasoning applies to the reference to the use of encryption technologies.

6. Still on the subject of the explanatory memorandum, it should be noted that there is already a legal regime regarding the collection and conservation of evidence in relation to crimes committed through a computer system - Cybercrime Law (Law No. 109/2009, of 15 September, amended by Law No. 79/2021, of 14 November) - for this reason, too, the content of this draft law does not appear to be founded.

7. In any case, in analyzing the regime of access to personal data relating to electronic communications proposed herein and its compliance with the Constitution of the Portuguese Republic (CRP) and the Charter of Fundamental Rights of the European Union (Charter), the CNPD it will be especially based on the arguments, conditions and limits explained by the Constitutional Court (TC) in the judgment 268/2022, of 19 April 20221, as well as in the judgments of the Court of Justice of the European Union (CJEU) Digital Rights Ireland2, Tele 23 and La Quadrature du Net4.

8. Bearing in mind the aforementioned jurisprudence, the option of creating a legal regime that does not provide for the generalized storage of personal data relating to traffic and location for the purpose of investigation and criminal prosecution is welcomed.

9. It is noted that the provision, for the purpose of criminal investigation, of access to personal traffic data stored by electronic communications operators for billing purposes does not, in itself, raise reservations. The purpose of criminal investigation and prosecution is in itself a purpose of public interest that can legitimize the reuse of personal data, provided that access proves to be adequate, necessary and not excessive in view of that purpose.

10. However, some of the solutions proposed go against the meaning of the case law cited above, reducing the guarantees of citizens' fundamental rights. It is on this point that the essence of the CNPD's assessment focuses.

i. The reduction of the fundamental guarantees of citizens

11. First of all, it should be noted that this Draft Law does not achieve the declared objective of ensuring a «prudent balance» between, on the one hand, the public interest in public security and peace, which justifies providing criminal police bodies and the judicial authorities of means of investigation and evidence

See https://dre.pt/dre/detalhe/acordao-trihunal-constitucional/268-2022-184356510

Judgment of April 8, 2014, procs. C-293/12 and C-594/12.

Judgment of December 21, 2016, procs. C-203/15 and C-698/15.

Judgment of October 6, 2020, procs. C-511/18, C-512/18 and C-520/18.

and, on the other hand, the fundamental rights of each citizen, namely respect for private and family life, informational self-determination and the free development of the personality.

12. In fact, in this Draft Law, there is a marked reduction in the guarantees of the fundamental rights of citizens, compared to the previous legal regime for the conservation and transmission of personal data relating to electronic communications, whatever was provided for in the Law No. 32/2008, of 17 July (on retention of data relating to electronic communications), or what is still provided for in the Cybercrime Law.

13. This decrease in the protection of fundamental rights causes the greatest perplexity, especially considering the context in

which the Draft Law appears: after the declaration by the TC of the unconstitutionality with general mandatory force of the legal regime of retention of data related to electronic communications , which did not offer adequate guarantees for the protection of those fundamental rights, and after successive decisions by the CJEU to point out the disproportionate violation of fundamental rights by the Union regime and by national legal regimes for the conservation and access to personal data relating to electronic communications.

14. In addition, this decrease in guarantees does not occur only in relation to a single aspect of the regime, but takes place on different planes, creating a strangling web of fundamental rights and freedoms. Let's see.

a, Access by judicial authorities

15. The reduction of fundamental guarantees occurs, from the outset, in terms of legitimacy and control of access to personal data relating to electronic communications for the purpose of investigation and criminal prosecution.

16. While in Law no. 32/2008, of 17 July, in paragraph 2 of article 3 and in article 9, access by the competent authorities (/.e., judicial authorities and criminal police authorities) by the investigating judge, to order or authorize the transmission of data, now, in this Proposal, the judicial authorities (therefore also the Public Prosecutor's Office, and the criminal police bodies, by delegation of generic powers , under Directive 1/2002, of 4 April, of the Attorney General's Office5) may access personal data without prior order from the investigating judge - cf. articles 2 and 3, no. 1, of the Draft Law. Moreover, at no point is there any provision for the intervention of the investigating judge.

5Accessible at https://files.dre.pt/2s/2002/Q4/0790000QO/0622106224.Ddf

17. Furthermore, the duty to provide detailed reasons for the request for access to data is not even imposed in the Draft Law, as provided for in Article 9(1) of Law No. 32/2008.

18. In this regard, it should be recalled that, according to Article 32(4) of the CRP, '[t]all instruction is the responsibility of a

judge, who may, under the law, delegate in other entities the practice of instructive acts that are not directly related to fundamental rights».

19. Bearing in mind that access to personal data relating to electronic communications, in particular to traffic and location data, entails a considerable restriction of the rights to informational self-determination and respect for private life and, in particular, freedom and free development of the personality, enshrined in articles 26 and 35 of the CRP, the absence of control by the investigating judge of access to such data has a direct impact on these fundamental rights and means a setback in their protection6.

20. It should be noted that even in the field of Cybercrime Law, where judicial authorities are entitled to access data or order such access, the intervention of the judge is safeguarded whenever the data collected may jeopardize the privacy of the accused or of third parties, under penalty of nullity of the evidence collected (cf. paragraph 3 of article 16 of the Cybercrime Law).

21. This legislative option is, therefore, of doubtful constitutionality, and raises the greatest perplexity, especially when the case law of the CJEU and the TC has persistently underlined the importance, in the judgment of proportionality, of the restriction of fundamental rights by virtue of access to data related to electronic communications, the legal provision of prior intervention by the judge.

22. Moreover, the European Court of Human Rights (ECtHR), in the Big Brother Watch judgment7, extends the presuppositions of a legitimate interception of electronic communications to the operation of access to data relating to electronic communications (cf. § 507). Thus, and as the TC summarizes in judgment 464/2019, of 21 October, the ECtHR establishes the following criteria for compliance of these measures with the right to respect for private and family life: "(7) the regime must comply with the law, in the sense that it is clear, accessible and predictable for citizens; (2) it must pursue a legitimate objective, (3) it must be necessary in a democratic society, being restricted to the fight against serious crime; (4) access must be subject to

6 The CNPD maintains the understanding, explained in previous opinions on this matter, that access to traffic and location data affects the content of the fundamental right to the inviolability of electronic communications, enshrined in article 34 of the CRP. However, for the sake of clarity of the exposition, in line with the recent TC ruling, the CNPD chooses not to focus, in this opinion, on the restriction of this fundamental right.

7 Judgment of May 25, 2021, complaints No. 58170/13, 62322/14 and 24960/15.

prior authorization decided by a court or an independent administrative body; (5) the law must provide adequate safeguards against arbitrariness».

23. The requirement for prior authorization by a court or an independent administrative entity implies that the need (and the stricto sensu proportionality) of access to such data is assessed by an authority that is not directly involved in the investigation, therefore, that is not either the one who wants to access the data or who directs the investigation. Hence the indispensability of a judge's intervention in this procedure.

24. For all these reasons, the CNPD recommends amending articles 2 and 3 of the Proposal, in order to provide for the need for an authorizing order from the judge to access personal data relating to electronic communications.

B. Expanding the catalog of crimes

25. But the reduction of fundamental guarantees for citizens is also manifested in the expansion of the catalog of crimes that justifies access to personal traffic and location data.

26. Contrary to the regime contained in Law No. 32/2008, of 17 July, which restricted the storage and transmission of personal data relating to traffic and location for the purpose of investigation, detection and prosecution of serious crimes (cf. paragraph 1 of article 1 and article 3, and also paragraph 1 of article 9), typified in subparagraph g) of paragraph 1 of article 2, the Draft Law defines a regime for the transmission of the same personal data for the investigation and prosecution of the following crimes:

i. provided for in paragraphs 1 and 2 of article 189 of the Criminal Procedure Code (CPP), therefore, in addition to the serious crimes provided for in subparagraph g) of paragraph 1 of article 2 of Law no. /2008, crimes punishable by a maximum prison sentence of 3 years;

ii. the crimes provided for in the Cybercrime Law, corresponding to computer crime with a degree of severity identified by a maximum prison sentence equal to or greater than 5 years (at least), with the exception of the crime of illegitimate access;

iii. «crimes committed by means of a computer system, provided that they are punishable with a maximum prison sentence

equal to or greater than 1 year».

Av. D. Carlos 1,134.1° 1200-651 Lisbon

T(+351) 213 928400 F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

27. In short, “crimes of terrorism, violent crime, highly organized crime, kidnapping, kidnapping and hostage-taking, crimes against cultural identity and personal integrity, against State security, counterfeiting of currency or securities equivalent to currency and crimes covered by the convention on the safety of air or maritime navigation" (which were provided for in Law no. others, crimes punishable with a maximum prison sentence of 3 years, as well as certain types of computer crime, depending on the respective criminal framework and all other crimes committed through a computer system, provided that they are punishable with maximum prison sentence equal to or greater than 1 year.

28. In other words, this Draft Law extends the purpose of accessing personal traffic and location data, in the context of the use of electronic communications, far beyond the provisions of Law No. 32/2008, and also going beyond of the provisions of the Cybercrime Law, including for crimes whose degree of censorship is manifestly low.

29. It would be unnecessary here to recall the relevance that the TC and CJEU jurisprudence has given, in the weighing of the rights and interests in tension with regard to access to personal traffic and location data, to the fact that access is limited to the investigation of the serious crime, as indicated in the Directive transposed by Law No. 32/2008. For example, the TC, in judgment no. 268/2022, cited above, states "[there seems to be no doubt that the investigation, prevention and repression of serious crimes, defined as "crimes of terrorism, violent crime, highly organized crime , kidnapping, kidnapping and hostage taking, crimes against cultural identity and personal integrity, against the security of the State, counterfeiting of currency or securities equivalent to currency and crimes covered by the convention on the safety of air or maritime navigation" (paragraph g) of no. 1 of article 2 of Law no. 32/2008) - purpose listed in no. 1 of article 1 of Law no. 32/2008 - assumes constitutional importance, as it aims to safeguard democratic legality and In fact, this was recognized in the Constitutional Court Judgment No. 420/2017 and is in line with the Court of Justice's conclusion, in the Digital Rights Judgment, according to which the fight

against serious crime and the terrorism are objectives of general interest of the Union (no. s41 to 43)".

30. In addition, in La Quadrature du Net (paragraph 167), the CJEU clarified that 'Member States have the possibility to provide in their legislation that access to traffic data and location data may, subject to the same substantive and procedural conditions, occurs for the purposes of combating serious crime or safeguarding national security when said data are kept by a provider in accordance with Articles 5, 6 and 9 or also with Article 15(1) of Directive 2002/58'.

31. At the same time, the ECtHR requires, in order to restrict the right to respect for private and family life, in this context, to be necessary in a democratic society, restricting itself to investigating and combating serious crime (cf. §§ 519 and 522 of the Big Brother Judgment Watch).

32. To that extent, the restriction of the rights to privacy, informational self-determination and the freedom of free development of the personality that access to traffic data always represents only appears to be proportionate if it has a view to investigation and repression of serious crimes, and no reasons were presented to justify the extension of the restriction of fundamental rights beyond what is already established in article 187 of the CPP and of the Cybercrime Law.

33. The legitimacy of access for the investigation of virtually any crime, regardless of its seriousness, in itself represents a disproportionate restriction of the rights to privacy, self-determination and the free development of the personality, in violation of no. 2 of article 18 and no. 1 of article 52 of the CRP; disproportionality that is accentuated by the joint provision of the possibility of access by the Public Prosecutor's Office without direct and prior control by a judge, as mentioned above.

34. Therefore, the CNPD recommends the elimination of paragraph c) of article 2 of the Draft Law.

ç. Expansion of personal data that are to be stored and accessed

35. And, on a third level, the Draft Law expands the categories of personal data that are to be preserved by operators that offer network and electronic communications services, changing the range of personal data provided for in Law No. 41/2004, of 18 August, amended by Law No. 46/2012, of 29 August - Law on Privacy in Electronic Communications.

36. In fact, under the pretext of updating the identification data of the equipment used, Article 8 of the Draft Law amends

paragraph 2 of Article 6 of Law No. 41/2004.

37. First of all, it is reiterated that the provision of access for the purpose of criminal investigation to personal traffic data stored by electronic communications operators for billing purposes does not, in itself, give rise to reservations. The purpose of criminal investigation and prosecution is in itself a purpose of public interest that can legitimize the reuse of personal data, provided that access proves to be adequate, necessary and not excessive in view of that purpose.

38. What already raises the greatest reservations is the legal provision for collection and conservation by operators of electronic communications of personal data that are not demonstrably necessary for the

billing purpose, but with the appearance 4dd?gkH8êigwf$pmento nes?^$in?fttesl&400 geral@cnpd.pt

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

PAR/2022/41

4v.

39. In fact, the range of subscriber and equipment identification data (basic data) initially provided for in Article 6(2) of Law No. 41/2004 is now introduced, in subparagraph a), various data, of which the IMSI (international identity of the mobile subscriber) and the IMEI (international identity of the mobile equipment) stand out. And here, without specifying whether the IMSI and IMEI are just those of the subscriber.

40. And, to the range of traffic data provided for in subparagraphs b) and c) of paragraph 2 of article 6 - 'total number of units to be charged for the counting period, as well as the type, start time and duration of calls made or the volume of data transmitted" and "date of the call or service and number called", respectively -, the data relating to the "associated date/time group" are now added (cf. the wording of point c) of Article 6(2) now proposed).

41. In addition, with regard to traffic data relating to Internet access, 'telephone number, IP protocol address used to establish communication, port of origin of communication, as well as the data associated with the start and end of Internet access" (cf. new subparagraph d) introduced by the Proposal in paragraph 2 of article 6).

42. Now, among this new list of personal data relating to electronic communications that is intended to be introduced in paragraph 2 of article 6 of Law no. 41/2004, there are data whose legal provision is, prima facie, unnecessary.

43. This is, of course, what happens with some data whose insertion seems redundant, as they are already provided for in paragraph 2 of article 6 in its current wording: the telephone number, provided for in the new subparagraph d), as it is already

included in the identification data listed in subparagraph a); and the data relating to the associated date/time group, since, if this expression is correctly interpreted, such data are already provided for in the current paragraphs b) and c) of the aforementioned precept (specifically, «type, start time and duration of calls made' and 'call date').

44. However, there are other data whose insertion in that rule proves to be unnecessary for the purpose of invoicing, and therefore their prediction is not admissible in this headquarters. This is clearly the case for traffic data, provided for in the new subparagraph d), relating to the beginning and end of access to the Internet: the "conservation of the volume of data transmitted" (already provided for in subparagraph b) of paragraph 2 of article 6 of Law no. 41/2004) seems to be sufficient for billing purposes, and it is not necessary to know the beginning and end of this access.

45. As for the forecast for the collection of the IMEI, in the new wording proposed for subparagraph a) of paragraph 2 of article 6, the need for its treatment in the context of the execution of the contract for the provision of the electronic communications, there remains serious doubt as to whether it is necessary for the purpose of

invoicing or payment for services provided, which is, remember, the purpose for which Article 6(2) of Law No. 41/2004 allows for the storage of traffic data.

46. As the need for such personal data for this specific billing purpose has not been demonstrated, any legal rule that provides for its collection and conservation for that same purpose represents a disproportionate restriction of fundamental rights to respect for private and family life, to free development of personality and informational self-determination, in violation of paragraph 2 of article 18 of the CRP and paragraph 1 of article 52 of the Charter, and specifically of the principle of data minimization, enshrined in subparagraph c) of the Article 5(1) of the GDPR.

47. It appears, therefore, that the retention of personal data for the purposes of criminal investigation is being imposed, under the guise of data necessary for the billing of the electronic communications services provided.

48. It should be noted that the TC jurisprudence does not make it impossible for the national legislator to impose on electronic communications operators the generalized retention of 'base data' of their customers (according to the concept adopted by that court) for the purpose of criminal investigation - here it is understood that "[t]he basic data refer to the connection to the

network, independently of any communication, allowing the identification of the user of a certain equipment - name, address, telephone number" (cf. point 6.1. of the judgment no. 268/2022). To the extent that it is understood and demonstrated that it is appropriate and necessary for the criminal investigation to retain more detailed equipment identification data than those required for invoicing and payment for electronic communications services, therefore, nothing prevents the national legislature provides for it on that specific basis8. But this Draft Law does not assume such an intention, rather considering such data as justified in the context of invoicing and payment of electronic communication services, without, however, demonstrating the need for the same for that same purpose.

49. For the rest, everything that is already included in the concept of traffic data - "the functional data necessary for the establishment of a connection or communication and the data generated by the use of the network (for example, user location, recipient location, duration of use, date and time, frequency) {...c]are, therefore, elements already inherent to the communication itself, insofar as they make it possible to identify, in

8 Cf. points 17.1. and 17.2 of the judgment of TC No. 268/2022; and points 152-159 of the judgment in La Quadrature do Net of the CJEU, which, in essence, allows, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, a generalized and undifferentiated conservation of the IP addresses assigned to the source of a connection, for a period limited to what is strictly necessary; and, for the purposes of combating (non-serious) crime and safeguarding public security, generalized and undifferentiated storage of data relating to the civil identity of users of electronic means of communication.

real time or a posteriori, the users, the direct relationship between them through the network, the location, frequency, date, time and duration of communication [...]» (cf. point 6.1. of the judgment of the TC No. 268/2022) - can only be preserved to the extent strictly necessary in the context of invoicing and payment for electronic communication services; it is true that for certain

services (with added value), Law No. 41/2004 even requires the consent of the data subject.

50. It is therefore disproportionate, in breach of Article 18(2) of the CRP and Article 52(1) of the Charter, as it is not necessary to process it for the purpose of invoicing and payment for communications services, the legal provision for the conservation of traffic data associated with the beginning and end of access to the Internet, and it is therefore recommended to eliminate it from subparagraph d) of paragraph 2 of article 6 of the Law No. 41/2004, in the proposed wording.

51. It is also recommended to delete data relating to the telephone number and associated date/time group (cf. subparagraphs c) and d) of paragraph 2 of article 6, in the proposed wording), due to its redundancy in compared to the data already provided for in the current version of this article.

ii. The right of information of the respective holders

52. The Draft Law also provides, in article 3, for the duty to notify data subjects.

53. As for the guarantee of the rights of data subjects, in particular the right to information that the TC highlighted, in line with the jurisprudence of the CJEU (cf. Judgment Tele 2, point 121) and of the European Court of Human Rights (ECtHR) - in particular, the Big Brother Watch judgment9 - the Proposal provides for the duty of the judicial authority to carry out such notification, in the order in which it determines the request for data, unless the Public Prosecutor, in an investigation, considers that the notification may jeopardize investigation, hinder the discovery of the truth or create danger to life, physical or mental integrity or to the freedom of procedural participants, victims of crime or other persons, in which case such notification may be delayed, under the terms provided for in Article 3(2).

54. In addition to not understanding the reason why this option of postponement is not specified for the judge, it is emphasized that, extending this notification to the holders of the transmitted data, this implies notification not only to the natural persons object of investigation , but also to all individuals with whom there has been communication or attempted communication, which significantly increases the universe of data subjects to be notified.

9 Judgment of May 25, 2021, complaints No. 58170/13, 62322/14 and 24960/15.

iii. data destruction

55. The data destruction regime provided for in Article 5 of the Proposal raises doubts as to its real scope. Especially when compared to the regime provided for in article 11 of Law No. 32/2008. It provided for the deletion of the data, by order of the judge addressed to the competent authorities for the criminal investigation, as soon as they were no longer necessary, specifying that this would happen in the event of definitive shelving of the criminal process, acquittal or conviction passed in res judicata, statute of limitations of criminal procedure and amnesty. Now, elimination is proposed only if they do not serve as evidence after the final decision that puts an end to the process has become final.

56. The intention of this provision is not achieved, admitting that there may be confusion between the retention of data in the context of criminal proceedings and the retention of data in the context of criminal investigation by the competent authorities.

57. The imposition of data destruction, after the decision has become final, only if they have not served as evidence, proves to be proportionate in the specific context of the criminal process; as for the data kept by the competent authorities for the criminal investigation, it will be manifestly disproportionate to foresee its destruction only in that circumstance. In fact, as the data are part of the criminal process, it seems appropriate and proportionate that their conservation by those authorities ceases in the circumstances listed in article 11 of Law No. 32/2008.

58. It is therefore recommended to clarify Article 5 of the Proposal, as to its scope of application, suggesting the reproduction of the content of Article 11 of Law No. 32/2008.

iv. The competence to regulate the new access regime

59. A final note to point out that it is not explained in the explanatory memorandum, nor is it obvious from the content of the diploma proposed here, or from the object and scope of application of Law No. 41/2004, the reason why, in article 4 . of the Proposal, the Government member responsible for the defense area is recognized as regulatory competence when it is certain that the purpose of the transmission of the data regulated herein is that of criminal investigation (cf. Article 1 of the Proposal), even considering the functions performed today by the Military Judiciary Police.

60. Specifically regarding the regulation of the conditions for the transmission of personal data, the minimum guidelines for the exercise of regulatory competence must also be defined in the legislative plan, in particular, the binding to guarantee the integrity and confidentiality of the personal data subject to streaming.

61. And recalls that Ordinance No. 469/2009, of 28 April, was published, in which the technical rules for the transmission of information are precisely defined, in order to guarantee the confidentiality and integrity of the transmitted data, as well as the auditability of all accesses.

62. It is also recalled that the technological system provided for in that ordinance was designed and implemented both on the side of the Ministry of Justice and on the side of electronic communications operators. However, first by Ordinance No. 131/2010, of March 2, and later by Ordinance No. 694/2010, of August 16, the optional nature of its use for a trial period was determined, specifying although this period would end when this was determined by a joint order of the members of the Government, which has not happened to date.

63. The CNPD can therefore only recommend the establishment of the same regulatory regime and the determination of its effective application.

III. Conclusion

64. Although it only provides for access for the purpose of criminal investigation to personal data relating to stored electronic communications, by companies that provide public network and electronic communications services, for the purposes of billing and payment of electronic communications services, this Draft Law substantially reduces the guarantees of citizens' fundamental rights, in comparison with the previous legal regime for the conservation and transmission of personal data relating to electronic communications (whatever was provided for in Law No. 32/2008, of 17 July, on retention of data relating to electronic communications, which is also provided for in the Cybercrime Law).

65. This reduction results from the combination of three distinct provisions: the provision for access by the Public Prosecutor's Office to personal data relating to electronic communications without direct and prior control by a judge; the extension of the purpose of access, now for the investigation of practically any crimes, regardless of their seriousness; and the imposition on operators that provide network and electronic communications services to retain more personal identification and traffic data than the

necessary for the purpose of invoicing and paying for electronic communications services with the data subject.

66. These three provisions constitute, per se, a disproportionate restriction of the fundamental rights to the reserve of private life, to informational self-determination and to the free development of the personality, but their simultaneous provision implies a strangulation of the fundamental guarantees of citizens in the context of the use of electronic networks and communications, with the risks of abusive intrusion into the private life of citizens and of conditioning their fundamental freedoms.

67. To that extent, the Draft Law contradicts national and European jurisprudence, in particular the content of the judgment of the Constitutional Court No. 262/2022, as well as the jurisprudence of the Court of Justice of the European Union and the European Court of Human Rights , representing a disproportionate restriction of the fundamental rights to privacy, self-determination and the free development of the personality, in violation of paragraph 2 of article 18 of the Constitution of the Portuguese Republic and paragraph 1 of article 52 .° of the Charter of Fundamental Rights of the European Union.

68. Thus, on the grounds set out above, the CNPD recommends:

i. The amendment of articles 2 and 3 of the Proposal, in order to provide for the need for an authorizing order from the judge to access personal data relating to electronic communications;

ii. The elimination of article 2(cj) of the Proposal;

iii. The amendment of article 8 of the Proposal, eliminating the following data from subparagraphs c) and d) in the new wording given by that article to paragraph 2 of article 6 of Law No. 41/2004: relative traffic data the group date/time of the call, telephone number and the data associated with the start and end of Internet access.

69. The CNPD also recommends:

i. clarification of the scope of application of the data destruction forecast, in article 5 of the Proposal;

ii. the reconsideration, in article 4 of the Proposal, of the option of recognizing regulatory competence to the member of the Government responsible for the area of defence, in the context of access to data for the purposes of criminal investigation;

iii. the imposition, in article 4 of the Proposal, that the regulation ensures the confidentiality and integrity of the personal data

object of transmission, as well as the auditability of this transmission in terms equivalent to those established in Ordinance No. 469/2009, of 28 April.

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

70. Finally, the CNPD points out, with regard to paragraph 1 of article 3 of the Proposal, that, in accordance with the right to provide information on the processing of data, the notification of access is extended to the holders of data transmitted, this implies notification not only to the natural persons subject to the investigation, but also to all natural persons with whom there has been communication or attempted communication, which significantly increases the universe of data subjects to be notified.

Approved at the meeting of June 21, 2022

Filipa Calvão (President)