National Data Protection Commission

OPINION/2021/36

I. Order

1. The Secretary of State for the Presidency of the Council of Ministers submitted to the National Data Protection Commission (hereinafter CNPD), for an opinion, the Draft Law Proposal that transposes Directive (EU) 2019/713, on the fight against fraud and counterfeiting of means of payment other than cash (Reg. PL 678/XXII/2020).

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 implements the GDPR (hereinafter, the Execution Law) in the domestic legal system and, also, as a result of the provisions of subparagraph c) of paragraph 1 of article 44 of Law no. 59/2019, of August 8th.

II. Analysis

3. The draft bill under analysis aims to promote a set of amendments to various diplomas in force. Due to the nature of these changes, which relate to revisions of the applicable penal frameworks, reformulations and additions of types of crime, in addition to the necessary and subsequent compatibility in related diplomas1, and since they do not contain relevant data protection matters personal information, the CNPD, except for occasional relevant notes, will only issue its opinion on articles 1, 4 and 5.

4. The aim of this draft Law Proposal is to promote changes in national legislation that can clearly align it with a set of obligations of a criminal nature imposed by Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and

1 We are talking here about changes to various professional statutes (judicial administrators, lawyers, solicitors, notaries, company recovery mediators) and, as well, regimes, such as the Statute of Private Social Solidarity Institutions; the electronic

documents and digital signature, of the Regulation of the Pension Fund for Lawyers and Solicitors; 137/2019, of 13 September, which approves the new organizational structure of the Judiciary Police.

Av. D. Carlos 1,134, I

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA (Directive (EU) 2019/713).

5. It is not, therefore, a transposition in the strict sense of a directive, but only a set of specific conditions that it provides and that are understood not to be properly covered by Portuguese legislation.

6. Among these, the projected rules regarding the extension of the current regime of criminal liability in the context of offenses provided for in the Penal Code to legal persons stand out2.

7. Equally relevant are the proposed amendments regarding the inclusion, in the legal provision of the currently existing incriminating rules, of "counterfeit and counterfeit tangible non-cash payment instruments other than credit cards (eg debit cards)", whose conducts are also concentrated in Law No. 109/2009, of September 15 (Cybercrime Law).

8. In this vein, it is also considered relevant to determine the frameworks of some conducts already punished by national law3 and, as well, to add conducts described in article 5 of the Directive, namely, "Having a payment instrument does not material other than cash illicitly obtained, counterfeited or counterfeited for fraudulent use, at least if the illicit origin is known at the time of its possession and "The acquisition for oneself or for a third party, including the sale, transfer or distribution, or the making available of a non-tangible payment instrument other than cash that has been illicitly obtained, counterfeited or falsified for fraudulent use."

9. Taking advantage of the changes resulting from the adaptation of national law to the requirements of the Directive, the aim is to promote "a new systematic insertion of norms, in line with the provisions of the Penal Code with those of the Cybercrime

Law" (cf. explanatory memorandum) .

10. In addition to all this, "it is made clear that national incriminations also cover acts carried out by reference to virtual currencies (of which bitcoin is a common example), in addition to other currencies already recognized by our legal system as integrating a system of payments: physical currency, book-entry currency and electronic currency.". This precision adds that "preparatory acts for crimes of computer forgery and counterfeiting of cards or other payment devices are punished regardless of whether or not the respective counterfeiting and counterfeiting actions are carried out".

2 In articles 203 to 205, 209 to 211, 217, 218, 221, 223, 225, 231 or 232

3 Notably Article 6(1) of the Cybercrime Law).

O

National Data Protection Commission

11. Alongside all these changes, others of lesser scope are promoted, such as the adjustment of the point of contact provided for in article 21 of the Cybercrime Law (which now includes the Public Prosecutor's Office, given the nature of the information to be exchange) and various diplomas4 where it is therefore inevitable to combine the novelties arising from the "transposition" with the content of the former. At this level, legal references in the Cybercrime Law (which will now refer to Law No. /2019 and no longer to the revoked Law No. 67/98, of October 26) and "correct[s] some expressions, semantic disharmonies or evident lapses contained in the Penal Code".

12. More problematic, however, are the novelties that are intended to be introduced both in article 17 of the Cybercrime Law and in Law no. this last one).

i. Amendments to Article 17 of the Cybercrime Law

13. Note the justification presented in the project for the changes to be made to article 17 of the Cybercrime Law:

“In another p/year, and even though it is an aspect that does not concern the transposition of Directive (EU) 2019/713, the opportunity is taken to adjust article 170 of the Cybercrime Law, whose content has generated jurisprudential conflicts that harm procedural economy and generate unnecessary doubts.

The purpose of this adjustment is to clarify the e-mail seizure model and the respective judicial validation, in light of the accusatory structure of Portuguese criminal proceedings.

The aim is, on the one hand, to clarify that the seizure of e-mail messages or of a similar nature is subject to an autonomous regime, which is in force in parallel with the resumption of the seizure of correspondence provided for in the Criminal Procedure Code. The latter regime only applies to the seizure of e-mails or similar messages in the alternative, and with the necessary adaptations.

On the other hand, it is intended to clarify that the seizure of e-mails or similar messages stored on a given device, although involving computer data of special content, is not technically different from the seizure of another type of computer data.

4 The Criminal Procedure Code, Decree-Law no. 137/2019, of 13 September, the Code of Mutual Associations, Law no. the Statute of the Order of Solicitors and Enforcement Agents, the Statute of the Bar Association, the Regulation of the Pension Fund for Lawyers and Solicitors, Law No. 22/2013, of 26 February, Law No. 32 /2008, of July 17, Law No. 52/2003, of August 22, Law No. 5/2002, of January 11, Decree-Law No. 290-D/99, of 2 of August, and the Statute of Private Institutions of Social Solidarity.

Av.D. Carlos 1,134.1°

1200-651 Lisbon

I (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

Thus, the Public Prosecutor's Office, after analyzing the respective content, must submit to the judge the e-mails or similar messages whose seizure has ordered or validated and which it considers to be of great interest for the discovery of the truth or for the evidence, considering the judge to add it to the case file, taking into account the interests of the specific case.

This solution seeks to replicate, in the field of e-mail messages or of a similar nature, the solution currently applicable to computer data and documents whose content may reveal personal or intimate data, jeopardizing the privacy of the respective owner or third party, under the terms of the Article 16(3) of the Cybercrime Law.

In addition to the above, it is clear that the fact that e-mails or messages of a similar nature should not be identified as "open"

or "closed" should not be procedurally overlooked since, contrary to what happens with correspondence on paper , such identification may be freely made by its holder." (emphasis added).

14. The draft wording of the new article 17, which embodies these motivations, resulted in the following article:

"1- When, in the course of a computer search or other legitimate access to a computer system, e-mails or similar messages are found, stored in that computer system or another to which legitimate access is allowed from the first that are necessary for the production of evidence, with a view to discovering the truth, the competent judicial authority authorizes or orders its seizure by order, even when they have not been opened or known by the respective addressees.

2- The criminal police body may carry out the seizures referred to in the previous number, without prior authorization from the judicial authority, in the course of computer research legitimately ordered and carried out under the terms of article 15, as well as when there is urgency or danger in the delay, such seizure must be validated by the judicial authority within a maximum period of 72 hours.

3- The Public Prosecutor's Office submits to the judge, under penalty of nullity, e-mails or similar messages whose seizure it has ordered or validated and which it considers to be of great interest for the discovery of the truth or for the evidence, the judge considering the its addition to the case file, taking into account the interests of the specific case.

4- The technical supports that contain the seized messages whose junction has not been determined by the judge are kept in a sealed envelope, at the order of the court, and destroyed after the final decision that puts an end to the process.

5- In what is not provided for in the previous numbers, the regime of seizure of correspondence provided for in the Criminal Procedure Code is applicable, with the necessary adaptations."

15. Article 17 of the Cybercrime Law currently provides, under the heading "Seizure of electronic mail and records of communications of a similar nature" as follows:

"When, in the course of a computer search or other legitimate access to a computer system, e-mails or records of communications of a similar nature are found, stored in that computer system or in another to which legitimate access is

allowed from the first , the judge may authorize or order, by order, the seizure of those who appear to be of great interest for the discovery of the truth or for the evidence, correspondingly applying the refund of the seizure of correspondence provided for in the Code of Criminal Procedure." (emphasis ours).

16. The regime for the seizure of correspondence provided for in the Criminal Procedure Code (CPP) is that contained in article 179, which provides that:

“(1) Under penalty of nullity, the judge may authorize or order, by order, the seizure, even at post and telecommunications stations, of letters, parcels, valuables, telegrams or any other correspondence, when he has well-founded reasons to believe that: a) The correspondence was sent by the suspect or is addressed to him, even if under a different name or through a different person; b) This is a crime punishable by a maximum prison sentence of 3 years; and c) Diligence will prove to be of great interest for the discovery of the truth or for the proof.

(2) The seizure and any other form of control of correspondence between the accused and his defender is prohibited, under penalty of nullity, unless the judge has well-founded reasons to believe that it constitutes the object or element of a crime.

(3) The judge who authorized or ordered the investigation is the first person to become aware of the content of the seized correspondence. If he considers it relevant to the evidence, he has it added to the file; otherwise, he returns it to the person entitled to it, and it cannot be used as a means of proof, and he is bound by a duty of secrecy in relation to what he has learned and has no interest in the proof.” (emphasis ours).

17. From the CNPD's point of view, it is evident that article 17 of the Cybercrime Law devises a system for validating the seizure of e-mail messages (or records of communications of a similar nature) in (almost) everything coinciding with the provided for in article 179.05 of the CPP. As the purpose of the Cybercrime Law is the "establishment of substantive and procedural criminal provisions, as well as provisions relating to international cooperation in criminal matters, relating to the field of cybercrime and the collection of evidence in electronic form", it constitutes, as far as to the evidence in electronic form true lex specialis as a counterpoint to the CPP. Even so, the legislator chose to implement the restriction of the constitutional right

to the inviolability of correspondence, provided for in article 34 of the Constitution of the Portuguese Republic (CRP), with a clause that practically replicates paragraph 1 of article 179 of the CPP, except when the triple condition is mentioned in this item as a condition to support the authorization or seizure order.

18. However, if it is accepted that a legislative change can serve to overcome "jurisprudential conflicts that harm the procedural economy and generate unnecessary doubts", greater difficulties are already pointed out to admit that this modification may intend to overcome these problems through the reduction of rights constitutionally enshrined fundamental rights - in particular, a fundamental right that has precisely as its object the reservation of the content of communications.

19. It can also be understood "that the seizure of e-mails or similar messages stored on a given device, although involving computer data of special content, is not technically different from the seizure of other types of computer data", but this conclusion it becomes incomprehensible if it is intended to justify the equating of personal and non-personal data. In fact, the CRP not only reserves a sphere of protection for the privacy of private life, but also better embodies the right to the inviolability of correspondence, and also singles out the protection of personal data in this catalog of “directly applicable” precepts.

20. It would therefore be unjustified, from the outset on the constitutional level, to enshrine in the legislation the indistinction between personal and non-personal data. Furthermore, this would constitute a latent violation of the recognition that is due to the right to respect for private and family life, as set out in Article 8 of the European Convention on Human Rights and, as well, in Articles 7 and 8. ° of the Letter

5 And Article 178, regarding open correspondence.

of the Fundamental Rights of the European Union6, respectively regarding respect for private and family life and the protection of personal data.

21. We have, therefore, that such an objective, declared in the explanatory memorandum, contradicts both the Constitution and the international commitments of the Portuguese State, and the reason for its inclusion in the Cybercrime Law is unfathomable.

22. Nor should it be said, as is advanced in the Project, that what is intended is the assimilation to the regime of the seizure of

computer data, contained in article 16, specifically that provided for in paragraph 37. First of all, the seizure of computer data, unlike electronic mail and the communication records of article 17, does not necessarily have to involve personal data or revealing the dimension of the private life of the persons concerned, which is the reason why the aforementioned paragraph 3 of the article 16 to guard against potential cases in which this happens, reinforcing the guarantees of citizens through the mandatory intervention of the Judge.

23. Then, because, unlike communications, it will be common to find this information (/.e., computer data) not sealed or closed (or with similar indication)8, depending on the knowledge of the existence of personal or intimate data of the contact direct and unavoidable with the content of these computer data9 even before the potential intervention of the Judge.

24. Finally, as it degrades the regime applicable to communications, it should not be seen as the obvious and suitable means of meeting the constitutional requirements that Article 18(2) and (3) of the CRP place whenever it is intended to limit or restrict rights, freedoms and guarantees. Especially when such degradation departs, to a disproportionate extent, from the regime provided for in the CPP for the seizure of correspondence, which was, until now, perfectly applicable to the cases provided for in Article 17 of the Cybercrime Law10.

6 In addition to article 52, due to its practical relevance in terms of restrictions on fundamental rights provided for in the Charter of Fundamental Rights of the European Union.

7 "If data or computer documents are seized whose content is likely to reveal personal or intimate data, which may jeopardize the privacy of the respective holder or of a third party, under penalty of nullity such data or documents are presented to the judge, who will consider the its addition to the case file, taking into account the interests of the specific case".

8 We will return to this point in more detail.

9 Note the definition that Article 2(d) of the Cybercrime Law offers "«Computer data», any representation of facts, information or concepts in a form susceptible of processing in a computer system, including programs capable of performing a computer system perform a function:"

,0 Cf. Judgment of the Lisbon Court of Appeal of 6 February 2018, available at http://www.dosi.pt/itrl.nsf/33182fc732316039802565fa00497eec/a1b9fce5f23b342480258242004327a37QoenDocument.

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

25. A final note, regarding the explanatory memorandum, regarding the procedural disregard of the indication “that e-mails or similar messages are identified as “open” or “closed” since, contrary to what happens as for paper correspondence, such identification may be freely made by the holder." (emphasis added).

26. The final assertion that it is now possible for any recipient of messages of this type to identify them as closed (or unread) is not contested. What becomes incomprehensible is how the legislator derives from this circumstance the consequence of the inevitable degradation of the fundamental right to the inviolability of correspondence. And this in completely new terms, disqualifying situations in which, in fact, the communications had not yet been known to the person concerned, disregarding, in this way, the need for intervention by the judge and placing in the hands of the Public Prosecutor's Office, when not even the body of criminal police, the possibility of effecting the seizure of this correspondence.

27. The principle of proportionality, referred to in paragraph 2 of article 18 of the CRP11, seems to require the inclusion of the criminal investigation judge in this operation of validation of seizures, maintaining a regime identical to that of article 179 of the CPP12, and certainly whenever the messages are indicated as "closed/unread"13. Nor should it be said that the intervention of the investigating judge in the proposed manner harms or may harm the accusatory structure of the criminal process, since it is merely modeled on the CPP regime, whose compliance with the CRP is not questioned.

28. Without prejudice to possible nuances that could be introduced by reference to the specifics of the messages whose seizure is provided for in article 17 of the Cybercrime Law, operating a presumption of this gravity, always to the detriment of any person who sees this type of correspondence seized , appears to be disproportionate and, therefore, in violation of the constitutional principles that govern restrictions on rights, freedoms and guarantees.

11 And, although we are in the criminal field, why not consider the same criterion postulated in the aforementioned article 52 of the CDFUE.

12 And if there were any doubts, this is emphasized by Article 269(1)(d): during the investigation, it is exclusively up to the investigating judge to first take cognizance of the content of the seized correspondence, under the terms of no. 3 of article 179. Remember that, as Paulo Pinto de Albuquerque notes, "The failure to examine the correspondence by the judge constitutes a nullity of article 120, no. 2, al. d, because it is a legally binding procedural act", note 12 to article 179 in Commentary on the Criminal Procedure Code in the light of the Constitution of the Republic and the European Convention on Human Rights, Lisbon: Universidade Católica Editora, 4th edition 2011.

13 Note should also be made of the legislative option set out in paragraph 3 of article 17, in the wording now designed, of omitting, strangely, the setting of a deadline for the submission of electronic messages to the Criminal Investigation Judge.

ii. The intervention of the Public Ministry in the light of the jurisprudence of the Court of Justice of the European Union and the amendment to Law No. 32/2008

29. The amendment to the Cybercrime Law resulting from the project is based, as assumed in the explanatory memorandum, on the adaptation of the national legal system to that provided for in Directive (EU) 2019/713. It is a fact that the aforementioned law focuses on criminal and procedural discipline in the field of cybercrime and evidence in electronic form, it being known that "in the current state of Union law, it is, in principle, exclusively for national law to determine the rules relating to the admissibility and examination, in the context of criminal proceedings instituted against persons suspected of criminal acts, of information and evidence"14.

30. It should not be forgotten, however, that European Union law has been growing in importance and relevance in shaping the criminal legislation of the Member States15. Furthermore, the Cybercrime Law itself results from the transposition into national law of Framework Decision no. Council of Europe. And the legislator's opportunity to, for the first time, make changes to Law No.

31. It is undeniable that the projection of Union law and the European Convention on Human Rights into domestic law must be considered here. And, likewise, the considerations of the competent Courts17 must be considered to judge, in the end, the

conformity of domestic law with the provisions of the Union and with the Convention.

32. In terms of digital evidence, the interpretative path that the Court of Justice of the European Union (CJEU) has been leading in recent years is particularly relevant, especially in the evaluation of Directive 2006/24/EC of the European Parliament and of the Council, 15 March 2006, as well as the national laws that transposed it.

33. We do not need to describe in detail all the judgments that have been dealing with it, it is sufficient to mention that the Directive was considered invalid in 2014, in the judgment Digital Rights Ireland, Ltd.,

14 Cf. § 41 of the CJEU judgment of 2 March 2021, in case C-746/18.

15 Note the article by Anabela Miranda Rodrigues, «European Criminal Law in the light of the principle of necessity - the case of market abuse», published in Católica LawReview, Vol. 1, no. 3, nov. 2017, available at https://fd.lisboa.ucp.pt/asset/3041/file.

16 In the meantime repealed by Directive 2013/40/EU of the European Parliament and of the Council, of 12 August 2013, on attacks against information systems.

17 Respectively the Court of Justice of the European Union and the European Court of Human Rights.

of 8 April 2014, in the context of preliminary rulings that gave rise to cases C-293/12 and C-594/1218.

34. The CNPD issued Deliberation 641/201719, where, as a consequence of the declaration of invalidity resulting from the judgment of the CJEU, "[e]understand[u] (...) it is its duty to alert the Assembly of the Republic to the need to re-evaluate Law No. 32/2008, of July 17, in terms of compliance with the Charter, but also with the CRP, since the fundamental rights restricted by that regime are constitutionally enshrined and the legal restriction of such rights complies with the constitutional terms to the

same principle of proportionality." Having concluded, among others, that "Law No. 32/2008 contains rules that provide for the restriction or interference with the fundamental rights to respect for private life and communications and the protection of personal data (Articles 7 and 8) of the Charter of Fundamental Rights of the European Union) with great breadth and intensity, in clear violation of the principle of proportionality and, therefore, in violation of Article 52(1) of the Charter.

35. On the same grounds, there is a disproportionate restriction of the rights to the privacy of private life, the inviolability of communications and the protection of personal data, in violation of the provisions of paragraph 2 of article 18 of the Constitution of the Portuguese Republic."20

36. This opinion is not intended to stress the arguments set out there to justify the relevant need to reassess Law No. 32/2008, of 7 July, in the light of the CJEU jurisprudence, which has not yet happened, if, in this particular, for the aforementioned deliberation, whose content remains totally current. In fact, a request for review of the constitutionality of the aforementioned diploma, submitted by the Ombudsman, is under consideration by the Constitutional Court.

37. However, it is considered essential to reinforce the suggestion of revising this law in the light of the evolution of recent CJEU jurisprudence, which only confirmed the conclusions contained in the CNPD's deliberation and introduced new elements of analysis to which the national legislator cannot fail to confer significant importance.

38. Without prejudice to the useful clarifications introduced by the CJEU Judgment of 6 October 2020, in case C-623/17, especially with regard to the delimitation of the exceptions or restrictions allowed by no.

18 Available in

httP://curia.europa.eu/iuris/document/document.isf:isessionid=9ea7d0f130d63d34ffbab785491ab755b34740570fe7.e34Kaxilc3eO c40LaxaMbN4Pax0Oe0?text=&docid=150642&paaelndex=0&doclanci=PT&dir.

19 Available at https://www.cnDd.pt/umbraco/surface/cnDdDecision/download/101085.

20 Cf. conclusions of the aforementioned resolution.

1 of article 15 of Directive 2002/5821, we believe that it is a priority to point out here the conclusions of the CJEU Judgment, of

2 March, in case C-746/18, as the court stopped here on the legitimacy of the Public Prosecutor's Office to authorize access by a public authority to traffic data and location data for criminal investigation purposes.

39. In this case, three questions were posed to the CJEU, and for the present opinion, we will focus only on the third one, due to the special relevance it demonstrates.

40. As the court postulated, the question referred for a preliminary ruling was thus summarized "if Article 15(01) of Directive 2002/58, read in the light of Articles 7, 8, 11 and 52. Article 1(1) of the Charter must be interpreted in the sense that it precludes national legislation that confers competence on the Public Prosecutor's Office, whose mission is to direct criminal investigations and, where appropriate, exercise public action in a subsequent proceeding. , to authorize access by a public authority to traffic data and location data for the purpose of criminal investigation."22

41. Starting from the uncontroversial idea that "it is true that it is up to national law to determine the conditions under which providers of electronic communications services must grant competent national authorities access to the data they have, [the CJEU notes that,] for satisfy the requirement of proportionality, such regulations must provide for clear and precise rules governing the scope and application of the measure in question and imposing minimum requirements, so that the persons whose data have been kept have sufficient guarantees to effectively protect that personal data against the risks of abuse."23

42. These “material and procedural” rules must “be based on objective criteria to define the circumstances and conditions under which access to the data in question must be granted to the competent national authorities.”24. access by the competent national authorities to the stored data is, in principle, subject to prior review carried out by a court or tribunal

21 Which provides: "Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Articles 5 and 6, in Article 8(1) to (4) and in Article 9 of the this Directive where such restrictions constitute a necessary, appropriate and proportionate measure in a democratic society to safeguard national security (i.e. State security), defence, public security, and prevention, investigation, detection and prosecution of criminal offenses or unauthorized use of the electronic communications system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may in particular adopt legislative measures providing for that the data be kept for a limited period, for the reasons set out in this paragraph. All the measures referred to in this paragraph must comply with the general principles of Community law, including those mentioned in s(1) and (2) of Article 6 of the Treaty on European Union."

22 Cf. § 46 of the judgment.

23 Cf. § 48 of the judgment.

24 Cf. § 49 and 50 of the judgment.

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

or by an independent administrative body and that the decision of that court or body is taken following a reasoned request from those authorities made, in particular, in the context of prevention, detection or criminal prosecution proceedings. In case of duly justified urgency, the inspection must be carried out within short deadlines"25 26

43. And, continuing, he notes, "This prior inspection requires (...) that the court or entity in charge of carrying out the aforementioned prior inspection has all the powers and presents all the necessary guarantees with a view to ensuring a conciliation of the As regards, more specifically, a criminal investigation, such supervision requires that court or entity to be able to ensure a fair balance between, on the one hand, the interests linked to the needs of the investigation in the context of the fight against crime and, on the other hand, the fundamental rights to respect for privacy and the protection of the personal data of the persons to whom access concerns."25

44. Hence, "...the independence requirement that the authority in charge of carrying out the prior inspection (...) must satisfy requires that authority to act as a third party in relation to the authority requesting access to the data, so that the former is in a position to carry out such supervision in an objective and impartial manner, free from any external influence. In particular, in the criminal field, the requirement of independence implies (...) that the authority in charge of that prior inspection, by a hand, is not involved in the conduct of the criminal investigation in question and, on the other hand, has a position of neutrality vis-à-vis the parties to the criminal proceedings.

This is not the case for a Public Prosecutor's Office that directs the investigation and carries out, where appropriate, public

action. Indeed, the Public Prosecutor's mission is not to decide a dispute with complete independence but to submit it, if necessary, to the competent court, as a party to the process that carries out the criminal action.

The circumstance that the Public Prosecutor's Office is obliged, in accordance with the rules that regulate its powers and statute, to verify the incriminating and exculpatory elements, to guarantee the legality of the investigation of the case and to act only in accordance with the law and in accordance with its conviction is not sufficient to grant it the status of a third party in relation to the interests at stake in the sense described in paragraph 52 of this judgment.

25 Cf. § 51 of the judgment.

26 Cf. § 52 of the judgment.

It follows that the Public Prosecutor's Office is not in a position to carry out the prior inspection referred to in no. 51 of the present judgment, 1'27

45. However, the CJEU is unequivocal in the indispensability of mediation by a judge or independent authority in the access to data kept under Directive 2002/58/EC28. This is another criterion that is added to those already defined by this Court29 and that applies directly to the national context, since, despite our process not being a process of parties, but of subjects, the reasoning of the judgment because here too "[t]he Public Ministry represents the State, defends the interests that the law determines, participates in the execution of the criminal policy defined by the sovereign bodies, carries out criminal action guided by the principle of legality and defends democratic legality, in the terms of the Constitution, the present Statute and the Law"30, "enjoy[ing] only autonomy in relation to the other organs of central, regional [,..]"31.

46. This means, in the context of this opinion, that, in the first place, the legislator should take advantage of the opportunity presented to him to amend Law no. substantive and procedural criteria in force in it to legitimize the conservation and access to data generated or processed in the context of the provision of publicly available electronic communications services or public communications networks. Instead of limiting itself, as seen in the draft bill, to adding a conduct to the catalog of those

that already exist in the concept of “serious crimes”, provided for in paragraph g) of article 1 of the so-called Law on Retention of Given that, the legislator could and should have expanded the impetus for revision in order to overcome the current context of unsustainable fragility in which the diploma finds itself.

47. The relationship between this incursion into the CJEU jurisprudence and the proposed changes to the Cybercrime Law do not concern the obligation of the national legislator to apply, ipsis verbis, to the revision of this law what is defended for the Data Retention Law. In any case, one cannot fail to draw consequences from this judgment for other pieces of legislation that provide for solutions, such as the one now proposed for article 17, to allow the Public Prosecutor's Office a wide scope of action in the validation and order of seizure of the e-mails or similar messages. Now, without postponing the competence of the Member States to define the criminal regime and internal criminal procedure, the combination of legal systems

27 Cf. §§ 54 to 57 of the judgment.

28 Conservation which, in Portugal, is regulated by Law no. 32/2008, of 7 July.

29 Cf. point 2 of the CNPD's conclusions in the aforementioned Deliberation.

30 Cf. article 2 of Law No. 68/2019, of 27 August (Statute of the Public Prosecutor's Office/EMP).

31 Cf. Article 3(1) of the EMP.

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

/

nationals with which they come from the European Union - especially when partially or totally linked by obligations to transpose directives must, at least, consider the structural implications arising from the obligations of the Member States, here, specifically, regarding respect for the provisions of the Charter of the Fundamental Rights of the Union.

48. Basically, the perplexity arises from the pretension of admitting such interference with uncontroversially sensitive data, such as communications, when the CJEU requires much stricter criteria to admit access to other personal data (such as traffic and location)32. And it is reinforced by the clear contradiction with the provisions of Article 52(1) of the Charter of Fundamental Rights of the European Union.

49. Also in terms of ECtHR jurisprudence, if it is true that it is not possible to apply directly to this Draft the judgments concerning the assessment of access to communications data by secret or intelligence services33, the perplexity at the proposed amendment of Article 17 against the provisions of Article 8 of the European Convention on Human Rights.

I. Conclusion

50. On the grounds set out above, the CNPD understands that:

The. The amendments to article 17 of the Cybercrime Law, as found in the draft bill under analysis, represent a clear degradation of the level of protection for citizens in a critical domain of their private sphere, such as communications;

B. By uncontroversial divergence from the regime provided for in article 179 of the CPP, the Draft Law Proposal introduces additional and unsubstantiated restrictions on the rights, freedoms and guarantees to the

32 Despite the fact that the CNPD's position is completely in line with that of the CJEU, as noted in Point II of the aforementioned Deliberation: "In fact, these are data that reveal at all times aspects of the private and family life of individuals: allowing the location of the citizen throughout the day, every day (provided that you carry your mobile phone or other electronic device for accessing the Internet) with whom you contact (call - including attempted and unsuccessful calls - by phone or mobile phone, sending or receiving SMS, MMS, or email), duration and regularity of these communications and which websites you consult."

33 Cf. Judgment Big Brother Watch and others v. the United Kingdom of 13 September 2018 (available at http://hudoc.echr.coe.int/fre?i=001 -140713) and Judgment Roman Zakharov v. Russia, December 4, 2015 (available at http://hudoc.exec.coe.int/fre?i=004-14134l.

inviolability of communications and, reflexively, the protection of personal data, as enshrined in articles 34 and 35 of the CRP,

respectively;

ç. Admitting that the Public Prosecutor's Office may, without prior control by the Criminal Investigation Judge, order or validate the seizure of electronic communications or similar records does not excessively protect persons who may be suspected or who have incidentally interacted with these suspects, and the requirement for the intervention of the Investigating Judge, under the same terms of article 179 of the CPP, can never be seen as distorting the accusatory principle that governs criminal proceedings in Portugal;

d. Moreover, and taking into account the recent judgment of the CJEU, of 2 March, in case C-746/18, which rules out the possibility of an entity that is in every way similar - in terms of powers and hierarchical dependence - to the Portuguese Public Prosecutor's Office to be able to accessing traffic and location data, within the framework of criminal proceedings and in compliance with the exceptions provided for in paragraph 1 of article 15 of Directive 2002/58/EC, without the prior authorization of a judge or independent entity, only the proposed amendment to article 17 of the Cybercrime Law may be considered inadmissible, as it clearly contradicts the provisions of article 52 of the Charter of Fundamental Rights of the EU (and without waiving the provisions of paragraph 2 of the Article 18 of the CRP).

51. As for the amendment to Law No. 32/2008, of July 7 (Data Retention Law), which is proposed in article 4 of the Project, limiting itself to adding a new conduct to those already contained in the concept of "serious crime", it is difficult to understand that, after the CJEU has declared the Directive that this law transposes invalid and when its own constitutionality is being judged, the legislative amendment has this content, instead of correcting or supplying the rules in crisis. The CNPD understands, therefore, that the legislator can only carry out a deep and meticulous review of the substantive and procedural regime of the aforementioned law. This is stated as an imperative resulting from the constant jurisprudence of the CJEU and an essential condition to overcome the current situation of fragility, to say the least, in which the law finds itself.

Lisbon, March 26, 2021

Filipa Calvão (President, who reported)

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