?ART2021t67

tL\'-

OPINION/aOZ1IV4

I. Order

1. The Committee on Constitutional Assistance, Rights, Freedoms and Guarantees of the Assembly of the Republic requested the National Data Protection Commission (CNPD) to issue an opinion on Draft Law no. 9&IXIV n.a (Gov), which "Transposes Directive (EU) 2019/713 on combating fraud and counterfeiting of payment other than in cash.

2. The CNPD issues an opinion within the scope of its attributions and competences as an administrative authority with powers of authority to control the processing of personal data, conferred by the Article 57(1)(cJ) in conjunction with Article 58(3)(b) and Article 36.0(4), all of Regularnento (EU) 2016/679, of April 27, 20i 6 - General Data Protection Regulation (hereinafter, GDPR), in conjunction with the provisions of article 3, paragraph 2 of article 4, and point a) of paragraph 1 of the article 6.0, all of Law No. 58/2019, of August 1st. which implements the GDPR in the domestic legal order (hereinafter, Law Execution) and, also, as a result of the provisions of subparagraph c), of paragraph 1 of article 44 of Law no. 59/20i9, of I of August.

3. The CNPD has already commented through its Opinion No. 3612021, of March 23, on the Draft Proposal for Law No. 678IXXill2A20 whose content remains practically unchanged in the diploma now submitted. So, because the observations produced at that time remain relevant and necessary, it limits itself to reproducing with small adjustments to the Opinion formulated.

il. Analysis

4" The proposed law 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 diplomas, 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 5th-

1 We are talking here about changes in various professional statuses (judicial administrators, lawyers, solicitors, notaries. mediator for the recovery of companies) and, as well, of returns, such as the Statute of Private Solidarity Institutions Social; that of electronic documents and digital signatures. of the Regulation of the Social Security Fund for Lawyers and Solicitors;

of the code of Mt{ualist Associations and Decree-Law No. 1 37/201 9, of 13 September, which approves the new organizational structure

of the Judiciary Poliria"

P4W2021t67

1Y

\q:--

5. It is intended, with this Draft Law, to provide changes in national legislation that, in a clear way, can 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 counterfeiting of means of payment other than cash and replacing Council Framework Decision 2001/413/JAl (Directive (EU) 201 9/71 3).

6. It's not about. therefore, of a transposition in the proper sense of a directive, but only of a set of specific conditions that it provides and that are understood not to be duly covered by the Portuguese legislation.

7. Among these, those relating to the extension to legal persons of criminal liability in the framework of illicit activities already provided for in the Penal Code2.

8. Equally relevant are the proposed amendments regarding the insertion, in the legal provision of the nonnas existing incriminating acts of 'corporeal payment instruments other than cash counterfeit and counterfeit other than credit cards (e.g. debit cards)' whose conduct are still. concentrated in Law No. 10912009, of 15 September (Cybercrime Law).

9. In this path, it is also considered relevant to investigate the frameworks of some conducts already punished by law

national e. well, to add to it the conduct described in article 5 of the Directive, namely, "The detention of a

non-tangible payment instrument other than cash obtained illegally, counterfeit or falsified

for fraudulent use, at least if the illicit origin is known at the time of your arresti and "The

acquisition for yourself or for a third party, including the sale, transfer or distribution, or making available

of a non-tangible payment instrument other than cash obtained illegally, counterfeit or

counterfeited for fraudulent use.'.

10- Taking advantage of the changes resulting from the adaptation of national law to the requirements of the Directive, the aim is to

to promote a new systematic insertion of norms, in line with the provisions of the Penal Code with the

of the Cybercrime Law' (cf. explanatory memorandum).

11. In addition to all this, it is clear that national criminal offenses also cover acts carried out by

reference to virtual currencies (of which bitcoin is a common example), in addition to other already recognized currencies

by our legal system as part of a payment system: physical currency, book-entry currency and

electronic currency.'. This precision is added to that 'that the preparatory acts for crimes of computer forgery

? In articles 203.0 to 205.0, 209.0 to 2'l'1"o, 217"o, 218.0.221.o, 223.a,225.0,231-o

3 Namely paragraph 1 of article 6"0 of the Cybercrirne Law)-

oul 232.0

p4W2821t67

=K(--'

and counterfeiting of cards or other payment devices are punished regardless of whether

or not of the respective actions of falsification and counterfeiting".

12. 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, in view of the

nature of the information to be exchanged) and of several diplomas where it is consequently inevitable to combine the

novelties arising from the 'transposition' with the content of the former. At this level, remissions are still corrected

in the Cybercrime Law (which will now refer to Law No. 59/2019 and no longer to the revoked Law No. 67198 of 26

October) and "some expressions, semantic discrepancies or obvious lapses in the

Penal Code'.

13. More problematic, however, are the novelties that are intended to be introduced either in article 17 of the Law on Cybercrime, or in Law No. 3U2008 (although here it is an operation to reconcile the changes

from the former to the latter).

i" Amendments to article 17 of the Cybercrime Law

14- Pay attention to the justification presented in the proposal for the changes to be made to article 17 of the Law on Cybercrime:

'On another level, and even though it is an aspect that does not concern the transposition of Directive (EU) 2019/713, takes advantage of the opportunity to adjust article 17 of the Cybercrime Law, whose content has generated conflicts jurisprudence that harm the procedural economy and generate unnecessary doubts.

The purpose of this adjustment is to clarify the e-mail seizure model and the respective

judicial validation.

On the one hand, it should be noted 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 regime for the seizure of correspondence provided for in Penal Code Process. This last regime only applies to the seizure of electronic connection messages

or similar in nature to the subsidiary title. and make the necessary adaptations.

a 0 Code of Fenal Procedure, Decree-Law No. '137l20i 9, of '13 September, the Code of Mutual Associations, Law No. 6/20'18,

of February 22, the Statute of the Order of Notaries. the Statute of the Order of Solicitors and Enforcement Agents, the Statute of the Order of Lawyers" the Rryularnento of the Pension Fund for Lawyers and Solicitors, Law n-o 2212013, of 26 February, Law no. 32/2008, of July 1 7, Law no. 52/2003, of August 22, Law no. 5f2002, of January 1 1, and Decree-Law no. 290-D/99, of 2 August and the Statute of Private Social Solidarity Institutions-

P^Rt2oz1t67

**

I

\L§

On the other hand, it is intended to clarify that the seizure of electronic messages or of a similar nature

stored on a given device. embara focusing on infarmatic data of es@ial content. it is not

technically in order to prevent the seizure of another type of formal data.

Assrm, should Mrhrsfdrio Priblico, after analyzing the respective song, present the eorreia messages to the judge

au electronics of a simrlar nature whose learning has been ordered au validated and which you consider to be of great

importance

interest for the discovery of the truth or for the prava, the judge considering its addition to the file taking into account

the interests of the specific case.

fsfa solution can be replicated. in the field of electronic au messages of a similar nature. the solution

presently applicable to data and documents in forms whose content may reveal personal data or

rhythms jeopardizing the privacy of the respective owner or a third party, under the terms of no. 3 of article !6.' of law

of 0ibercrime.' (emphasis ours).

15. The proposed wording of the new article 17, which embodies these motivations, resulted in the following

articulated:

"l- When, in the course of computer research or other legitimate access to a computer system,

are found, stored on that computer system or another to which legitimate access is allowed

from the first, messages of an electronic mail or of a similar nature that are necessary for the

production of evidence, with a view to discovering the truth, the judicial authority comFtenally authorizes or

orders his arrest by dispatch.

2- The criminal police agency may carry out the seizures referred to in the previous number, without prior authorization

of the judicial authority, in the course of computer research legitimately ordered and carried out in the

of article 15, even when there is urgency or danger in delay, such seizure must be validated by the

judicial authority within the maximum period of T2haras.

3- To the seizure of messages by electronic pen and of a similar nature, the provision in nos. 5 to

8 of the previous article.

4- The Public Ministry presents to the judge, under penalty of nullity, the messages of electronic connection or similar nature which the apprehension has ignited or validated and which is considered to be of great interest to the discovery of the truth or for the prava, the judge pondering its joining with the auIos, in trust with the mIeresses of the concrete case.

5- The hard supports that contain the seized threads whose junction has not been determined by the judge are kept in a sealed envelope, to the order of the court, and enjoyed after the final judgment of the decree to put an end to the process.

6- In what is not foreseen in the previous numbers, it is applicable, with the necessary adaptations, the correspondence seizure regime provided for in the Criminal Procedure Code-'

16. Today, Article 17 of the Cybercrime Law, under the heading 'Seizure of electronic mail and records communications of a similar nature'as follows:'When, in the course of a computer search or other legitimate access to a computer system, are found, stored on that computer system or another to which legitimate access is allowed from the first, e-mail messages or communications records of a similar nature. the judge may authorize or order. by dispatch. the apprehension of those who appear to be of great interest for the discovery of the truth or for the proof, applying correspondingly the regime of the seizure of correspondence provided for in the Code of Criminal Procedure.' (emphasis ours).

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

(i) Under penalty of nullity, the judge may authorize or order. by order, the seizure, even in the stages of correbs and Íelecomunica@es, letters, orders, values, telegrams or any other correspondence, when you have good reason to believe that: a) The correspondence has been sent by the supervisor or is addressed to him, even if under a different name or through a different person; b) This is a crime punishable by imprisonment to exceed, at most, 3 years; and c) Diligence will prove to be of great interest in discovering the truth or wra the proof

(2) It is prohibited, under penalty of nullity, the seizure and any other means of controlling correspondence between

the accused and his defender, unless the judge has well-founded reasons to believe that the former constitutes an object or eemenIon of a crine

(3) The judge who has authorized or ordered the diligence is the first person to be aware of the content of the apprehension. If you consider it relevant for the test, please add it to the file, otherwise, return it to anyone from dketta, it cannot be used as a means of proof, and is bound by the deuer of secrecy with respect to that of which you have become aware and are not of interest to the prava.' (emphasis added).

18- From the CNPD's point of view, it is evident that article 17 of the Cybercrime Law builds a system of validation of seizure of e-mails (or records of communications of a

"""ftL*-

similar) in (almost) everything coinciding with the provisions of article i79 of the CPPs. Being the object of the Law of cybercrime is the 'establishment of material penal provisions and practices as well as the provisions relating to international cooperation in criminal matters, relating to the field of cybercrime and the collection of evidence in eiect'Ínrbo' support", it constitutes, as regards the evidence in electronic support, true lex specals in contrast to 0 CPP. Even so, the legislator chose to implement the restriction of the constitutional right to 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 that in this item is pointed out as a condition to substantiate the authorization or order of apprehension.

19. Now, if it is accepted that {A legislative amendment can serve to overcome the jurisprudence that harm the pracessuale economy 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 fundamentals - in particular, a fundamental right that has precisely by object the reservation of the content of the communications.

20- It can also be understood that the seizure of electronic mail messages or of a similar nature stored in a certain drspositr'vo, although it focuses on computer data of esryial content, it is not Based on the seizure of another computer data', but this conclusion is incomprehensible. if it is intended to justify the assimilation of personal and non-personal data. Indeed, the CRp reserves

not only a sphere of protection for the reserve of the intimacy of private life, as it is best concretized in the law
to the inviolability of compliance, and also singles out the protection of personal data in this catalog of
'directly applicable' precepts.
21. It would therefore be unjustified, from the outset on the constitutional level, to enshrine in legislation the indistinction
between
personal data and non-personal data. Furthermore, this would constitute a latent violation of the recognition that
due to the right to respect for private and family life as set out in Article B.o of the Convention
European Union of the Rights of Hornem, as well as Articles 7 and 8 of the Charter of Fundamental Rights of
European Union6, respectively regarding respect for private and family life and the protection of personal data.
22. We have, therefore, that such an objective, declared in the explanatory memorandum, contradicts both the Constitution
and the
the international commitments of the Portuguese State, the reason for its inclusion in Leido being unfathomable
cybercrime.
5 And article 1 78.0, regarding open compliance.
6 In addition to article 52, given its practical relevance in terms of restrictions on fundamental rights provided for in the CDFEU
PAW2021t67
\\-t:'
23. Nor should it be said, as advanced in the Proposal, that what is intended is the assimilation to the seizure regime
of computer data, contained in article 16.0, specilically as provided for in paragraph 37. First of all, the seizure
computer data, unlike e-mail and Article 17 communications records, does not
necessarily have to involve personal data or data revealing the dimension of the private life of the persons concerned,
this being the reason why the aforesaid paragraph 3 of article 16.0 cautions potential cases in which this happens,
citizens' guarantees are reinforced through the mandatory intervention of the Judge.
24. Second, because, unlike communications, it will be common to find this information (r.e., the data
computers) not sealed or closed (or with similar indication)8, depending on the knowledge of the
existence of personal or intimate data from direct and unavoidable contact with the content of these data

computersq even before the potential intervention of the Judge.

25. Finally, as it degrades the regime applicable to communications, it should not be seen as the obvious and suitable to meet the constitutional requirements that paragraphs 2 and 3 of article 18 of the CRP always place intended to limit or restrict rights, freedoms and guarantees. Especially when such degradation is 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 Law.

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

26. The amendment to the Cybercrime Law resulting from the Proposal is based, as assumed in the explanatory memorandum,

in adapting the national legal system to that provided for in Directive (EU) 2019/713. It is a fact that the said law focuses on criminal and procedural discipline in the field of cybercrime and electronic evidence. being It is known that, in the current state of Union law, it is, in principle, exclusively for national law to determine rules on admissibility and assessment, in the context of criminal proceedings brought against persons suspected criminal acts of information and evidence']1.

7 'If you seize data or computer donations whose content is liable to reveal personal or limited data, which may injure the privacy of the respective holder or of a third party, under penalty of nullity these data or documents are presented to the judge who will file their lawsuit in the light of the interests of the specific case'.

And at this point we will return in more detail-

and Note the definition that Article 2(d) of the Cybercrime Act offers '"Computer data", which is a representation of Facts, information or concepts are a susceptible form of processing,) a computer srbIem, including suitable programs to do a srslerna rhfonnátrbc to perform a function

r0 Cfr. Judgment of the Lisbon Court of Appeal of 6 February 2018, available at http://www.dgsi.pt/jtrl.nsf/331 82fc73231 6039802565fa00497eecia1 b9fce5f23b342480258242004327a3?0oenDocument.

ní Cfr. § 41 of the judgment of the CJEU of March 2, 2021, in case C:146118.

\t\"

27. It should not be forgotten, however, that European Union law has been growing in importance and relevance in compliance with the criminal legislation of the Member States12- Moreover, the cybercrime law itself results from the transposition into national law of Framework Decision No. 2005/222lJAl, of the Council, of 24 February, the in addition to adapting domestic law to the Council of Europe Convention on Cybercrime, and the opportunity of the legislator in, for the first time, making changes to Law No. 3212008, of 7 July, cannot fail to to convene a serious reflection on its overall suitability in the face of the Union's legal system.

28. It is undeniable that the projection of Union law and the European Convention on Human Rights in the internal has to be considered here. And, thus, the weightings of the Courts must be considered competentl4 to judge, in the end, whether domestic law conforms to the provisions of the Union and to the convention.

29. In terms of digital evidence, the interpretative path taken by the CJEU is particularly relevant. played a leading role in recent years, especially in the evaluation of Directive 20A6l24IEC of the European Parliament and the Advice. of March 15, 2006, as well as the national laws that transpose it.

30. We do not need to describe in detail all the judgments that have been made about it, being enough to note that the Directive was considered invalid in 2014, in the judgment DigitalRghts lreland, Ltd., of 8 April 2014 in the context of judicial referrals that gave rise to cases C-293/12 and C-594/1215-

31 "The CNPD issued Resolution 6411201716, where, as a result of the resulting invalidity declaration of the judgment of the CJEU, '[e]understand[u] (...) that it is its duty to alert the Assembly of the Republic to the need to reassess Law No. 32120A8, of 17 July, in terms of compliance with the Charter, but also with the CRP, since the fundamental rights restricted by that regime have constitutional consecration and the restriction of such rights obeys, in the constitutional terms, the same principle of proportionality.'. Having concluded, among others, that Law no. 32/2008 contains rules that provide for the restriction or interference in the rights fundamental to respect for privacy and communication and the protection of personal data (Articles 7

12 Atenlese in the artiEo by Anabela Miranda Rodrigues,0 Direrto fmal european in the light of the principle of necessity * the case of abuse of

market, published in Católica Law Review, Vol. 1, No. 3, Nov. 2017, available at httpsl/fd.lisboa.ucp.pVasseU304lllile.

n3 However, repealed by Directive 201 3140/EU of the European Parliament and of the Council, of 1 2 August 2013,

concerning attacks

against information systems.

14 Respectively, the Court of Justice of the European Union and the Europzu Court of Honnem-

15

http://curia.europa.eu/juris/document/document.jsfisessionid=9ea7d0f1 30d63d34ffbab7B5491

ab755b34740570fe7.e34KaxiLc3e0

c40LaxqMbN4Pax00e0?text=&docid='1 50642&pageIndex=0&doclanS=PT&mode=lst&dir=&occ=Íirst&part=1 &cid=48371.

16 Available at https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/101 085-

Available

in

PÀny2021/67

\§q^q)',

and 8th of the Cafia on Fundamental Rights of the European Union) with great breadth and intensity, in clear

breach of the principle of proportionality and therefore breach of Article 52(1) of the Charter.

32- On the same grounds, there is a disproportionate restriction of the rights to reserve the

privacy of private life, the inviolability of communications and the protection of personal data, in violation of the

provided for in paragraph 2 of article 18 of the Constitution of the Portuguese Republic-']7

33. This opinion is not intended to repress the arguments set out therein to justify the relevant

need to reassess Law n-o 3212008, of 7 July, in the light of the CJEU jurisprudence, which has not yet

happened, referring, in this particular, to the aforementioned deliberation, whose content remains totally current.

In fact, a request for review of constitutionality is under consideration by the Constitutional Court

of the aforementioned diploma, submitted by the Ombudsman.

34. However, it is considered essential to reinforce the suggestion of revising this law in the light of the evolution of the

recent jurisprudence of the CJEU, which only confirmed the conclusions contained in the CNPD's deliberation and

introduce new elements of analysis to which the national legislator cannot fail to give significant

importance.

35. Without prejudice to the useful clarifications introduced by the CJEU Judgment of 6 October 2020, in

case C 623117, in particular as regards the delimitation of the exceptions or restrictions allowed by paragraph 1

of Article 15 of Directive 2002/5818, we believe that it is a priority to point out here the conclusions of the CJEU Judgment,

of March 2, in case C:146118, because here the court stopped on the legitimacy of the Ministry

Public authorizing a public authority's access to traffic data and location data for

of criminal instruction.

36. In this case, three questions were asked to the CJEU, and for the present opinion, we will focus only

in the third, for the special relevance it demonstrates.

i7 Gfr. conclusions of the aforementioned deNberation.

i8 Which thus provides: 'Os Eslados{, remember can adopt legislative measures to restrict the scope of the rights and

obligations

presIons in arficles 5"a and 6"6, in articles 1 to 4 of article 8 and in article 9 of this directive, whenever such resIons constitute

an adequate and necessary necessary measure shared in democratic satiety to safeguard national security (i.e., the

Eslado security], defense, asryurançapúôlim, ea prevatso, ainvestigaSo, adetxgão and repressionofhpenalfractionsora

unauthorized use of the electronic communications system as referred to in paragraph 1 of aftiEo t3-o of Directive 95i.46/EC.

For

the effect, the lZember States @wn desrgnantly adapt legblatrvà measures providing that the data sqbm conserved during

a limited period, for the reasons stated in the present number. All the payments referred to in this number shall be

complies with the main principles of Community law, including those mentioned in Article 6(6)(1) and (2) of the Treaty of the

Union

European.""

?^Rt2021t67

5v

\LL:.

37. As the court postulated, the preliminary question was summarized as follows "if article '15.", no. 1, of the Directive 20A2/5B, read in the light of articles 7"",8.",'l'1." and 52.", no." '1 of CAFTA should be uninterpreted in the sense that it opposes the u{in the national regulation that assigns competence to the Public Prosecutor's Office, assigns responsibility and directs the investigation

penaf and exercise, where appropriate, the public action in a postenbr process, to authorize the access of a public authority to traffic data and location data for criminal prosecution purposes.'le

38. Starting from the uncontroversial idea that "it is true that it is up to national law to determine the conditions in that communication and/or electronic service providers must give permission to national authorities competent authorities 0 access to qr. data and available for TUE, to satisfy the requirement of prapartiality, such regulation must provide clear and precise rules that regulate the scope and application of the as far as the cause is concerned and they involve minimal defects, so that people with data will be tired. have sufficient guarantees that make it possible to effectively protect such personal data against the nesks of abuse.'20

39. These "material and procedural" rules must 'be based on effective criteria to define the and the conditions under which access to the data in question must be granted to the competent national authorities"'21 " Being that "it is essential that the access of competent national authorities to the preserved data is in principle, sryetto to a prior inspection carried out Wr a court or administrative entity is independent and that the description of this jurisdictional division or this entry be made in the sequence of a request. substantiated statement of these authorities presented, namely, within the scope of prevention, detection and or criminal prosecution. In case of duly justified urgency, the inspection must be carried out within short'22

40" And, continuing, note, 'This prior inspection requires (*) that the jurisdictional body or the wronged entity to carry out the aforementioned inspection, he has all the attributions and presents all the guarantees necessary to ensure a conciliation of the different interests and rights in question. how much more specifically, to a criminal investigation, such inspection requires that that judicial body or that entity can ensure a fair balance between, on the one hand, the interests linked to the needs of the investigation within the scope of the

iq Cfr" § 46 of the judgment.

20"4e cfr. § ag of the judgment.

?r CYr. §'t9 and 50 of the judgment.

tr Cf. § 51 of the judgment.

PASy2021/67

..-(,(q.-*

.\

fight against crime and, on the other hand, the fundamental rights to respect for privacy and data protection

people of people to quarb access says respect.'n

Hence,'...the independence requirement that the authority in charge of exercising 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 exercise this inspection in an objective and

Impartial, protected from any outside influence. In the criminal field in particular, the requirement for independence

implies (...) that the authority in charge of this prior inspection, on the one hand, is not involved in the

conduct the criminal investigation in question and, on the other hand, has a position of neutrality in relation to the parties

in criminal proceedings.

This is not the case of a Public Prosecutor's Office that directs the investigation and exercises, where appropriate, the public

action. With

In effect, the Public Ministry's mandate is not to decide a dispute with complete independence, but to submit it, if

necessary, to the competent court, as a party to the criminal proceedings.

The circumstance that the Public Prosecutor's Office is obliged, in accordance with the rules that regulate its

competences and their style, to verify the incriminatory and exculpatory elements, to guarantee the legality of the

investigation of the case and to act solely within the terms of the law and according to his conviction, it is not enough to grant

him

the stress of a third party in relation to the interests at issue in the sense described in paragraph 52 of this judgment-

As a result, the Public Ministry is not in a position to carry out the prior inspection referred to in paragraph 51 of the

present judgment.44

41. 0ra, the CJEU is unequivocal in the indispensability of mediation by a judge or independent authority in the access to data kept under Directive 2002t58t}825. This is yet another criterion that joins those already defined by this Court26 and which applies directly to the national context, since here too, '[the] 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 the criminal action guided by the principle of legality and defends democratic legality, under the terms of the Constitution, the present Statute and the Law"27, "enjoy[ing] only] of autonomy in relation to other organs of central, regional and local power'28.

s Cf. § 52 of the judgment-

t+ Cfr- §§ 54 to 57 of the judgment.

25 Conservation that. in Fortugal, it is governed by Law no. 32/2008, of 7 July.

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

I Cfr" article 2" of Law No. 68/2019, of August 27 (Statute of the Public Prosecutor's Office/EMP)_

?8 See Article 3(1) of the EMP.

PAWzAnt67

\Lr'-

42. In the context of this opinion, this means that, first of all, the legislator should take advantage of the opportunity to amend Law No. 32/2008, of 7 July. focusing on a detailed review of the 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 proposed law, to adding a conduct to the catalog of those already existing in the concept of 'serious crimes', provided for in paragraph g) of article 1 of the also called the Data Retention Law, the legislator could and should have expanded the review impetus in order to overcome the current context of unsustainable fragility in which the diploma finds itself.

43" The relationship of this incursion by the CJEU jurisprudence with the proposed changes to the Cybercrime Law, does not

concern the obligation of the national legislator to apply rpsis verbiq to the revision of this law, which is defended for the Data Retention Act. 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 validating and ordering the seizure of mail messages electronic or similar. Now, without delaying the competence of the Member States to define the criminal procedure and internal criminal procedure, the combination of national legal systems with what comes of the European Union - especially when partially or fully linked by obligations to transpose directives - it must at least consider the structural implications arising from Member States' obligations, here. specifically with regard to compliance with the provisions of the Charter of Fundamental Rights of the Union.

44, In the background. the perplexity arises in the face of the pretension of admitting an interference of this level relatively to uncontroversially sensitive data, such as communications, when the CJEU requires well-defined criteria stricter to allow access to other personal data (such as traffic and location)zq. and is reinforced for the manifest contradiction with the provisions of Article 52(1) of the Charter of Fundamental Rights of the Union European.

45- Also in terms of TEDI-| jurisprudence, if it is true that a direct application cannot be made to the present Proposal of the judgments regarding the evaluation of access to communications data by 2q In spite of the fact that the position of the CNPD is completely in line with that of the CJEU, as can be seen in Point II of the aforementioned Deliberation: "In effect,

These are data that reveal aspects of the private and family life of individuals at any given time: allowing for the identification of the citizen's location

throughout the day, all dths (provided that I carry the Íetrernóve/ or other electronic Internet access dÀposrtrvoJ wm quffn ffiNacta

(call * including slowed and unconfirmed - by phone or mobile phone, sends an SMS, MMS, or electronic), duration and legality of these communications and that internet service providers sound."

PARy2021167

part of the secret or information services, the perplexity remains with the projected alteration of the

Article 17 against the provisions of Article 8 of the European Convention on Human Rights.

lll. Conclusion

46. Based on the above grounds, the CNPD understands that:

The. The amendments to article 17 of the Cybercrime Law, as found in the Draft Law in analysis, represent a manifest degradation of the level of protection of citizens in a domain critical of its private sphere, such as communications;

B. By uncontroversially differing from the regime provided for in article 179.0 of the CPP, the Draft Law introduces additional and unsubstantiated restrictions on the rights, liberties and guarantees of inviolability of communications and, reflexively, the protection of personal data, as enshrined in articles 34 and 35 of the CRP, respectively;

ç. Admit that the Public Ministry may, without prior control by the Criminal Instruction Judge, order or validate the seizure of electronic communications or similar records does not protect excessively people who may be suspicious or who have incidentally interacted with these suspects, and the requirement for the intervention of the .iuiz de lnstrução, in the same terms of article 179 of the CPP, can never be seen as distorting the accusatory principle who presides over criminal proceedings in Portugal;

d. Furthermore, and taking into account the content of the recent judgment of the CJEU, of 2 March, in case C-746l1 8, where the possibility of an entity in everything similar - in powers and dependence hierarchical - the Portuguese Public Prosecutor's Office to be able to access traffic and location data, within the framework of a criminal procedure and in implementation of the exceptions provided for in paragraph 1 of article 15 of Directive 20OU58|EC, without prior authorization from a judge or independent entity, can only the proposed amendment to article 17 of the Cybercrime Law is considered inadmissible, as it manifestly contradiction with the provisions of article 52 of the Charter of Fundamental Rights of the Ut (and without waive the provisions of paragraph 2 of article 18 of the CRP).

M Cf. .Accurdam 8rE Srother Watch aN oIFters y. http.//hudoc.echr.coe-inUfre?i=001-1,[071 3) and Judgment

http://hudoc.exec. strain. int/fre?i=004-1 41 34).

the Unrted Kingdom, September 13, 2018 (available at

Raman Zakharoy y. Russra, December 4, 2015 (available at

PAWaA?lt6t

47. Regarding the amendment to Law No. 3212008, of July 7 (Data Retention Law), which is proposed in article 4 of the Proposal, limiting itself to adding a new conduct to those already included in the concept of 'serious crime', as soon as understands that, after the CJEU has declared the Directive that this law transposes invalid and when it is being judged its own constitutionality, the legislative amendment has this content, instead of correcting or supplying the Rules in crisis - Therefore, the CNPD understands that the legislator can only carry out a thorough and meticulous review of the substantive and procedural regime of that law. This is stated as an imperative resulting from the constant jurisprudence of the CJEU and essential condition to overcome the current situation of fragility, to say the least, where the law lies.

Lisbon, I of June 2021

\t(qrs"q"*\

Maria Cândida Guedes de Oliveira (Rapporteur)