NATIONAL COMMISSION

: DATA PROTECTION

OPINION R/2020/117

I - Order

The Committee on Constitutional Affairs, Rights, Freedoms and Guarantees of the Assembly of the Republic asked the National Data Protection Commission (CNPD) to comment on Bill No. 498/XIV/1.a, initiated by the parliamentary group of the PAN - People Animals Nature, which approves the Charter of Digital Rights and a set of complementary measures that ensure the strengthening of citizens' guarantees in the digital domain.

The request made and the present opinion fall within the attributions and powers of the CNPD as the national authority to control the processing of personal data, in accordance with the provisions of subparagraph c) of paragraph 1 of article 57 and paragraph 4 of article 36 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation - RGPD), in conjunction with the provisions of article 3, n. 2 of article 4 and subparagraph a) of paragraph 1 of article 6, all of Law no. internal legal order.

The assessment of the CNPD is limited to the assessment of the rules that provide for or regulate the processing of personal data.

II - Appreciation

The bill in question aims to ensure the strengthening of citizens' guarantees in the digital domain, without limiting the fundamental rights currently provided for in the Constitution and in the law.

However, the draft of the Project seems to forget that many of the rights, here consecrated as digital, are already recognized, and with a well-defined scope, in binding legal instruments for the Portuguese State. And, therefore, consecrated and delimited in such terms that they cannot now, at the national legislative level, be changed, even if in an expansive sense of the subjective positions of the data subjects.

It is from this point that the present analysis begins, without forgetting to highlight that some of the norms of this Project employ concepts whose definition is contained in legal diplomas of Union Law, having therefore a specific meaning, but which are not, by any means,

remission, explained in the text of the Project, which makes it difficult to interpret these rules, including in terms of their scope of application, harming the predictability and legal certainty that rules enshrining rights, which correspond to the obligations of third parties, cannot fail to ensure.

1. Nonconformity of the Project's rules with European Union Law

Throughout the Project, rights are already enshrined, not only in the Constitution of the Portuguese Republic, in the Charter of Fundamental Rights of the European Union and in the European Convention on Human Rights, but also in more specific conventions1 and even in European Union diplomas. directly applicable in the Portuguese legal system, as with the GDPR.

If it is accepted that the Bill does not intend to exclude, in the context of cyberspace, the current rules that enshrine and protect rights, freedoms and guarantees (as provided for in Article 2 of the Bill), the truth is that several of its provisions appear to repeat the rights already provided for and regulated in Union law, especially in the RGPD, with the aggravating factor that they are often written in terms that modify the meaning and scope of these rights.

In this regard, it is recalled that the Court of Justice of the European Union (CJEU) has already censured the practice of replicating the content of Union regulations in national law, subjecting them to national law and, to that extent, also affecting the jurisdiction of the European court. The CJEU underlined that this creates a misunderstanding with regard to the legal nature of the provisions to be applied, reiterating that any implementation modalities that may impede the direct effect of the regulations are contrary to the Treaty.

1 The Council of Europe's Convention 108 for the protection of individuals with regard to the automated processing of personal data should be highlighted, which was amended in 2018 by a protocol already signed by the Portuguese State, but not yet ratified, whose modernized version is commonly referred to as Convention 108+, available at https://rm.coe.int/CoERM PublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808ac91

and, in this way, may jeopardize their uniform application within the Community2.

And as for national rules that distort the meaning of Union law rules, the CJEU specified that the Member States have a duty not to obstruct the direct applicability inherent to the regulations, and strict compliance with this obligation is an indispensable condition for an application uniform and simultaneous implementation of the Regulations throughout the Community.

Now, the Bill under analysis, in an effort to bring together the rights recognized in the Portuguese legal system in the digital context, integrates a set of norms that are presented in disagreement with European Union Law, in terms that put in crisis the primacy of the European Union law and the hierarchy of norms recognized by Article 8(4) of the Constitution of the Portuguese Republic. The CNPD understands that, in accordance with the aforementioned jurisprudence, such rules should be eliminated from the Bill.

However, given that, within the scope of the legislative procedure concerning the implementation of the GDPR, the national legislator opted, in Law no. contravened rules of the RGPD, the CNPD will make recommendations here aimed at alleviating non-compliance with European Union law.

Let's see.

1.1. Firstly, Article 9 stands out, which intends to regulate the right to digital privacy.

Paragraph 4 recognizes a right to protection against illegal profiling.

2Cf. Judgment Commission / ks. Italy (proc. 39/72), point 17, in

http://curia.europa.eu/juris/showPdf.jsf;isessionid=9ea7d2dc30ddbf94149c102f4a878610d7c0bd468c6f.e34Kaxi

Lc3qMb40Rch0SaxyNbxz0?text=&docid&dir&lst=PT =first&part=1& * 3

cid=601673

3 Cf, the Smallpox judgment (proc. 34/73), point 10, in

http://curia.europa.eu/iuris/showPdf.jsf?text=&docid=88457&pageIndex=0&doclang=EN&mode=req&dir=&occ=f

irst&part=1&cid=378305

If this provision alone does not raise reservations, as it implicitly refers to the diploma where the limits to the definition of profiles are defined, which substantially corresponds to the RGPD, the exemplification that follows raises the greatest reservations. There it is explained, as a situation corresponding to a definition of profiles carried out illegally, when the decision-making regarding the natural person or the analysis of their preferences, behavior or attitudes is at stake.

First of all, there seems to be a misunderstanding here: decision-making concerning a natural person is not in itself illegal, nor is the definition of profiles to serve as a basis for decision-making concerning a natural person always contravenes the law or deserves, per se, censorship. Profiling can be legitimately carried out, with the aim of helping to make decisions about natural persons and to analyze their preferences or behavior (cf., for example, the provisions of paragraph 2 f) Article 13(2)(g) of Article 14 and Article 21(1) and (2) of the GDPR).

What will eventually be intended here is the automated definition of profiles - based on information collected in the digital environment, which the standard in question does not make explicit - so it would be useful to refer to the GDPR regarding this concept. But even with regard to this definition (profiiing), what is considered illegal, in certain circumstances, is the automated decision process about a natural person from profiles thus created. However, those circumstances are regulated in Article 22 of the GDPR, and the national legislature, regardless of the goodness of the scope it intends to give to the right enshrined therein, cannot establish a regime different from the regime of Union law, claiming that any and all use of profiling when it comes to making decisions regarding a natural person or analyzing their preferences, behavior or attitudes.

In short, on the one hand, the very concept of profiling used in paragraph 4 of article 9 of the Project only makes sense, within the scope of this Project, if a reference is made to the concept enshrined in paragraph 4) of the Article 4 of the GDPR; on the other hand, the exemplification contained in the final part of that provision contradicts the regime of law enshrined in article 22 of the RGPD, by extending the terms in which the use of these profiles will be considered illegal.

The CNPD therefore recommends the elimination of paragraph 4 of article 9 of the Project, or, if this is not the case, the revision of its wording in terms that do not contradict the provisions of article 22 of the GDPR.

Also within the scope of article 9 of the Project, the imposition, in paragraph 5, of a duty for the Public Administration to use tools and computer systems that guarantee the highest standards of privacy and security is highlighted. Although the CNPD agrees that it should avoid keeping the information with providers that are demonstrably unable to guarantee the confidentiality of the information, it already has serious doubts that the rules of competition and the free provision of services within the European Union or even the European economic area (EEE) are not threatened insofar as it binds the Public Administration to avoid, whenever possible, keeping information on non-national servers. It is therefore recommended that this part be deleted and replaced by the reference to servers located in territories of third countries in relation to the European Union or the EEA, and in any case it must be required that their management is effectively attributed to the entities administrative.

1.2. In relation to article 12 of the Project, the CNPD begins by recalling that there are rules of European Union law that regulate electronic identification, highlighting Regulation (EU) 910/2014 of the European Parliament and of the Council, of 23 July, 2014, so the provisions of paragraph 2 of article 12 cannot fail to be read in the light of such rules.

But it emphasizes above all the provisions of paragraph 4 of article 12. While it is well understood what is intended to be safeguarded here, the ban on the use of a two-dimensional code does not seem to be necessary, nor does it appear to be a sufficient guarantee of the rights of natural persons.

In fact, it is not sufficiently guaranteed because it does not consider the possibility of representing higher-dimensional codes that affect the rights of individuals in the same way, thus running the risk of quickly becoming obsolete. The two-dimensional code, such as the QR Code, can be followed by the use of three-dimensional or n-dimensional codes, which allow the processing of personal data with equal or, possibly, greater intensity and impact. It is therefore important to find a formula that not only avoids the use of two-dimensional codes, but also higher-dimensional codes.

Although it is not unknown that the larger the size, the more information the code contains, it cannot be said, without further ado, that there is a direct relationship between the size of the code and the risk to the rights of holders. Indeed, the introduction of two-dimensional codes,

in addition to the possibility of representing more information, it made it possible, through the use of easily accessible

applications (e.g., using a smartphone), to read the representation of the code. However, it is from the readability of the representation of the codes and, therefore, from the susceptibility of generalized knowledge of the information contained therein, that a greater affectation of the rights of individuals can arise. It is this result that must be avoided.

It is in this perspective, and considering that dimensional codes can be very useful tools, that the CNPD considers the ban on two-dimensional codes, without further ado, to be too radical and unnecessary a measure.

Therefore, the CNPD recommends that, instead of an absolute ban on the use of this type of code, and in line with the security measures provided for in Article 32 of the GDPR, it is allowed, as an alternative to the ban, that representation be subject to to a method of secure encryption of information prior to code generation.

The CNPD dares to suggest the following wording for paragraph 4 of article 12 of the Project: Any form of use of a two-dimensional code, or of a higher dimension, to process information on health status or any other aspect related to the rights of natural persons, sa/vo if secure encryption is applied to the information prior to the generation of the code.

1.3. Still regarding the rights enshrined in the GDPR and which are reaffirmed in the Project in the digital context, it is now important to analyze the right provided for in Article 13 of the Project.

Firstly, it is pointed out that the designation of the right as the right to be forgotten is not the most appropriate (even if it is popularized), since the meaning of the right corresponds to a claim “to be forgotten” (cf. 17 of the GDPR), which does not contradict the right to memory. The CNPD therefore recommends changing the heading of Article 13 of the Project to Right to be forgotten.

Second, the CNPD reiterates its concern for the legislative option of seeking to reproduce the rules of the RGPD in the specific digital context with the risk of distorting the scope of the law defined in that diploma, and that the reference to the “terms of the law” may not be enough to get rid of it. Take, for example, the mention in paragraph 1 of article 13 of the Project, among a short list of reasons justifying this right, to “for another reason

relevant". Such reference seems to leave a discretionary space for the applicator of the legal norm, when in fact the grounds for the ownership and exercise of this right are exhaustively listed in paragraph 1 of article 17 of the RGPD and in more

extensive terms than those listed here.

Once again, it is recommended that, if the reference to this right is persisted in the context of this Draft diploma, one should refer to the grounds or reasons provided for in article 17 of the RGPD.

With regard to paragraph 2 of the same article 13 of the Project, it is recommended to revise the wording of the same, as it involves an interpretation that would go beyond the scope of the right to disassociate the result of a search from the name of the data subject in the search engine, as recognized by the CJEU4 and enshrined in the aforementioned article 17 of the GDPR.

In fact, the current wording allows the interpretation that the search in the digital source which contains information about the data subject cannot be carried out based on the name of the data subject, when the rationale of the rule seems to be to recognize that the right elimination of search engine results based on the name of the holder does not affect a search in the search engine based on a term other than the name of the holder. It is important here to distinguish, due to the completely different impact it has on the rights of the holders, a search carried out in a search engine of national or international scope, or a search limited only to a website and, therefore, only aggregating the information contained in that website. website and not the entire Internet.

The CNPD therefore recommends a clarification of the wording of this paragraph 2 of article 13 of the Project.

Thirdly, the imposition, in paragraph 3 of article 13, of the exercise of the right to erase personal data provided to social networks or information society services using a simple digital form and its guarantee within a reasonable period, will further than Article 12 of the GDPR stipulates - in binding terms for the Member States. It imposes on the controller the obligation to facilitate the exercise of the rights, and

4 Cf. Judgment Goog/e Spain SL Goog/e tnc v. Agencia Espanda de Protección de Datos, of May 13, 2014, in case C-131/12.

a maximum period of one month is determined from the receipt of the request, which may be extended (see Article 12(2) and (3) of the GDPR).

Furthermore, the grounds for deleting personal data are being limited to cases of obsolete or inaccurate data, which, it is reiterated, grossly contradicts the provisions of Article 17(1) of the GDPR.

Furthermore, the CNPD draws attention to the delimitation of the context in which this right is intended to be regulated, since the concept of information society services has a well-defined meaning in Directive (EU) 2015/1535, of the European Parliament and the Council, and no similar services are achieved. Reasons of predictability of legal norms justify, therefore, rigor in the concepts used and their clarification.

To that extent, the rule must be eliminated or revised, as it imposes the means of fulfilling the obligation when the GDPR has not done so and because it refers to a reasonable period that has already been implemented by the European legislator, in disregard of article 12. of the GDPR, and also for restricting the scope of the right to erasure of personal data provided for in article 17 of the GDPR.

Finally, the scope of paragraph 4 of article 13 of the Project is not understood. The provision that data concerning minors will be deleted without the limitation provided for in the previous number can refer to the requirement of a digital form for the exercise of the right and its guarantee within a reasonable period, as well as the grounds for exercising the right. of that right, which in paragraph 3 are limited to the inaccuracy or obsolete nature of the data. It is therefore important to clarify the meaning of the rule.

In any case, whatever its meaning, this provision is unnecessary, as the right to erase the personal data of minors collected in the context of offering information services referred to in Article 8(1) of the GDPR, is enshrined in subparagraph f) of paragraph 1 of article 17 of the same diploma.

1.4. Note also paragraph 1 of article 14 of the Project, when it refers to the right of users of digital platforms, over-the-top and similar services to obtain a copy of the data concerning them interoperable way and the erasure of this data on the platform.

Firstly, for reasons of normative predictability, it would be appropriate to define, for the purposes of this law, the concept of digital platforms and over-the-top services, so that, from the outset, it is possible to understand what similar services correspond to, under penalty of lack of predictability and legal certainty of this legal regime. In any case, the right that seems to

be at issue here is the right to data portability, enshrined in article 20 of the GDPR, which, here, because it refers to the change in contractual conditions, falls under point a) of Article 20(1) of the GDPR, but restricted to the processing of personal data carried out on the basis of a contract.

However, the right to portability does not necessarily imply the deletion of personal data by the controller. The right to erasure exists in the cases provided for in paragraph 1 of article 17 of the RGPD and, for what is relevant here, it can be affirmed when the basis of lawfulness of the treatment ceases or the data are no longer necessary (for having terminated the contractual relationship). There are simply circumstances, in accordance with paragraph 3 of article 17, that may justify the retention of data (e.g. to defend rights in legal proceedings, to comply with legal obligations in tax matters and to combat money laundering of capital).

While it is true that the national legislator may create legal obligations to delete data, under the terms of subparagraph e) of paragraph 1 of article 17 of the RGPD, the CNPD nevertheless recalls that there may be reasons for the retention of data. , therefore recommending that this provision be re-weighted.

1.5. With regard to the right to protection against abusive geolocation, enshrined in article 16 of the Project, the CNPD begins by insisting, once again, on the need to clarify the concepts used, which actually correspond to defined concepts in diplomas of Union law.

This is the case with several terms used in this article (for example, the concept of call), which refer to the Electronic Communications Privacy Law (Law no. 46/2012, of 29 August), which transposed the e-Privacy Directive (Directive 2002/58/EC, of the European Parliament and of the Council, of 12 July, on the processing of personal data and the protection of privacy in the electronic communications sector, with the amendments introduced by Directive 2009/136/EC, of the European Parliament and of the Council, of 25 November).

Since the CNPD does not have reservations about the general provisions of this article, it believes, however, that the wording of paragraph 2 needs clarification and revision.

It follows from this precept that personal geolocation data, within the scope of mobile or fixed public networks, can only be used by legally competent authorities in the fields of civil protection, public health and criminal investigation.

It so happens that the regime for the processing of this data is regulated in the Electronic Communications Privacy Law, which transposed the e-Privacy Directive, where the processing of geolocation data by electronic communications operators is allowed in certain circumstances (cf. article 7 of the Electronic Communications Privacy Act). However, as it is worded, Article 16(2) of the Project seems to prohibit the processing of such data in the cases provided for in Article 7 of that national law, which would count the e-Privacy Directive.

On the other hand, authorization for the processing of these data by the legally competent authorities in the fields of civil protection, public health and criminal investigation broadens the universe of entities legitimized by Law No. 41/2004 (Article 7(2)) and by the e-Privacy Directive itself (Article 10(b) and Recital 36) to process geolocation data: in these diplomas only authorities competent by law to receive and respond to emergency calls are authorized to process such data and not all authorities responsible for civil protection and public health.

Although the e-Privacy Directive recognizes, in its article 15, the Member States have the power to, by law, restrict the rights to the inviolability and confidentiality of electronic communications, traffic data and geolocation data, that restriction must prove to be adequate, necessary and not excessive in relation to the purposes pursued, since it involves the restriction of the fundamental rights to respect for private life and the inviolability of communications, enshrined in Article 7 of the Charter of Fundamental Rights , and in articles 26 and 34 of the Portuguese Constitution. Especially in the open, non-detailed terms, in which such access is foreseen. Also taking into account that this rule derogates from paragraph b) of article 10 of the Directive and partially amends the provisions of paragraph 2 of article 7 of Law no. reasons does not expressly mention it, nor is the suitability and need to expand the universe of administrative entities with the power to know location data in the context of electronic communications demonstrated.

The CNPD recommends, therefore, that the provisions of Article 15(2) be considered, stressing that it reflects the partial derogation of rules provided for in Law No. 41/2004 and in the e-Privacy Directive, and that, also because of the open terms in

which access is provided, it seems to violate the principle of proportionality (cf. Article 18(2) of the CRP and Article 52(1) of the Charter).

2. Analysis of other legal provisions

Still from the perspective of the compatibility of the Project rules with the personal data protection and personal data security regime, the CNPD draws attention to the following aspects of the regime.

2.1. Firstly, a short observation regarding the regime enshrined in article 7 of the Project, which enshrines the right to protection against on-Une disinformation.

No. 3 of this article presents the definition of the concept in question, specifying that it presupposes the susceptibility to cause public harm, indicating, by way of example, threats to democratic political processes. It is further specified in subparagraph e) of no. 4 that political or commercial communications addressed to organized trolling are considered to be demonstrably false or misleading information.

The CNPD recognizes the sensitivity of the process of harmonizing fundamental rights to freedom of expression with other fundamental rights or constitutionally relevant interests and, specifically, the difficulty of this conciliation with the objective of public protection against online disinformation.

In any case, taking into account that the purpose here is specifically to regulate protection against disinformation in the context of political campaigns or that affect democratic political processes, the CNPD recalls that the exercise of the right to freedom of expression and opinion may involve the treatment of personal data (e.g., the use of this data, especially in the context of profiling processes based on personal information collected on social networks), underlining that in the specific context of the political campaign the European Union provided for a sanctioning regime only when the disinformation process based on, or taking advantage of, the violation of personal data protection rules - cf. Article 10-A of Regulation (EU/Euratom) 1141/2014 of the Parliament

European Parliament and Council of 22 October 2014, last amended by Regulation (EU/Euratom) 2019/493 of the European Parliament and of the Council of 25 March 20195.

2.2. In article 8 of the Project, regarding the right of citizens to participate in public activity, paragraph 3 provides for the duty to

record in video support of the meetings of the Assembly of the Republic, municipal assemblies and municipal councils. , when these are public meetings, as well as their disclosure in free access on the respective Internet portal. Paragraph 4 also provides for the live transmission of these meetings of the aforementioned municipal bodies through the portal or another digital platform.

Understanding the public interest in publicizing the public meetings of municipal bodies, the CNPD recalls that these meetings have a very different characteristic from the meetings of the Assembly of the Republic. It is because in these, citizens either do not have active participation, or when they participate, they do not do so as citizens to expose their needs or their personal perspectives on public needs, but rather as representatives of public or private entities or as experts in a particular field.

Contrary to what happens in public meetings of municipal assemblies and municipal councils, which allow, in legal terms, the intervention of citizens in the meetings in terms that easily result in the exposure of private and family life.

It is therefore important here, in this context, to consider the risks of exposure and improper reuse of images and statements made by citizens in this context, a consideration that must be made bearing in mind the personal data protection regime contained in the RGPD and Law n. 58/2019, of August 8th. In fact, the concern shown in this Bill, in particular, in Article 7, with the manipulation of videos and trolling, cannot fail to be felt here too intensely.

In this sense, the CNPD recommends reconsidering the balance between the fundamental rights at issue here, underlining the importance of, in this context, respecting the principles and basic rules of the GDPR.

Under the terms of the GDPR, although this legal rule may constitute the basis for the lawfulness of this processing of personal data, it cannot be without guarantees.

5 https://eur-lex.europa.eu/legaI-content/PT/TXT/PDF/?uri=CELEX:02014R114l-20190327&from=EN

of citizens' rights. In particular, the principle of minimization of personal data, enshrined in subparagraph c) of paragraph 1 of article 5 of the GDPR, must be considered and implemented here, in the light of which the limitation of recording appears to be justified, and above all the on-Une transmission and the permanent availability on the Internet of the recording, to the interventions of citizens who expressly and freely consent to it, it being evident that, in any case, it is essential to ensure a

complete right to information and with a clear definition of the conditions for the online dissemination of their declarations (cf. article 13 of the RGPD). Otherwise, the fundamental right to privacy can be seriously affected, above all, it is insisted, taking into account the nature of citizens' interventions at municipal bodies meetings and the risks associated with the permanent availability of this type of information on the Internet. .

Thus, the CNPD recommends the elimination of the legal imposition contained in paragraphs 3 and 4 of article 8, or, if it persists in its maintenance, the provision of guarantees of citizens' rights, in accordance with the provisions of the RGPD .

2.3. In paragraph 5 of article 12 of the Project, there is a duty to respect the indication of the holder of personal profiles on social networks or similar regarding the possible deletion of the same after his death.

The rule needs further densification, namely by specifying the appropriate means for demonstrating that will by the data subject, as well as with whom such an expression of will can be formulated (e.g. the person responsible for the social network in question).

This recommendation is based on the difficulties that have been experienced by those responsible for the processing of personal data in verifying the assumptions for the application of paragraphs 2 and 3 of article 17 of Law no. August, concerning the exercise of rights relating to the processing of data of deceased persons.

Therefore, it is insisted, under penalty of this Project norm also running the risk of unenforceability, in its densification.

2.4. Recognizing the importance of affirming the rights of citizens in the interaction with the Public Administration through electronic means, the CNPD here points out some reservations to the terms of its provision in article 17 of the Project.

First, it notes that the generic provision of a right not to repeat the provision of data already provided, needs to be further densified, first of all with regard to the recipient of that provision. Although the political-legislative tendency is to guarantee the interoperability of the information available in the Public Administration, there are constraints that have to be considered, also for reasons of security of the information systems, so the desirable simplification of the interaction between the citizens and the Public Administration knows, in fact, limits.

The same can be said of the right to adopt a digital administrative procedure. The transformation of the decision-making administrative activity of the Public Administration into an exclusively electronic model has been progressive, not only because

of the economic costs, which not all public entities are able to immediately bear, but also because of the information security guarantees and the information systems that cannot be neglected. This norm should be affirmed more as a principle or programmatic norm than as an immediately enforceable right, because the security of the Public Administration's information systems (and with that the security of the Portuguese State itself, as well as the privacy of citizens) is not compatible with the immediate guarantee of such right.

The CNPD therefore recommends a densification of the rights provided for in paragraphs a) and d), in order to safeguard the security of information and the information systems of the Public Administration.

Thirdly, the right to benefit from “Open Data” schemes that provide access to data contained in public service computer applications and allow their reuse, enshrined in article 17(e) of the Project, is provided for with a degree of indeterminacy not compatible with the predictability, proportionality and legal certainty that a legal rule attributing rights must be endowed with, especially when, as is the case here, the affirmation of that right is liable to restrict other fundamental rights.

In fact, in the absence of an explanation of the concept of open data, it is essential to delimit the set of information existing in IT service applications.

public, under penalty of enshrining a right of open access to personal data. This cannot certainly be the meaning of the consecration of this right of access, because it is, from the outset, delimited, among other diplomas, by the Code of Administrative Procedure and by Law No. 26/2016, of 22 August, and Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of information in the public sector (recast).

For this reason, the CNPD recommends clarifying the wording of subparagraph e) of article 17 of the Project, suggesting that it be added, eventually, at the end, as provided for in iei.

2.5. Finally, the provisions of article 18 of the Project are considered.

There, a set of duties of the Public Administration in digital matters are foreseen, not all of them presented with the same degree of clarity and, above all, many of them difficult to implement.

It is, of course, the case of the duty to create graphic notification systems of all administrative acts and administrative

regulations addressed to consumers, referred to in paragraph b). Here, too, it seems essential to explain, in the standard, the concept of graphic systems. Assuming that it refers to a visual system that can be interpreted directly by a user, leading back to a portal, the CNPD recommends imposing the duty to adopt measures that guarantee the confidentiality of the personal data of each citizen.

Furthermore, the question remains whether the duty to create graphic notification systems is restricted to the relationship between the Public Administration and consumers, or whether the reference at the end of the paragraph to consumers is restricted to administrative regulations. Even so, it is not understood which universe of consumers is at issue here (e.g., consumers of goods and services provided by the Public Administration, consumers of essential goods and services provided by private entities), and consequently which universe of administrative regulations are subject to notification. , since this form of communication is, under the terms of the Administrative Procedure Code, reserved for administrative acts.

But execution difficulties can be accentuated with regard to the duty to migrate all software to open-source, referred to in paragraph d), due to the complexity of ensuring, in this type of software, the necessary updates and interoperability with

r

other systems. To that extent, the CNPD recommends that this legal imposition be rethought, and that, at least, the requirement to guarantee interoperability with other systems be added at the end of the paragraph.

III - Conclusion

1. Although recognizing the value of a diploma that aims to bring together all rights in the digital context, the CNPD cannot fail to point out the rules that repeat rights regulated by rules of European Union law, in disagreement with the jurisprudence of the CJEU, some of the which, seeking to replicate rights already recognized in the RGPD, change the content of these rights, by innovating where the RGPD exhaustively defines their assumptions or by distorting their meaning or scope of application, in contradiction with Union Law. Notwithstanding that the CNPD understands that such norms should be eliminated from the Bill, it presents recommendations that aim to reduce the non-compliance with Union Law.

In addition, some of the norms foreseen in the Bill of Law employ concepts whose definition is contained in legal diplomas of Union Law, having therefore a specific meaning, but which are not, even by reference, explained in the Articles of the Project,

thus hindering their interpretation and affecting the predictability and legal certainty required of rules enshrining rights to which third-party obligations correspond.

Thus, the CNPD, in the light of these arguments and the specific reasons set out above, regarding the rules listed below, the CNPD recommends:

a) The elimination of paragraph 4 of article 9 of the Project, or, if not understood, its wording in terms that do not contradict the provisions of article 22 of the GDPR;

b) Amendment of the wording of paragraph 4 of article 12, with the introduction of the terms marked in italics: Any form of use of a two-dimensional code, or of a higher dimension, to process information on the state of health or any other other aspects related to the rights of natural persons, unless secure encryption is applied to the information prior to the generation of the code.;

c) In article 13:

i. The revision of paragraph 1, referring to the grounds for the right to be forgotten provided for in article 17 of the GDPR;

ii. Clarification of the wording of paragraph 2;

iii. The elimination of paragraph 3, or, if this is not the case, its revision in terms that do not contradict the provisions of paragraphs 2 and 3 of article 12 of the GDPR, nor restrict the grounds for the right to erasure of personal data provided for in Article 17 of the GDPR;

iv. The deletion of paragraph 4, as it adds nothing in relation to paragraph f) of paragraph 1 of article 17 of the GDPR;

d) In paragraph 1 of article 14, the reconsideration of the provision of a right to erasure of data within the scope of digital platforms, in the light of the exceptions provided for in paragraph 3 of article 17 of the GDPR;

e) In article 16, the reconsideration of the provisions of paragraph 2, emphasizing that it reflects the partial derogation of the rules provided for in Law no. that access is provided for appears to violate the principle of proportionality (cf. Article 18(2) of the CRP and Article 52(1) of the Charter).

2. The CNPD, on the grounds set out in point II.2., also recommends:

a) The elimination of the legal imposition contained in paragraphs 3 and 4 of article 8, or, if it continues to be maintained, the provision of guarantees for the rights of citizens, in accordance with the provisions of the RGPD, namely limiting the recording and, above all, the transmission and availability on the Internet, of the interventions of citizens who have expressly and freely consented to it;

b) The densification of paragraph 5 of article 12, either in order to specify the means and with whom such expression of will by the holder of personal profiles on social networks can be made in relation to the post-mortem deletion of such profiles;

c) Densification of the rights provided for in paragraphs a) and d) of article 17 of the Project, to safeguard the security of information and information systems of the Public Administration; and

d) Clarification of the wording of subparagraph e) of article 17 of the Project, suggesting that it be added, eventually at the end, under the terms provided for by law;

e) Clarification and reconsideration of some of the duties provided for in article 18, due to the difficulty in enforceability, and in particular:

i. In paragraph b) of article 18, the clarification of its wording, and the provision of a duty to adopt measures that guarantee the confidentiality of the personal data of each citizen;

ii. In subparagraph d), at least the requirement to guarantee interoperability with other systems is added at the end.

Approved at the meeting of September 28, 2020

Filipa Calvão (President)