/ NATIONAL COMMISSION ON DATA PROTECTION

OPINION/2020/129

I. Order

The President of the Committee on Constitutional Affairs, Rights, Freedoms and Guarantees of the Assembly of the Republic requested, on October 21, 2020, the National Data Protection Commission (CNPD) to comment on Draft Law No. /2.a (GOV), which determines the mandatory use of a mask or visor to access or stay in public spaces and roads and the mandatory use of the S TA YA WA Y CO Vi D application in a work or similar context, school and academic, as well as on Bill No. 570/XIV/2.a, which determines the transitory imposition of the mandatory use of a mask in public spaces.

The request made and the present opinion fall within the attributions and powers of the CNPD, as the national authority for the control of the processing of personal data, in accordance with the provisions of subparagraph c) of paragraph 1 of article 57 and n. 4 of article 36 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Regulation on Data Protection - RGPD), in conjunction with the provisions of article 3. , in Article 4(2) and Article 6(1)(a), all of Law No. 58/2019, of August 8 (which aims to ensure the execution , in the domestic legal order, of the GDPR).

In accordance with its attributions and powers, the CNPD pronounces itself on all the rules that provide for or imply processing of personal data.

Since Bill No. 570/XIV/2.a was, in the meantime, approved1, the CNPD limits its analysis to Draft Law No. 62/XIV/2.a, in the part relating to the STAYAWAY application COVID, making only recommendations regarding the implementation of the rules contained in that Project.

II. appreciation

A. Mandatory use of the STAYAWAY COVID application and introduction of the legitimation code

1 Cf. Law No. 62-A/2020, published on the date of approval of this opinion.

r

The Draft Law, in article 4, determines the mandatory use of a mask or visor to access or stay in public spaces and roads and

the mandatory use of the STA YAWA Y COViD application in a work or similar, school and academic context. . And it especially binds workers in public functions, employees and agents of the Public Administration, including the state, regional and local business sector, professionals from the Armed Forces and security forces.

In order to guarantee the feasibility of this measure, it is also necessary, in paragraph 3 of article 4, for the user to insert in the application the pseudorandom legitimation code, which must appear in the report containing the test result. diagnostic laboratory.

Before starting the analysis of the proposed diploma, the CNPD makes two observations.

The first concerns the form of the present draft diploma. At issue is a draft law, as it deals with a matter relating to rights, freedoms and guarantees, reserved for the legislative competence of the Assembly of the Republic, in accordance with the provisions of paragraph b) of paragraph 1 of article 165 and of Article 18(3) of the Constitution of the Portuguese Republic (CRP). The CNPD thus emphasizes that, this time, possibly due to the highly restrictive content of the rights that the proposal presents, it has chosen to submit to the national Parliament the definition of the regime for this processing of personal data. The definition of rules on the exercise of rights, freedoms and guarantees and, in particular, restrictive rules must be the object of a broad public debate, which cannot fail to take place, from the outset, in what is the national democratic space. for excellence. It is a pity that the proposed diploma was not accompanied by an impact study on the protection of personal data, as required by paragraph 4 of article 18 of Law n.° 43/2004, of 18 August, as amended finally by Law No. 58/2019, of 8 August.

The second observation aims to underline that the CNPD understands the need to define adequate measures to safeguard the public interest of public health and to safeguard the fundamental rights to life and physical integrity, which may imply restrictions on other fundamental rights, such as the right to to freedom and privacy. It cannot fail to emphasize, however, that such restrictions must reflect a balance between the different rights and values that are constitutionally protected, and cannot go beyond the ultimate limit of respect for the essential content of rights, freedoms and guarantees, within the framework of the democratic rule of law. in which we move.

*J7%

jf NATIONAL COMMISSION ON DATA PROTECTION

Thus, aware of the need to harmonize the different values and rights in tension, the CNPD, in an effort to understand the purpose and (practical) scope of the restrictive measures now proposed, seeks, through this opinion, to contribute to the definition of a that safeguards, to the appropriate and sufficient extent, the rights, freedoms and guarantees of natural persons in the context of the processing of personal data.

1. Prior point: STAYWAY COVID, the GAEN interface and the voluntary nature of using the application

STAYWAY COVID is a digital proximity tracking system (contact tracing)2, available for personal mobile devices with iOS or Android operating systems, using Biuetooth technology as a proximity sensor, specifically with low energy consumption (Biuetooth Low Energy.

From a technical point of view, STAYAWAY COVID assumes itself, not so much as a screening solution, but more as an application for notification of individual exposure to contagion risk factors. Its objective is precisely to be able to inform an application user that their mobile device was at a distance of less than 2 meters, for more than 15 minutes, from the device of another person using the application who was later diagnosed with COVID. -19, with a risk of contamination, given the physical proximity and duration of contact.

It is also recalled that the STAYAWAY COVID application is based on a decentralized system for processing personal data (in other words, it is on each user's mobile phone that information about proximity contacts with other users is generated and stored, information that is pseudonymized), which makes it possible to mitigate the impact on privacy and the risk of misuse of this data, which, if associated with the information that the user is a carrier of the virus, can generate discriminatory treatments.

2 According to the World Health Organization (WHO), proximity screening is the process of identifying, evaluating and managing people who have been exposed to a disease in order to prevent its transmission; when systematically applied, proximity screening will interrupt chains of contagion, thus becoming an essential public health tool in controlling infectious disease outbreaks -cf.https://www.who.int/publications/i/ item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

It is therefore important to make it clear that the STAYAWAY COVID system essentially treats pseudonymized data, which are personal data, under the terms of paragraphs 1) and 5) of article 4 of the GDPR, since they allow, by relationship with other information , identify the person concerned.

However, in this system, the IP address (Internet Protocot) of the user's equipment is also specifically processed whenever it communicates with the Diagnostic Legitimation Service and the Diagnostic Publication Service. It is recalled that the IP address is personal data, as it makes it possible to identify, without disproportionate effort or cost, who was the person who accessed the server via the Internet (cf. point 1) of article 4 of the GDPR and jurisprudence of the Court of Justice of the European Union (Case Breyer, C-582/14, points 44-49, ECLI:EU:C_2016:779).

Note that, even without resorting to information held by third parties to identify the user, the IP address immediately allows to know an approximate geographic location of the users3 4. It should also be noted that the users of the application access the Diagnostic Publishing Service daily , four times, and that, in addition, some users can be referred to as people with a positive diagnosis of COVID-19, when they authenticate to send the respective TEK (Temporary Exposure Ke^)A. In fact, the entity that developed this application in Portugal has always assumed, in the documentation sent to the CNPD, the existence of processing of personal data.

Furthermore, even though the Bluetooth Device Address and the Rolling Proximity Identifier are updated and randomized, the circumstance that such operations are very unlikely to occur simultaneously (i.e., in exactly the same minute and second) makes them relatable, thus allowing, for example, , traceability by third parties who have systems (antennas) that read those signals.

Thus, within the scope of its attributions and competences regarding the processing of personal data, the CNPD pronounced itself, in the context of prior control, regarding the impact assessment on the

3 In case users access from an institution where they work, for example, the IP may also reveal the user's association with that institution.

4 The initial TEK key is generated on the first run of the personal mobile device after the application starts up, using the native pseudorandom number generators of the Android{Java) and iOS (Swif()) platforms. The TEK keys are stored on the respective device mobile for 14 days.

data protection, in Deliberation/2020/2775. And issued an opinion on the legal diploma that came to regulate some aspects of

this processing of personal data - cf. Decree-Law No. 52/2020, of August 116.

However, as the CNPD explained in the aforementioned Deliberation7, although the use of B/uetooth technology is less intrusive than a technology that allows the immediate recording of the user's location, Google's Android electronic devices made the operation of Bluetooth technology dependent on the collection (permanent) of the location data, thus allowing the tracking by this company, for other purposes, of the location and movements of the users of the application.

In fact, Google and Apple created an interface (GAEN) to enable the operation of proximity tracking applications, providing access to functionalities at the operating system level of the mobile device, such as access to the B/uetooth component, the generation of keys and pseudorandom identifiers and their crossing to calculate the risk, which are not performed by the application. With this, a substantial part of the data processing is not controlled by the controller (the Directorate-General for Health), but by a partnership of two of the largest private technology companies.

This is also one of the reasons why the use of the application was only considered legitimate in the national legal system if its use depended exclusively on the will of the citizens, the same applying to the introduction of the legitimation code, which triggers the contagion risk alert with the of application users who have been registered as having been close to the user who has the virus. In fact, those companies only provide the interface (GAEN) if the installation of the contact tracing application is voluntary.

In fact, as will be better explained below, it was the fact that the use of the application (and the introduction of the code) was voluntary that allowed, at an early stage of the pandemic, in which there was general uncertainty as to the means capable of combating it, not to question the proportionality of the restriction on fundamental rights to the reservation of private life and the protection of personal data, since the fact that the provision of personal data is in the

5 Cf. §§ 87 and 89.

6 Cf. Opinion/2020/82, of July 21, available at https://www.cnpd.pt/home/decisoes/Par/PAR_2020_82.pdf

7 Cf. §§ 87 and 89.

citizen availability softens the degree of demand in demonstrating the suitability and necessity of this processing of personal

data in order to achieve the intended purpose of breaking the chain of contagions more quickly.

For all these reasons, the CNPD insisted on the voluntary nature of the use of the application in the aforementioned Decision, in line with the position taken in Guidelines no. and means of screening contacts in the context of the COViD-198 outbreak.

Thus, Decree-Law No. 52/2020, of 11 August, which provided a legal framework for some aspects of the processing of personal data carried out by the STAYAWAY COVID application, assumes in article 1 (final part) and in the paragraph 1 of article 4 the voluntary nature of the use of the application and the insertion of the information that one is infected by the virus.

It should be noted that in the aforementioned legal diploma, in article 2, it is foreseen that the application must respect the European and national legislation applicable to the protection of personal data, as well as the European initiatives adopted in the context of combating COViD-19 through the use of solutions based on personal data, namely [...] the Guidelines n.0 4/2020, of the European Data Protection Committee, on the use of location data and means of tracking contacts in the context of the outbreak of COVID-19.

Strangely, the Draft Law now makes a clean slate of what was defined in the aforementioned Decree-Law and of the understanding, expressed in the Guidelines that the Government (in the aforementioned diploma) says it follows, that one of the requirements considered essential, in the light of the legislation European and national protection of personal data, is the voluntary nature of the use of the application9. These Guidelines state that the “systematic and large-scale monitoring of the location and/or contacts between individuals constitutes a serious intrusion on their privacy. Tai can only be legitimized if it relies on a voluntary adoption by users for each of the respective purposes. This would imply, in particular, that individuals who choose not to or cannot use such

8 Cf. in particular §§ 8, 24, 31 and 43 of Guidelines No. 4/2020 of the European Data Protection Board available at https://www.cnpd.pt/home/orientacoes/Diretrizes_4-2020_contact_tracing_covid_with_annex_en_PT.pdf

9 Cf. §§ 8, 24, 31 and 43 of Guidelines No. 4/2020 of the European Data Protection Committee, available at https://www.cnpd.pt/home/orientacoes/Diretrizes_4-2020_contact_tracing_covid_with_annex_en_PT.pdf

applications should not suffer any disadvantage."10.

Having made this clarification, in particular regarding the impact that the use of the STAYAWAY COVID application, despite the mitigating measures adopted, has on people's privacy, it is now important to consider the change that this Draft Law intends to introduce, by eliminating the voluntary nature the use of the application and the insertion in the application of the legitimation code, imposing the obligation of such measures.

2. The mandatory use of the application and the fundamental rights to freedom, respect for private life (in electronic communications) and the protection of personal data, as well as the fundamental right to non-discrimination

In particular, it is important to consider the impact of the legal imposition of such duties on the fundamental rights to freedom, the reserve or respect for private life, the inviolability of electronic communications and the protection of personal data - rights enshrined in Articles 26, 27. 34 and 35 of the Constitution of the Portuguese Republic (hereinafter, CRP) and in articles 6, 7 and 8 of the Charter of Fundamental Rights of the European Union (hereinafter, Charter). Under the terms defined in these fundamental diplomas, the restriction of rights, freedoms and guarantees is only admissible if it respects the principle of proportionality, which implies that the adequacy, necessity and non-excessive character of the restriction is demonstrated, and provided that it does not affect the essential content. of rights - cf. Article 18(2) and (3) of the CRP and Article 52(1) of the Charter.

Now, the Draft Law not only imposes the duty to use the application and the duty to insert the legitimation code (which corresponds to a personal health data), establishing a sanctioning framework (offence) for non-compliance, but also assigns the power of inspection to the security forces and services and also to the Maritime Police and the Municipal Police.

2.1. The imposition of use of the application and the forecast of the power of inspection

10 § 24 of Directives No. 4/2020 of the European Data Protection Committee, already cited, italics added.

The impact on fundamental rights does not only result from the imposition of the use and availability of proximity information (and even the location of users of some types of smartphones) and information related to the health of users. It goes further, due to access and consultation, by law enforcement agencies, of information regarding the content downloaded on smartphones and other interactions carried out in the context of this application and, therefore, due to access to electronic

communications that the aforementioned power of supervision implies. Indeed, the concept of electronic communication encompasses “any information exchanged or sent between a finite number of parties using a publicly available electronic communications service”™.

Clearly, these are restrictive provisions of fundamental rights and which prove to be disproportionate, in breach of the provisions of Article 18(2) of the CRP and Article 52(1) of the Charter. Let's see why.

First of all, pay attention to the imposition on citizens to use an application on electronic equipment. Such imposition obviously implies the restriction of the right to freedom regarding the contents of our electronic equipment and regarding the interactions that we make in the context of their use. Basically, it translates a violation of the free will that each one is recognized in any democratic State of Law.

However, when this imposition is added to the provision for inspection of compliance by different agents of police entities (according to the provisions of article 5 of the Proposal, the Public Security Police, the National Republican Guard, the Maritime Police and the Municipal Police), also means the restriction of the right to the inviolability of electronic communications, enshrined in Article 34 of the CRP and in Article 7 of the Charter, insofar as the verification of compliance with this duty implies the power of a agent of a police entity knows or requires any citizen to:

1. ° Show if you have a cell phone with you;

2. ° Unlock it, at the risk of the agent knowing the code, and allow the agent *

"Cf, subparagraph a) of paragraph 1 of article 2 of the Law on Privacy in Electronic Communications (Law no. 41/2004, of 18 August, amended by Law no. August, in transposition of European Directives).

check its typology, especially if it is a smartphone and which version of this equipment (hardware and software)12;

3. ° Show if you have downloaded the application, with the risk of showing other applications that may have been installed;

4. ° Demonstrate that you keep Bluetooth active.

This implies, therefore, the obligation to expose to a police officer the interactions that each one makes on their smartphone and, before that, the obligation to demonstrate whether or not they have a device of this type in a version of the operating

system that supports this application. .

It is believed that the description of the different steps to be taken to effectively monitor compliance with this duty is sufficient to understand the degree of interference in citizens' electronic communications and in their privacy. It is also sufficient to understand that the provision of this obligation is in clear contradiction with paragraph 4 of article 34 of the CRP, where interference by public authorities in correspondence, telecommunications and other means of communication is prohibited, unless the cases provided for in the iei in terms of criminal proceedings.

Moreover, if there were any doubts as to the inadmissibility of such interference in electronic communications for the prevention and detection of illicit acts of mere social order, it was sufficient to pay attention to the General Regime for Administrative Offenses and Fines (herein subsidiary applicable by determination of article 7 of the Draft Law), which, in Article 42, prohibits intrusions into correspondence and the means of telecommunications.

Even if another way of carrying out the inspection provided for in the Draft Law were found, this would imply providing the different police entities (including the Municipal Police) with information on who installed the application and on who inserted the legitimation code, which translates into a an equally serious interference with the privacy of citizens in the context of electronic communications.

In addition to the fact that, currently, the private life of each one is, in essence or, at least, in many aspects and dimensions, mirrored in their mobile phone,

12 This is because, as the CNPD pointed out in its Deliberation/2020/277, of 29 June, not all smartphones can make use of this application, requiring newer versions of the devices, which reduces the universe of potential adherents. Google announces that it is necessary to have at least one Android version 6.0 device. (API version 23) and Apple indicates version /OS 13.5 or later.

especially when it corresponds to a smartphone. Consequently, the possibility of accessing the personal mobile device and consulting the contents has a very significant impact on the reservation of privacy.

Furthermore, from the combination of paragraph 1 of article 4 and article 5 of the Proposal, it seems that the inspection

process implies the apparently free access of police officers to public and private establishments where the activities considered relevant for this purpose: in addition to school and academic activities, the express reference to the work or similar context covers any establishment or place (including the domicile, in the case of domestic service providers) where workers or other professionals provide service. In this context, workers in public functions, employees and agents of the Public Administration, including the state, regional and local business sector, professionals from the Armed Forces and security forces are subject in particular.

In this regard, it is important, first of all, to remember that article 174 of the Criminal Procedure Code, even in the context of criminal investigation, makes the power to carry out searches and searches depend on a previous order of the judicial authority, and that only in presuppositions very tight and for very serious crimes, admits that criminal police bodies can take such an initiative, subject to immediate communication and consideration by the judge of the case. It is good to see that a process of inspection (preventive!) of conduct that corresponds to infractions cannot offer less guarantees to citizens than a process in which a crime is suspected.

Therefore, it is not possible to see how this power of inspection can be implemented in the different types of contexts mentioned above. Above all, when it comes to establishments where there are special duties of professional secrecy, as is the case of credit institutions, newsrooms of the media, law firms and lawyers' offices, medical offices, where, even in the context of criminal investigation , any search or search must be carried out in the presence of the investigating judge.

In fact, even in the Public Administration, there are entities that enjoy independence from the Government and its ministries, which is why the entry of police officers into the respective facilities depends on the authorization of the highest manager or representative of the entity, when there is no court order. It is, for example, what

as with universities and polytechnics.

2.2, The lack of adequacy (and the excess) of the imposition of use of the application for the intended purpose

But the restriction of privacy does not only materialize at the level of inspection. It predates that moment. In fact, the use of the application, as explained, implies the collection and subsequent processing of information regarding proximity (distance and time) in relation to other people who have downloaded the application. Furthermore, at least for Android devices, the GAEN

interface implies the permanent collection of the 'location' data, since it is no longer up to each one to be able to deactivate this functionality if and when they wish, thus allowing Google to track the displacements and movements of citizens using this application for other purposes.

Considering the universe of people who are recipients of this obligation, the impact that this treatment has in terms of exposing their private life is evident.

Now, in order to understand whether the purpose of detecting as early as possible situations of potential contagion and thus interrupting the contagion chain (to safeguard the public health interest) is sufficient to justify the restriction of the fundamental rights already listed, it is essential assess the proportionality of this legal imposition, as required by Article 18(2) of the CRP and Article 52(1) of the Charter, as well as Article 5(1)(c). ° of the GDPR.

In this judgment on proportionality, one cannot fail to start with the assessment of the suitability or aptitude of this measure to achieve the intended purpose, even before assessing its need. As mentioned above, the voluntary nature of the use of the application has so far made it possible not to question the proportionality of the restriction of fundamental rights to the reservation of private life and the protection of personal data, since the fact that the provision of personal data is available to the citizen (which can at any time deactivate the application, not introduce the code, or even uninstall it) softened the degree of demand in demonstrating the adequacy and necessity of this processing of personal data to achieve the intended purpose of breaking the chain of contagions.

From the moment it is intended to make the use of an application that entails the restriction of rights, freedoms and guarantees a mandatory use, that restriction could only be considered admissible if it was demonstrably suitable for achieving the intended purpose.

The truth is that the circumstance, already highlighted in Deliberation/2020/277, of June 29, that this application can only be installed on smartphones and on more recent versions of them, which a significant part of the population does not have, strongly harms the effectiveness of this solution and raises doubts as to the adequacy of imposing its use when it is known from the outset - which is, moreover, assumed by the legislator - that this measure is not likely to apply to a good part of the universe of people who especially if you want to protect yourself from the chain of contagions. In fact, the World Health

Organization (WHO), in guidelines dated May 28 of this year, regarding ethical considerations for the use of digital proximity screening technologies13, states that the effectiveness of this digital proximity screening as a means of detecting contagion chains is yet to be proved.

This effectiveness is further called into question by the fact that low-energy B/uetooth generates errors in the reading of distances between people, greatly increasing false positives and, therefore, promoting alarms of potential contagion that do not correspond to a real probability of risk. of contagion, according to the criteria defined by the DGS14.

Furthermore, the usefulness of the alleged obligation to use the application (and the introduction of the legitimation code) would depend on a massive capacity for inspection (and, obviously, on the legitimacy of such inspection). And it is not possible to see that this inspection on a large scale is feasible. In fact, this would presuppose that there are enough police officers to carry out such a mission and with sufficient technical knowledge to verify, first of all, whether a particular citizen is part of the universe of persons bound by such an obligation. Only at this point, this would involve analyzing not only whether the hardware supports this application, but also whether the installed software is compatible with the application. Then there are factors that make it difficult to verify that the application remains active, because the user can walk on the public road with the data.

13 Cf. https://www.who.inVpublications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

14 Cf. WIRED article, 10/14/2020, relating to a study carried out by Trinity Col/egede Dublin accessible at https://www.wired.co.uk/article/contact-tracing-app-notification-bluetooth

» 'iprjni

/MM'/

£##

switched off, and only connect to the Internet later (or the next day), without affecting the use of the application.

Furthermore, it is not possible to verify compliance with the obligation to introduce the legitimation code, imposed in paragraph 3 of article 4 of the Draft Law. This is because if the citizen has entered the legitimation code in the application, a message appears on the mobile phone screen informing that from that moment on STAYAWAY COVID will no longer monitor their contacts (obviously, because it assumes that the user will be in a situation of isolation) and also states that, «[after recovery,

when you resume your normal life, you must reinstall STAYAWAY COViD to restart the monitoring process-). In other words, it is not possible to demonstrate that the referred code has been entered on the user's mobile equipment.

Given the lack of adequacy of the imposition of the duty to use the application and to introduce the legitimation code, it can already be concluded that it violates the principle of proportionality.

In addition, since the use of the STAYAWAY COVID application was presented in Decree-Law No. , freedoms and guarantees would always be considered unnecessary, as there are other measures available to health authorities that can be applied to all citizens and that do not affect, or do not affect with the same intensity, those rights. In fact, the assumed complementary function of an instrument with such a degree of intrusion on privacy in the context of electronic devices is enough to conclude that it is unnecessary, in the sense that it is recognizing that there are mechanisms that are less harmful to the fundamental rights of citizens. that guarantee the same purpose.

Finally, even if it were intended that, in the current circumstances, the public interest of public health would justify any restrictive measure of rights, freedoms and guarantees, even a restriction whose adequacy and necessity has not been demonstrated, these imposing norms would not pass the sieve of the prohibition of the excess. The rules of articles 4 and 5 of the Draft Law, with which they imply restriction of free will

and freedom, on the one hand, and interference by police entities in citizens' electronic communications and, therefore, in their sphere of privacy, on the other hand, would mean such a violation of these fundamental rights that one would have to conclude by affecting the essential content thereof.

In addition, the impact arising from its approval represents an opening of doors to future restrictions of the same type, in different circumstances, even if always in the name of the common good.

2.3. The discriminatory effect of restrictive measures

At the end of this point, it is also important to point out the delimitation of the imposition of that obligation only on people who have equipment that allows them to fulfill that obligation.

Even if, by an absurd hypothesis, such an imposition were considered adequate and necessary, and even considering that an obligation should not be imposed on those who do not have the means to fulfill it, it cannot fail to be emphasized that inflicting a restriction on rights, freedoms and guarantees with this degree of impact to only a few citizens translates into an unequal and discriminatory restriction.

The legal recognition to citizens of a differentiated legal-fundamental sphere, depending on the ownership or possession of electronic devices of a certain type - which presupposes or is based on a certain economic power or a certain professional situation - represents a degree of arbitrariness and social discrimination unbearable in the current legal framework in which we live (cf. Article 13 of the CRP and Article 21 of the Charter).

Regarding the inequality that the imposition of the use of this application will objectively accentuate, taking into account that a part of the population does not have electronic equipment or does not have the versions of the equipment that allow them to download this application and use it, the CNPD recalls again the reservations raised by the National Council of Ethics for the Life Sciences regarding this application (even within a framework of voluntary use)15. Also the WHO, in guidelines dated May 28

15 Position of the National Ethics Council for Life Sciences, of June 29, 2020, on Mobile digital applications to control the transmission of COViD-19 - relevant ethical aspects, accessible at

this year, regarding ethical considerations for the use of digital technologies for proximity tracking16, believes that this type of resource can exacerbate inequalities, as not all citizens have access to these applications and will only be able to benefit from them very indirectly, underlining that the bet in digital proximity tracking to the detriment of traditional approaches can reduce access to essential services for already marginalized populations, in particular the elderly or those living in poverty.

In view of the above arguments, the CNPD can only conclude that the legal imposition of the use of the STAYAWAY COVID application and the introduction of the legitimizing code is unconstitutional, and the violation of European Union law, in view of the disproportionality of the restriction of fundamental rights to freedom. , the reservation or respect for private life, the inviolability of electronic communications and the protection of personal data, as well as the discrimination in the treatment of

citizens resulting from that.

3. Changing the process for issuing the legitimation code

A final note on the Draft Law, to refer to the amendment recommended in paragraph 3 of article 4, regarding the process of issuing the legitimation code. There you can read that the pseudorandom legitimation code [...] must appear in the report containing the result of the diagnostic laboratory test.

It is important, in this regard, to clarify that the solution accepted in the system involves the doctor who communicates the diagnosis, at the request of the citizen, issuing the legitimation code, for subsequent submission in the application. This solution is certainly related to the fact that, in the Portuguese legal system, clinical diagnoses are the exclusive competence of doctors.

It seems that the code is now intended to be issued in the analysis laboratory. Although it is possible to admit a simplified process of issuing the code, the truth is that the analysis laboratories do not make diagnoses. In any case, this change seems to make the issuance of a legitimation code for analytical results universal.

https://www.cnecv.pt/files/t593523643^62f80ed69c317b6cee76810d493bb77a_posic-a-o-cnecv-apps-mo-veis-controlo-covid 19-29-06-2020. pdf

16 Accessible at https://www.who.int/publications/i/item/WHQ-2019-nCoV-Ethics_ContactJracing_apps-2020.1

positive, without explaining or understanding the procedure to be adopted for this purpose, in particular which information systems will interact. However, since the impact study on data protection was not carried out regarding this change in the system, nor were adequate security measures presented for the adoption of this mechanism, the CNPD cannot assess, or pronounce, on the consequences of such a change. solution.

B. Mandatory use of mask in public spaces

With regard to the legal imposition of wearing a mask in public spaces, considering that the draft diploma has already been approved, the CNPD limits itself, in its pronunciation, to pointing out the need, in the execution and inspection of such duty, to respect the principle of minimization of personal data, as defined by point cj of paragraph 1 of article 5 of the RGPD.

Thus, the CNPD recommends that medical certificates of incapacity or medical statements be limited to declaring that there is

a reason for dispensing with the use of the mask, without specifying the cause that justifies such exemption. The inspection function by the police authorities does not require, and to that extent does not justify, knowledge of the grounds, relating to people's health, of such exemption.

III. Conclusion

The CNPD focuses this opinion on Proposed Law No. 62/XIV/2.3, specifically on the provisions regarding the duty to use the STAYAWAY COVID application. In relation to the imposition of the duty to wear a mask, the CNPD limits itself here to alerting to the need, in the context of its execution, and by virtue of the principle of minimization of personal data and the protection of privacy, in the medical certificates of incapacity or medical declarations only if it states the existence of a reason for waiving the use of the mask, without specifying it.

Regarding the mandatory use of the STAYAWAY COVID application and the insertion of the legitimation code:

1. The use of this application implies a restriction of the fundamental rights to the reservation of privacy and the protection of personal data, since

i. This application processes personal data, even though most of this data is pseudonymised;

ii. The fact that access to mobile phone operating system features, in particular B/uetooth, depends on an interface provided by Google and Apple (GAEN) to fulfill the intended purpose and that Google additionally collects on Android smartphones, Automatically and permanently, the data 'location' of the mobile phone, enhances the impact on privacy (in addition to the use that third parties can make of the constant activation of B/uetooth).

2. However, the voluntary nature of its use - as well as the insertion of the legitimation code (code that confirms the positive diagnosis of the virus) -, leaving to the free will of each citizen the decision to provide their data, softened the degree of requirement in demonstrating the adequacy and necessity of this processing of personal data to achieve the purpose of faster interruption of the chain of contagions, which is why, at an early stage of the pandemic characterized by uncertainty as to the means capable of combating it, the CNPD and the other personal data protection authorities of the Member States of the Union chose not to question the proportionality of that restriction.

3. From the perspective of the CNPD, this Draft Law, by eliminating the voluntary nature of the use of the application and the insertion in the application of the legitimation code, imposing the obligation of such measures, and by providing for the inspection of the fulfillment of these duties by the entities law enforcement agencies (without defining the conditions and limits of this inspection), disproportionately restricts the fundamental rights to freedom (free will), to privacy, to the inviolability of electronic communications and to the protection of personal data, in terms that seem to affect the essential content of those rights, in particular, the right to privacy in electronic communications that Articles 26 and 34 of the Constitution and Article 7 of the Charter of Fundamental Rights of the European Union enshrine.

4. On the one hand, the suitability of imposing the use of this application to achieve the intended purpose has not been demonstrated, for three reasons: the application cannot be downloaded on any mobile phone, but only on smartphones with certain hardware and software , leaving out part of the universe of people who are specially intended to be protected from the chain of contagions; Btuetooth Low Energy technology can generate false positives; it is not possible to verify compliance with this imposition and the imposition of insertion of the legitimation code, as explained above.

5. On the other hand, access and consultation, by police authorities, of information regarding the content downloaded on smartphones and other interactions carried out in the context of this application would always be considered excessive, as it corresponds to access to electronic communications where it appears a wide range of information regarding the privacy of the respective users.

6. Even if that were not the case, it is undeniable that the imposition of these duties only on some citizens, depending on the ownership or possession of electronic devices of a certain type - which assumes or is based on a certain economic power or a certain professional situation represents a degree of of arbitrariness and unbearable social discrimination in the current legal framework in which we live, in violation of article 13 of the CRP and article 21 of the Charter of Fundamental Rights of the Union.

7. With regard to the prediction of universal issuance of the legitimation code in the analysis laboratory, in the absence of indication of the terms in which this can operate, in particular which information systems will interact, and the impact study has not been carried out on data protection in relation to this change in the system, nor security measures presented, the CNPD

cannot assess, or pronounce, on the consequences of such a solution.

In short, the rules of articles 4 and 5 of the Draft Law, by limiting the free will and freedom of citizens, and with what they imply of interference by the entities

in electronic communications and in the personal data processed there, strongly impacting their privacy, represent a disproportionate restriction of these fundamental rights, in such terms that it can be said that their essential content is being affected, in violation of article 18, paragraphs 2 and 3 of the Constitution and article 52 of the Charter of Fundamental Rights of the European Union.

The CNPD also takes the liberty of underlining that the eventual approval of such norms would open the door to future restrictions of the same type, in different circumstances, even if under the invocation of the common good. In a democratic State of Law, such as ours, in which privacy and freedom are essential for the development of each person's personality and identity, the use of measures of this nature represents a setback of the constitutional acquis, with implications for the future of our society that cannot fail to be considered by the national legislator.

Approved at the meeting of October 27, 2020

Filipa Calvão (President)