

**RELEVANT REMARKS IN THE PRESIDENT OF THE ITALIAN DPA'S STATEMENT ON THE OPERATIONAL CONTINUITY OF THE 'COVID-19 ALERT SYSTEM' IN THE EXTENSION OF THE EPIDEMIOLOGICAL STATE OF EMERGENCY**

**SERGIO GUIDA**

Independent Researcher, Sr.Data/Information Governance Mgr.

**Key-words:** contact tracing - garante privacy - COVID-19 - eHealth algorithms

**Category:** Legal Area

In his October 19 Memo to the Committee I of the Italian Senate (Constitutional Affairs) the DPA President starts thanking for the possibility to highlight some profiles of particular interest in the "contact tracing"[1] implemented through the national alert system referred to in the Decree-Law No 28/2020 enacted with amendments by Law No 70/2020[2].

Digital contact tracing, developed in Italy through the "Immuni" app[3], has represented and still represents[4] a decisive issue in the emergency's management, expressive like few others of the balance between individual freedoms and collective interests as the most relevant in the pandemic context.

There are two fundamental rights at stake, the one as that to health, also in its meta-individual component of "collective interest" in public health and the other to the protection of personal data, qualified as a right "of freedom", independent of the traditional right to respect private life, from article 8 Charter of Fundamental Rights of the European Union (CFR)[5]: since 'tyrannical' hierarchies cannot be configured among fundamental rights (Constitutional Court, ruling 85/2013), even those to health and data protection require such a balance as to safeguard their essential content, which art. 52 CFR qualifies as inviolable.

The search for this balance constituted, in fact, one of the defining features of the positions taken by the Authority, with respect to the various provisions adopted in recent months to combat the pandemic: from those relating to the circulation of personal data, including health, among the subjects involved in the prevention action up, precisely, to the digital tracking system of contacts governed by art. 6 of the d.l. 28, which was modelled on the indications given by the DPA, since the 8

April[6] Hearing in the Committee IX of the Italian Chamber of Deputies (Transportation, Post, Telecommunications).

There we can read “we will see that selecting the most effective data category also impacts on the overall assessment of proportionality since increased selectivity reduces the intrusiveness of the given measure to what is strictly necessary and produces socially meaningful effects in terms of protecting the health of individuals and the community as a whole”. So the essential parameters of the legitimacy of the contact tracing tools were already indicated at that time, identifiable primarily in functionalization for purposes of social utility (containment of infections), rather than for repressive-sanctioning purposes, in the necessary partiality - since these solutions have to be integrated into a broader and more complex health prevention strategy - as well as in compliance with data protection rules as a condition, moreover, indispensable for the necessary social trust in such measures.

The DPA had, therefore, underlined the need for the contact tracing system to be regulated by law, due to the impact on individual privacy and the need for a unitary model of discipline capable of absorbing (also by reason of the attribution of the matter to the state legislative power) initiatives of the territorial authorities that at the time announced themselves as potentially dysfunctional. The system, under public ownership, should have been based on a truly voluntary adhesion (thus excluding any kind of prejudice against those who did not intend to lend it), on data not of geolocation but of mere proximity of the devices (much less significant and "invasive"), at least pseudonymised, on a delocalized information storing mechanism, as well as on solid guarantees of cybersecurity. The need for temporariness of the system was also emphasized, to be defined per relationem with reference to the persistence of the emergency condition and the necessary limitation of the collection to data only and to the only storage period indispensable for epidemiological purposes.

In its opinion (of April 29)[7] on the draft provision which would have been included in Decree-Law No. 28/20 for the regulation of the digital contact tracing system, the government's choice in favor of a notification system from exposure to significant contacts with positive subjects, based on the free adhesion of those who download a specific app on their device and on a national alert platform set up at the Ministry of Health, with a strong degree of data pseudonymization, as well as the prohibition of data communication to third parties, was welcomed.

In addition, the measures provided for by the law to ensure the specificity and exclusivity of the purpose have been positively evaluated: the tracking must be aimed exclusively at containing infections, excluding further purposes, without prejudice to the possibilities of use for scientific and statistical research purposes, only in the general terms provided for in the EU Regulation 2016/679, thus enhancing also in this sense the solidarity destination of the data.

Finally, the provision of the temporariness of the system was shared (as it complies with the indications already made), with the interruption of the platform's activities on the date of termination of the state of emergency and final safeguard deadline, as well as with the deletion or definitive anonymization of the collected data.

In addition, with the decision authorizing the impact assessment of 1 June[8], the Authority, having favorably acknowledged the choice in favor of an 'on-premises management system' for exposure notifications, indicated further measures aimed at strengthening the guarantees of processing also from the points of view of cybersecurity, transparency and user information.

In particular, they must be made aware of non-secondary profiles such as the risk of false positives (or even negatives), since the system cannot distinguish between dangerous contacts because they occurred, for example, in the absence of protection devices and contacts, although qualified for duration and proximity, but safe because they were held outdoors or in protective conditions. In fact, it should be remembered that, strictly speaking, Immuni represents an app functional to a notification system with respect to risk exposures, which therefore does not follow movements, but recognizes events (qualified and significant contact, from an epidemiological point of view)[9].

It was also found that, in the event of a positive swab, the start of the contact tracing system is in any case subject to a voluntary choice of the subject, who must provide the health worker with his OTP to allow the system to send alerts to potential infected. This profile has not been modified by the Prime Minister's Decree of 18 October[10], which merely intervenes in the obligations of health professionals.

This further element of the discipline (concretely implemented by ministerial decree on which, likewise, the opinion of the DPA was acquired) represents the completion and final guarantee of the effective voluntary nature of the digital contact tracing system, the adherence to which it expresses, at every stage and in all its consequences, a free choice (as much as responsible) of the individual, with the express legislative exclusion of any possible prejudice in the event of non-adhesion to the system itself.

More specifically, for the purposes of assessing compliance with the prescriptions made, with the measure of 1 June the Authority requested the Ministry of Health to provide feedback, in the next thirty days, on the following profiles:

1. precise indication of the algorithm and configuration parameters used by the system;
2. adequate information to users regarding the possibility (as mentioned above) that, due to the particular circumstances of the contact, exposure notification does not reflect an actual risk condition[11];

3. accessibility of the temporary deactivation function of the app;
4. adequate protection of analytics in the Immuni backend, avoiding any form of re-association with identifiable subjects;
5. clarification, in the information, of the operations carried out with reference to Epidemiological Info analytics and personal data collected in relation to the different categories of data subjects;
6. adequacy of the information and the alert message also with reference to the ability to discern underage users, even those over the age of fourteen;
7. adequacy of the information provided to users in relation to the characteristics of the testing phase;
8. integration of the impact assessment and information in relation to the procedures for exercising cancellation and opposition rights;
9. integration, on the accountability principle's basis, of the impact assessment with the description of the role and the operations attributable to other subjects likely to be involved in the 'Immuni System';
10. measuring the retention times of IP addresses to the extent strictly necessary for the detection of anomalies and attacks;
11. ensuring tracking of the operations carried out by system administrators on operating systems, the network and databases;
12. adoption of technical and organizational measures to mitigate the risks arising from the TEK[12] upload not referring to positive subjects as a result of any material or diagnostic errors.

Following the feedback provided (in terms) on 23 June, meetings were started between the Offices aimed at identifying the best solutions - still under examination by the Authority - to some difficulties that emerged in the fulfillment, in particular, of the requirements referred to in the fourth, ninth, tenth, eleventh and twelfth points of the previous list. In the meantime, the need to guarantee interoperability made it necessary to adopt a new impact assessment, which was received by the Authority on 16 October.

An analysis was also carried out by the Office on the risks - feared by press reports - of system vulnerability with respect to the so-called replay attacks, suitable to generate false notifications of exposure to risk. At present, this specific vulnerability (and the consequent need for further measures) does not seem to be recognizable, as this type of attacks, assuming the unlawful possession of the mobile device and the consequent change in configuration, would be attributable to criminally

unlawful conduct carried out in the context (which does not seem conceivable as a typical or inherent risk of the system) of a wider range of crimes, including against computer and communications confidentiality, public faith, etc.

On the other hand, the investigation is still underway regarding some cases, reported by press reports, related to the failure to activate the Tek loading procedure of subjects tested positive to Covid-19 provided for by the alert system. To overcome these omissions are evidently aimed the obligations listed in the Prime Minister's Decree of October 18 for healthcare professionals with respect to patients who have the Immuni app.

Finally, it should be emphasized that the 2020 Data Protection Report, adopted this month by the Council of Europe, with regard to digital solutions to combat the pandemic, recognizes the positive contribution provided by the Italian DPA in the legislative procedure and, in more general terms, in the scope of the development, by the Government, of a contact tracing system based on a synergy and a fair balance between public health and privacy.

### **The news of the decree-law**

In this context, the news referred to in Article 2 of the decree-law in conversion is inserted, which brings two essential innovations: the provision of interoperability - after a privacy impact assessment - of the national alert system with platforms operating, with the same purposes, in the European Union's territory (paragraph 1, point a), as well as the postponement of the final deadline for the use of the application and the platform - firstly commensurate with the effective end of the declaration of the national state of emergency, however no later than 31 December 2020 - until the cessation of public health protection and prevention needs, identified with the Prime Minister's Decree, and, in any case, by 31 December 2021.

As noted in the Explanatory Report of the conversion bill, the drafting of the law was preceded by the DPA opinion rendered, albeit informally, first with a note of 21 September, which provided some indications on the initially proposed text, to which the Government then, in the final draft of the provision, substantially complied. In particular, the opportunity to verify the uniformity, with respect to those granted by our alert system, of the guarantees ensured by the platforms used in other States was recalled. The need to limit, to the only necessary ones, the data exchanged, however in pseudonymised form, relating to users who tested positive for the virus, with the platforms of other States was also stressed.

Finally, the opportunity arose to integrate these additional guarantees in the specific impact assessment to be submitted for evaluation by the Authority, prior to the start of the treatment.

With reference, on the other hand, to the changes originally proposed to the regime of temporal effectiveness of the platform's activity, the need arose not to detach the final term from the emergency condition, due to the derogatory (and therefore exceptional, precisely non-ordinary) character of the discipline on contact tracing.

The Government then proposed the version (which would later be final) of the provision, considered by the DPA to be acceptable for the reasons set out below.

Interoperability is the consistent consequence of the design of the national alert system as part of a European pandemic response strategy. This systems feature has, in fact, been foreshadowed since last April by recommendation (C(2020)2296) on a package of common European Union tools for the use of technology and data, in which the Commission, in order to achieve a common European approach to the pandemic, called for 'interoperability throughout the European Union' of tracking systems[13].

On 13 May, EU member states, with the support of the European Commission, agreed, within the eHealth Network, guidelines for the cross-border interoperability of tracking applications in the Union[14].

Interoperability between tracing platforms in the territory of the European Union was then the subject of the 15 July Commission Implementing Decision (EU) 2020/1023[15]. This decision constitutes the legal basis that legitimizes, in the European context, the interoperability of national mobile contact tracking and alert applications (the so-called federative gateway), with reference to the Member States which have joined this specific form of collaboration.

Interoperability of the alert systems therefore represents, in this sense, a functional measure both to the strengthening of the contagion containment activities - as it allows to reconstruct the chain of contacts even in the case of intra-European mobility of the subject - as well as to the freedom of movement of citizens in the territory of the Union. This right (and, at the same time, the founding principle of the European legal system) risks being extremely prejudiced by the pandemic context and, in this way, can be safeguarded to some extent.

The impact that the interoperability of tracing systems inevitably determines on the protection of personal data is, moreover, adequately balanced not only by the tendential analogy of the guarantees adopted by member countries on this point - in particular following the aforementioned execution decision - but also from the prescriptions that the Authority, when examining the impact assessment, will be able to make to strengthen the safeguards at least from an internal point of view.

With regard, on the other hand, to the amendments referred to in point (b) of paragraph 1, the provision of the dies ad quem of operation of the platform until the cessation of the needs of protection

and prevention of public health, conforms to the need, represented by the DPA, to anchor the term of effectiveness, albeit per relationem, to the persisting pandemic condition.

In this sense, the modification made by the decree-law conforms to this model, as it assumes, among the parameters to which the operation of the system is to be anchored, the substantial one relating to the persistence of health prevention needs and that of a formal-regulatory nature, of the identification of the existence of the same needs with a Prime Minister's Decree. The guarantee of last resort is then entrusted to the provision, with a safeguard clause, of the final term of operation of the system as at 31 December 2021.

The deferral of the term of effectiveness of the system is therefore based on a double set of criteria. In the first place, there are public health needs related to the need to reconstruct, even digitally, the chain of contacts, with respect to which the Government assumes the responsibility of declaring its existence with a Prime Minister's Decree. Secondly, the guarantee with respect to the risk of "emergency normalization" is entrusted to the indication of the deadline of 31 December 2021 by which, in fact, regardless of substantive reasons, the activity of the tracking system must cease.

Thus described, in a nutshell, the reasons underlying the favorable opinion given by the DPA on the rules' scheme proposed and then, as anticipated, precisely reflected in the text of the decree-law, the position expressed at the time can only be confirmed. In fact, also due to the implementation of the indications provided by the Authority, both changes made to the contact tracing discipline underlie a reasonable balance between public health needs and protection of personal data, in accordance with that convergence between personalist demands and solidarity vocation on which our legal system is based.

**Source:** Memoria del Presidente del Garante per la protezione dei dati personali sul ddl di conversione in legge del decreto-legge 7 ottobre 2020, n. 125, recante misure urgenti connesse con la proroga della dichiarazione dello stato di emergenza epidemiologica da COVID-19 e per la continuità operativa del sistema di allerta COVID, nonché per l'attuazione della direttiva (UE) 2020/739 del 3 giugno 2020 - Commissione 1a (Affari Costituzionali) del Senato della Repubblica (19 ottobre 2020).

**Link:** <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9468919>.

[1] See the White Paper by Sergio Guida, *A Framework for Contact Tracing in Italy among scientific needs, technological possibilities and respect for Individual Rights and Freedoms in terms of Data Protection* in the European Journal of Privacy Law & Technologies, 16/09/2020 at [http://www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view\\_html?id\\_evidenza=62](http://www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view_html?id_evidenza=62).

[2] The text of the decree-law of 30 April 2020, n. 28 (in the Italian Official Gazette - General Series - n. 111 of 30 April 2020), coordinated with Law no. 70 of 25 June 2020 (in this same Italian Official Gazette on page 1), which states: '*Urgent measures for the enforcement of interception systems for conversations and communications, further urgent measures in prison law , as well as supplementary and coordination provisions in the field of civil, administrative and accounting justice and urgent measures for the introduction of the Covid-19 alert system*' (20A03469) (IOG General Series No. 162 of 29-06-2020) could be found at <https://www.gazzettaufficiale.it/eli/id/2020/06/29/20A03469/sg>.

[3] See the official website at <https://www.immuni.italia.it/>.

[4] See Simona Latte, *Immuni: framing and first considerations one month from the start* in the European Journal of Privacy Law & Technologies, 14/10/2020 at [http://www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view\\_html?id\\_evidenza=64](http://www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view_html?id_evidenza=64).

[5] The updated text Charter of Fundamental Rights of the European Union (2012/C 326/02) is available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN>.

[6] Cf. The Italian Data Protection Authority, *Hearing through video conference of the President of the Italian Data Protection Authority regarding use of new technologies and the Internet to counter the Covid-19 epidemiological emergency - Committee IX of the Italian Chamber of Deputies (Transportation, Post, Telecommunications)*, 8 April 2020” at [https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9308774#english\\_version](https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9308774#english_version).

[7] Cf. The Italian Data Protection Authority, *Opinion on the proposed legislation for the provision of an application for the tracking of COVID-19 infections, Register of measures No 79 of 29 April 2020* at <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9328050>.

[8] Cf. The Italian Data Protection Authority, *Authorization measure for the processing of personal data carried out through the Covid-19 Alert System - Immuni Apps - Register of measures No 95 of 1 June 2020* at <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9356568>.

[9] See the White Paper by Sergio Guida, *A Framework for Contact Tracing in Italy among scientific needs, technological possibilities and respect for Individual Rights and Freedoms in terms of Data Protection* in the European Journal of Privacy Law & Technologies, 16/09/2020 at [http://www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view\\_html?id\\_evidenza=62](http://www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view_html?id_evidenza=62), cit., 16-17.

[10] Details could be found at <http://www.governo.it/it/articolo/coronavirus-il-presidente-conferma-il-dpcm-del-18-ottobre-2020/15457>.

[11] See Simona Latte, *Immuni: framing and first considerations one month from the start* in the European Journal of Privacy Law & Technologies, 14/10/2020 at [http://www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view\\_html?id\\_evidenza=64](http://www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view_html?id_evidenza=64), cit, 3.

[12] Temporary Exposure Keys, or TEKs, “are anonymous keys shared between mobile devices to determine if two devices were sufficiently nearby to be considered “exposed” to one another. When an application user confirms they have been exposed, their keys are shared to the server in order for applications to download and determine if other users interacted with any of the now exposed keys”, see *Temporary Exposure Key (TEK) Publishing Guide | Exposure Notification Reference Key Server* at <https://google.github.io/exposure-notifications-server/getting-started/publishing-temporary-exposure-keys.html>. More details in the White Paper by Sergio Guida, *A Framework for Contact Tracing in Italy among scientific needs, technological possibilities and respect for Individual Rights and Freedoms in terms of Data Protection* in the European Journal of Privacy Law & Technologies, 16/09/2020 at [http://www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view\\_html?id\\_evidenza=62](http://www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view_html?id_evidenza=62), cit., 19.

[13] More details in the White Paper by Sergio Guida, *A Framework for Contact Tracing in Italy among scientific needs, technological possibilities and respect for Individual Rights and Freedoms in terms of Data Protection* in the European Journal of Privacy Law & Technologies, 16/09/2020 at [http://www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view\\_html?id\\_evidenza=62](http://www.ejplt.tatodpr.eu/Tool/Evidenza/Single/view_html?id_evidenza=62), cit., 14-15.

[14] Cf. eHealth Network, *Interoperability guidelines for approved contact tracing mobile applications in the EU, Brussels, Belgium, 13 May 2020* at [https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing\\_mobileapps\\_guidelines\\_en.pdf](https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf)

[15] The full text, *Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic (Text with EEA relevance) C/2020/4934* is available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D1023&from=EN>.