International Journal of Business and Economic Development
Vol. 1, No. 6; September, 2020. pp 55-65
ISSN 2692-5591 (print), 2692-5583 (online)

Published by International Center for Promoting Knowledge
www.icpknet.org

Covid-19, *contact tracing* and *GDPR*

Giuliana Amore
Professor
Department of Economics and Business
Institutions of Private Law
and
Researcher
Boston University School of Law (Boston)
United States

Abstract

Provisions recently issued relating to the Covid-19 pandemic spread emergency showed a considerable impact (also) about personal data processing and, consequently, on the right to their protection. Among the measures adopted (in several countries, including Italy) to cope the pandemic emergency, there are those based on collection and tracking of personal health data in order to control and contain the virus and in particular the so-called "Immuni" app, involving, prima facie, an invasive control in people's lives: hence, once the terms and characteristics of this tracking system have been reconstructed, the need to identify its legal basis in light of the General Data Protection Regulation (GDPR) and, in the event of a positive outcome of this assessment, the guarantees capable to ensure the necessary balance between the protection of public health and the protection of the private sphere from excessive compression or intrusiveness.

1. Introduction

As known, (also) the principles about data protection included in the so-called *data protection law*, i.e. in the EU Reg. no. 679/2016, are severely tested by Covid-19 and are called to play a fundamental role: in order to realize this, it is sufficient to look at the imposing stratification, which has occurred on recent months and constantly updated, of provisions issued relating to the Covid-19 pandemic spread emergency, starting from the beginning of the year and having, about what is relevant for our purposes, an impact on the processing of personal data and, consequently, on the right to their protection[1].

[1] Of particular importance, the l.d. 9 March 2020, n. 14, art. 14, as "until the end of the state of emergency resolved by the Council of Ministers on January 31, 2020, due to reasons of public interest in the public health sector and, in particular, to ensure protection from the cross-border health emergency determined by the spread of COVID-19 through adequate prophylaxis measures, as well as to ensure the diagnosis and health care of the infected or the emergency management of the National Health Service, in compliance with Article 9, paragraph 2, letters g), h), i), and Article 10 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 [...] may process personal data, including communication between them, also relating to articles 9 and 10 of Regulation (EU) 2016/679, which are necessary for the performance of the functions attributed to it in the context of the emergency caused by the spread of COVID-19 [...] Treatments of personal data referred to paragraphs 1 and 2 are carried out in compliance with the principles referred to in Article 5 of the aforementioned Regulation (EU) 2016/679, adopting appropriate measures to protect the rights and freedoms of the data subjects "; the d.l. 30 April 2020 n. 28, art. 6, according to which "for the sole purpose of alerting people who have come into close contact with subjects who tested positive and protect their health through the planned prevention measures in the context of public health measures related to the COVID-19 emergency, it is set up a single national platform for the management of

Among the measures proposed and already adopted to cope the pandemic emergency, there are those based on collection and tracking of personal health data in order to control and contain: in particular, we are speaking about the so-called *app* "Immuni".

This kind of measure, *prima facie*, looks like to involve an invasive control on people's lives: monitoring the progress of the virus could actually translate into subsequent monitoring of the person himself; in this regard, Chinese experience is emblematic, due to the development of infected or potentially infected people tracking app, together by the Government and the health authorities. In other words, this kind of system, although aimed to contain the risk, could be suitable to collect a large amount of information about each citizen, starting from health data[2], which, as well known, represent particularly "sensitive" data in the light of EU Reg. no. 679/2016 (so-called GDPR).

Therefore, we are wondering whether such a health emergency situation can actually justify measures aimed to delete (or almost) the protection of privacy, through the creation of apps or similar tools that invade so much the personal sphere of the individual: this check cannot be abstractly done, but on a case-by-case basis, i.e. concerning the specific tracking or monitoring system actually adopted. And, if digital technologies can undoubtedly be key elements in the fight against Covid-19 on the one hand, on the other hand, however, it is necessary to protect

---

the alert system for subjects who, for this purpose, have installed, on a voluntary basis, a specific application on mobile telephone devices [...]. The Ministry of Health, following an impact assessment, constantly updated, carried out pursuant to Article 35 of Regulation (EU) 2016/679, adopts appropriate technical and organizational measures to guarantee an adequate level of safety for high risks. the rights and freedoms of the interested parties, having heard the Guarantor for the protection of personal data pursuant to article 36, paragraph 5, of the same Regulation (EU) 2016/679 and article 2-quinquiesdecies of the Code regarding the protection of personal data referred to in legislative decree 30 June 2003, n. 196, ensuring, in particular, that: a) users receive, before activating the application, pursuant to articles 13 and 14 of Regulation (EU) 2016/679, clear and transparent information in order to achieve full awareness , in particular, on the purposes and on the processing operations, on the pseudonymisation techniques used and on the data retention times; the processing carried out to alert the contacts is based on the processing of proximity data of the devices, rendered anonymous or, where this is not possible, pseudonymised; in any case, the geolocation of individual users is excluded; […] D) the confidentiality, integrity, availability and resilience of the processing systems and services as well as adequate measures to avoid the risk of re-identification of the data subjects to whom the pseudonymised data being processed refer are guaranteed on a permanent basis; […] The data relating to close contacts are kept, even in the users' mobile devices, for the period strictly necessary for the processing, the duration of which is established by the Ministry of Health and specified in the context of the measures referred to in this paragraph; the data are automatically deleted upon expiry of the term. [...] The use of the application and the platform, as well as any processing of personal data carried out pursuant to this article, are interrupted on the date of cessation of the state of emergency arranged by resolution of the Council of Ministers of January 31, 2020, and in any case not after 31 December 2020, and by the same date, all personal data processed must be deleted or made definitively anonymous. The d.l. 10 May 2020 n. 30, in art. 1 provides that in consideration of the urgent need for reliable and complete epidemiological and statistical studies on the immune status of the population, which are essential to guarantee protection from the current health emergency, pursuant to Article 9, paragraph 2, letter g) ej), and of Article 89 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, as well as of Article 2-sexies, paragraph 2, letter cc) of Legislative Decree 30 June 2003, n. 196, the processing of personal data, including genetic and health-related data, is authorized for statistical purposes and scientific studies carried out in the public interest in the public health sector, as part of a "serum prevalence" survey conducted jointly by the competent offices of the Ministry of Health and by the National Statistical Institute (ISTAT), as data controllers and each for the profiles of their own competence, according to the methods identified in this article and in the protocol approved by the Technical Scientific Committee referred to Article 2 of the order of the Head of the Department of Civil Protection 3 February 2020, n. 630, as well as in compliance with the relevant deontological rules attached to the same legislative decree no. 196/2003 [...] The processing of samples and related data is carried out for the exclusive purposes of scientific research on SARS-COV-2 identified by the protocol referred to in paragraph 1, in compliance with the requirements of the Guarantor for the protection of personal data identified in the provision of 5 June 2019 and subsequent amendments. The data controller of the data collected in the biological bank is the Ministry of Health and access to the data by other subjects, for the aforementioned research purposes, is allowed only in the context of joint research projects with the same Ministry.

[2] These data concern physical and mental health. Recital 35 lists, by way of example, some health data, such as' information resulting from examinations and checks carried out on a part of the body or an organic substance, including genetic data and biological samples; any information concerning, for example, a disease, disability, risk of disease, medical history, clinical treatments or the physiological or biomedical status of the data subject, regardless of the source, such as a doctor or health care professional, a hospital, medical device or in vitro diagnostic test '. On this point, cf. L. BOLOGNINI - E. PELINO - C. BISTOLFI, The European Privacy Regulation, Milan 2016, p. 71.

oneself from the risk of effects that could prove irreversible, in the sense that it is essential to ensure that every measure adopted in these exceptional circumstances is necessary, limited in time, with minimal scope and subject to periodic and effective review: i.e., it is necessary to reconcile the management needs of the current health emergency with that relating to safeguarding the confidentiality of the interested parties[3].

It is also well known how, in the face of the emergency, a joint effort is underway to fight the spread of an infectious disease, still almost unknown, which endangers the health of citizens all over the world: at the same time, both European Data Protection Board (EDPB) and the Guarantor for the protection of personal data warn, however, that the measures that will be taken must in any case be immediately revocable at the end of the emergency period, in order to avoid an abnormal compression of the fundamental rights of the interested parties.

Although the purpose is represented by the emergency management and the contagion containment in order to protect the health of the entire population, there are several doubts regarding the modalities and the need for the treatment of health data and / or other data of the interested parties with systematic and large-scale methods. Therefore, our country, similarly to other European ones, has addressed and positively resolved the issue of taking measures to protect the right to health, which could involve the processing of "particular" or sensitive personal data on a large scale of the interested subjects, but also the profiling[4] deriving from the combination of these data: hence, the need to verify whether or not those kinds of measures are legitimate, excessively pervasive and

[3] With particular reference to the working context, the Guarantor has specified, in particular, that, in the context of the prevention and safety system in the workplace or anti-contagion safety protocols, the employer may require its employees to carry out serological tests only if ordered by the competent doctor or other health professional according to the rules relating to the epidemiological emergency. Only the occupational doctor, in fact, in the context of health surveillance, can establish the need for particular clinical and biological tests. And the competent doctor can always suggest the adoption of diagnostic tools, when he deems them useful in order to contain the spread of the virus, in compliance with the indications provided by the health authorities, also with regard to their reliability and appropriateness. With regard, then, to the protection of the workplace with respect to visitors and the administration of real questionnaires on the behavior and health data of these subjects, the Privacy Guarantor specified that the task relating to the assessment and collection of related information to potential contagion situations - presence of flu symptoms, movements to places considered at risk, contact with people of the so-called "Outbreaks", etc. - it is exclusively up to the competent bodies, which can be found in health professionals as well as in the Civil Protection. It is therefore expressly forbidden for private parties, including employers, to carry out independent investigations as well as specific requests for information. According to the Guarantor, this practice would be excessive and unjustified. The Authority also specifies that information relating to the diagnosis or family medical history of the worker cannot be processed by the employer (for example, by consulting the reports or the results of the examinations). Conversely, the employer can communicate the presence of a case of Covid19 infection to employees and collaborators without communicating information that is not necessary for this purpose and adopting effective protection measures; in case of disclosure of the name, it will be necessary to inform the interested party in advance in respect of his dignity and integrity. Finally, the Guarantor clarified that participation in serological screenings promoted by the regional prevention departments against particular categories of workers at risk of contagion, such as health workers and law enforcement, can only take place on a voluntary basis. The results can be used by the health facility that performed the test for the purpose of diagnosis and treatment of the person concerned and to arrange the epidemiological containment measures provided for by the emergency legislation in force (eg home isolation).

[4] As known, art. 4 of the GDPR defines profiling as "any form of automated processing of personal data consisting in the use of such personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning professional performance, the economic situation , the health, personal preferences, interests, reliability, behavior, location or travel of that natural person '. Therefore, to establish whether profiling is present, it is advisable to check whether natural persons are tracked on the internet, including any subsequent use of personal data processing techniques which consist in profiling the natural person, in particular to take decisions that they concern you or analyze or predict your preferences, behavior and personal positions. Therefore, the profiling activity consists of: automated processing; performance on personal data; purpose of evaluating the personal aspects of a natural person. There is a specific regulation of profiling precisely in the health sector: art. 22, par. 4, of the GDPR, as a general principle, prohibits the profiling of health data. Therefore, even in cases where the general prohibition of profiling is waived, this exemption does not apply to the acquisition of health data. In fact, these, being classified as particular personal data pursuant to art. 9 GDPR, require particular protection. The prohibition of profiling may however be waived in specific cases: in particular, the profiling activity of health data may exceptionally take place in the event that there is an explicit consent of the interested party; or a relevant public interest must be pursued in the field of public health; the owner (or manager) has adopted suitable and adequate security measures to protect the patient's rights, freedoms and legitimate interests.

ineffective, especially if not accompanied by the provision of an adequate number of protective devices for healthcare and for citizens, as well as by carrying out swabs for the detection of Covid-19.

2. The so-called app "Immuni" as emergency measure.

Italian Government has notoriously opted for the so-called "Immuni" *app*[5] for *contact tracing* management on both 2 and 3 phases of the coronavirus emergency[6]. It was substantially developed by the Italian company Bending Spoons and finds its own official *ratio* in two considerations mainly: the ability to promptly contribute to counteract the virus and the compliance with the European model outlined by the PEPP-PT Consortium[7]. The problem is to investigate the lawfulness of this instrument and, in the event of a positive outcome of this assessment, to identify the guarantees for respect of privacy.

A brief examination of the characteristics of the "Immuni" *app* is preparatory for the solution of both issues. This is a proximity tracking app, as it allows data exchanges among devices that are close to each other with Bluetooth enabled. A temporary and changing ID is assigned each device: if an individual whose smartphone has the "Immuni" *app* discovers his coronavirus positivity, a code to download into a server the list of smartphones IDs with the same *app* installed and activated, with which he came into contact in the previous days, is sent him.

A notification of contagion risk will be sent all those contacts, via the *app* again. This is composed by two parts, the first one dedicated to actual *contact tracing* (via *Bluetooth*) and the other one aimed to host a sort of "clinical diary", in which the user can progressively note the data relating to his health, such as the presence of symptoms compatible with the virus. Mobile phones store in memory the data of the other ones which came into contact with, in the form of anonymous encrypted codes. Metadata, such as the duration of the encounter between the devices or the strength of the perceived signal, are associated with these codes, and involved in the assessment - made directly on the individual device - of the risk of contagion. When one of the subjects who downloaded the *app* tests positive for the virus, health professionals should provide him with an authorization code with which he can download his anonymous code on a ministerial server, according to a decentralized model. Mobile phones with the *app* take the codes of the infected people[8] from the server and, if the *app* recognizes a code of an infected person among the codes in its memory, it displays the notification to the user. The data transmission would be encrypted and digitally signed to ensure maximum security and confidentiality in this phase of data "exit" from the smartphone of the individual user.

The entire architecture of the system chosen by the Italian government to collect useful data for reconstructing coronavirus infections is based on application that records the data, shares them with the central server and interrogates the archives to verify contacts at risk. The app associates each phone on which it is installed with an anonymous random code. Once the platform has been downloaded and the notification system is activated, the smartphone will begin to exchange its (anonymous and random) code via Bluetooth with other smartphones that are nearby and that have downloaded the *contact tracing app*.

If a citizen tests positive for the coronavirus, he or she can enter in the *app* a check code delivered with the test. At that point, the *app* will communicate the area of origin, the province of residence and the epidemiological information of the coronavirus positive subject to a central server[9]. After these steps only, those who have been in contact with the infected person for more than a few minutes in the last few days will be warned with an alert, but it does not seem possible to trace either the person, the place or time of the meeting.

---

[5] Starting from June 15, active throughout Italy.

[6] Only two technological solutions were identified, considered theoretically valid to be developed and tested for implementation purposes in the current emergency situation: "Immuni" and "CovidApp". Following its comparative analysis, the task force concluded that "Immuni" would use the technology developed by the PEPP-PT European Project Consortium, thus promising greater guarantees of interoperability and anonymization of personal data. This solution was also considered to be at a more advanced stage of development than the CovidApp solution. On the "Immune" app, see in particular the interview on www.qds.it with Salvatore Sanfilippo, well-known computer programmer, creator of "Redis".

[7] In fact, this model was only partially adopted by the app; then the app changed its model by adopting that of Apple-Google, more decentralized.

[8] In the centralized model, mobile phones would receive any notification of "risk subject" directly from the server.

[9] This server would be an Italian public infrastructure, managed by Sogei, with a software platform managed by the Ministry of Health.

The *app*, once it receives the notice that a subject has tested positive, sends a notification all the IDs who have been "in contact" with him in the previous two weeks; the subject who receives the notification is simply put in a position to know the contagion risk and it will be up to him to voluntarily adopt more precautionary measures (perhaps "recommended" by the *app* during the notification phase). Once the notification is open, only the contact can be known, while it will then be up to the health authorities on a regional basis to give advice on how to behave. The *app* is able to be deactivated at any time and the data of the individual meetings are stored on personal devices, and not on a central server[10].

The admissibility of taxation forms (albeit de facto) of the *app* was firmly excluded, contrary to the orientation and the proposal that the government's technical-scientific commission on the coronavirus was about to formalize in order to make the *app* almost mandatory: in this regard, it was hypothesized to make it a *condicio sine qua non* for the enjoyment of advantages (such as mobility in phase 2), matching it with self-certification. The solution adopted is respectful of the recommendations of the European Data Protection Board (EDPB) and of the Guarantor for the personal data protection, which monitor compliance with the legal profiles of the *contact tracing* application and which have strongly advised against both the mandatory installation and the implementation of incentives forms that scale or limit, even exclude, the access of citizens to services otherwise usable, according to the principles of equal treatment or that bind the exercise of freedom rights to the adoption of the *app*: those obligations, declared or disguised as incentives, would certainly represent a form of invasion in the private sphere involving doubts of constitutionality but which, if not foreseen, as demonstrated by evidence and daily data, would inevitably imply a weakening of the effectiveness of the *app* to the detriment of the protection of an interest of equally constitutional (and perhaps higher) rank, the public health.

Concerning the aspects strictly inherent to the investigation, it should be noted that the limits and obligations imposed on the right to privacy interfere with other fundamental rights and, in particular, with the right to health: these rights do not have absolute priority over each other, and not even the right to data protection can act as a "tyrant"[11]; this one, specifically governed by art. 8 of the European Charter of Fundamental Rights of the European Union, falls within the scope of art. 52, par. 1 and 3 of the Charter itself[12] and, as such, must be balanced on a case by case basis with respect to other rights recognized as fundamental. From this rule it seems possible to deduce the attribution of a specific pre-eminence, by applying certain assumptions, including certainly emergency situations in the health sector, to the objectives of general interest, such as the protection of public health. The conflict between interest in protection of collective health, contained in art. 35 of the Charter of Fundamental Rights of the European Union, and interest in the protection of personal data pursuant to art. 8 EU Charter should perhaps more correctly be solved in favor of the first one, in the name of which an invasion of the private sphere should be justified, not only for its individual, but general and social relevance or precisely "of the community" (art . 32 of the Constitution). It is a question of making a comparison and weighing the benefits and objectives pursued (public health) that would derive from the imposition of sacrifices on other rights and interests involved (protection of personal data), in light of the principle of "proportionality in the strict sense". This is the most delicate issue, which requires the legislator (first) and the interpreter (after) "to open the gaze of their evaluations, to the point of projecting themselves on the effective impact"[13]of the emergency measures introduced, balancing

[10] In summary, the app creates a register of contacts with which you "communicate", storing three pieces of information for each user: what is the device with which you came into contact, at what distance and for how long. If a person with whom one has come into contact will test positive for Covid-19 following a test, the medical operator authorized by the positive citizen, through the anonymous identification of the same, will send an input / alert message to inform the anonymously identified users who have come into contact with him. For privacy, the alert / message received does not contain the identification of the person who tested positive for Covid-19, but informs that someone with whom you have been in contact has tested positive for the new coronavirus, with information on how to behave accordingly.

[11] No fundamental right is protected in absolute terms by the Constitution, but - on the contrary - it is subject to limits to integrate with a plurality of other rights and values, since otherwise it would become a "tyrant" and would lead to the total annihilation of one or more factors at play: in this sense, Corte cost. n. 85 of 2013 cited above.

[12] Any limitations on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essential content of those rights and freedoms. In compliance with the principle of proportionality, limitations may be made only where they are necessary and effectively respond to purposes of general interest recognized by the Union or the need to protect the rights and freedoms of others.

[13] Thus, M. CARTABIA, *I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana*, in *Atti del seminario svoltosi in Roma*, Palazzo della Consulta, 13-14 October 1992, Milan, 1994, 5 and *Atti della Conferenza*

rights and interests at stake and seeking the solution that more than any other pursues in a balanced way the maximum expansion of all the rights and values involved[14].

3. The problem of "Immuni" app lawfulness: legal basis

On recent months, the *European Data Protection Board* (*EDPB*) adopted a formal Declaration and several guidelines about the use of location data and tracking tools, regarding the personal data processing during the pandemic, underlining the importance of guaranteeing always the personal data and the interested people protection, above all in order to avoid any return contagions once the containment measures adopted have been loosened, as well as to allow the control and isolation of new outbreaks. First of all, this document recommends compliance with the principle of lawfulness of processing resulting from the adoption of emergency measures, including the "Immuni" *app*.

On the hermeneutic level, the fundamental problem is to verify whether the health emergency can represent the legal basis to justify the restriction of freedom in favor of health data processing. Now, in Recital no. 46 of the GDPR, the processing carried out to control "the evolution of epidemics and their spread or in cases of humanitarian emergencies" is defined as lawful, and art. 9.2, lett. *i)*, of the same GDPR, which provides precisely for the treatment in situations of health emergency, such as that caused by Coronavirus, and in the same way as the processing of particular data - in this case, health data - is allowed in case of serious threats to health and social or collective security, based on a balance between different constitutionally guaranteed rights: the collective health,

on the one hand, and the privacy protection, on the other one.
In particular, art. 9, while generally forbidding (par. 1) the particular data processing[15], such as those "relating to health", allows the processing itself (among other things) when it is "necessary due to reasons of public interest in

trilaterale delle Corti costituzionali italiana, portoghese e spagnola, Rome, 2013, 12.

[14] As known, in Italian constitutional jurisprudence, the judgment of balancing rights has been known and practiced for a long time, as an indispensable tool for the implementation of a pluralist Constitution, which welcomes a "dignitary" concept of rights, distinct from the so-called "Libertarian": fundamental rights are never affirmed in absolute terms, but are part of a complex constitutional fabric in which other rights and other constitutionally protected interests and assets can legitimately limit their scope. In the Italian Constitution, every right is always preached together with its limit and, in this context, balancing is an interpretative and argumentative technique that allows the necessary reasonable reconciliation or proportionality of a plurality of competing constitutional interests: emblematic, in this regard, the recent judgment on the ILVA case, no. 85 of 2013, in which the Court made explicit the not absolutely prevalent character of fundamental rights, the object, rather, of a balance. The interruption of the activities of the ILVA steel mills in Taranto, ordered by the judge to protect the health of workers and citizens, was countered by the need to preserve an economic activity of great impact in Italian and European society, especially due to the enormous number of jobs put at risk by the irreversible effects of the shutdown of the blast furnace ordered by the judge. The Court was therefore faced with two conflicting sets of rights: the right to health and the environment, on the one hand, and the right to work and the exercise of economic activities on the other. In this context, the Court, with a particularly effective formulation, affirmed that "all the fundamental rights protected by the Constitution are in a relationship of reciprocal integration and it is therefore not possible to identify one of them that has absolute prevalence over the others. Protection must always be "systemic and not split into a series of uncoordinated and potentially conflicting rules" (judgment no. 264 of 2012). If this were not the case, there would be an unlimited expansion of one of the rights, which would become a "tyrant" against the other constitutionally recognized and protected legal situations, which together constitute an expression of the dignity of the person. […]». On the subject, without any claim to completeness, considering the complexity of the topic and the vastness of literature about it, see *ex multis*, R. BIN, *Diritti e argomenti: il bilanciamento degli interessi nella giurisprudenza costituzionale*, Milan 1992; G. PINO, *Diritti umani tra norme, fatti e retorica. Diritti fondamentali e principio di proporzionalità*, in *Ragion pratica*, p. 541 and following; D. U. GALETTA, *Il principio di proporzionalità nella Convenzione europea dei diritti dell'uomo, fra principio di necessarietà e dottrina del margine di apprezzamento statale: riflessioni generali su contenuti e rilevanza effettiva del principio*, in *R. it. d. pubbl. comun.* 1999, p. 743 and following; C. SARTORETTI, *Il diritto alla privacy tra sicurezza e principio di proporzionalità: il punto di vista della Corte europea dei diritti dell'uomo*, in *D. publ. comp. eur.* 2009, p. 583; A. SITZIA, *I «controlli tecnologici» del datore di lavoro tra necessità e proporzionalità. Chiare indicazioni lavoristiche dalla prima Sezione civile*, in *Nuova g. civ. comm.* 2014, 2, p. 103 ff. In foreign literature, in particular, CFR. A. BARAK, *Proportionality*, Cambridge 2012, p. 175 and following; A. STONE SWEET - J. MATHEWS, *Proportionality Balancing and Global Constitutionalism*, in *47 Columbia Journal of Transnational Law* 2008, p. 73.

[15] The *ratio* of the prohibition is represented by the object of the processing, consisting of those data that Directive 95/46 / EC defined as "sensitive". In this regard, the Cass. civ., section a., n. 30984 of 2017, in G. it. 2018, 12, p. 2639, which clarified the concept of "sensitive data" as that data, in particular, capable of detecting the state of health. A broad and comprehensive

the public health", such as protection from "serious cross-border threats to health or ensuring high standards of quality and safety of healthcare, medicinal products and medical devices based on Union or Member State law which provides for appropriate and specific measures to protect the rights and freedoms of the interested subject" [art. 9, par. 2, lett. *i*)].

But, if the health data processing therefore appears legitimate in the light of art. 9.2, lett. *i)*, *GDPR*, the risk of intersection of information (primarily relating to health, but not limited to it), capable of producing effects in the legal sphere of the data subject or significantly affecting his person[16], is worrying. In particular, we are referring to the so-called profiling, notoriously defined in art. 4, par. 4 of the *GDPR* as form of automated processing of

reading of any information deemed particularly relevant is offered, such as health or sexual orientation. Sensitive data, or particular categories of data, represent a numerus clausus: in this sense, R. TUCCILLO, Art. 9 GDPR, in A. BARBA - S. PAGLIANTINI (edited by), *Delle persone*, vol. II, in E. GABRIELLI (directed by), *Commentario codice civile*, Vicenza 2019, p. 156 s. As is known, this general prohibition is followed by the list of a series of exceptions and exceptions, which allow the processing of the data. The first hypothesis of lawfulness of the processing of particular data is the consent of the interested party; further exceptions occur in cases where the consent of the interested party is replaced, as the legal basis of the processing, by different needs deemed to prevail with respect to the position of the interested party. Specifically, in addition to the hypotheses connected with health, healthcare and scientific research, these are those in which the processing is necessary for purposes related to labor law, safety and social protection; reasons of public interest; the exercise or defense of a right in court. Personal data relating to the physical or mental health of a natural person, including the provision of health care services, are those that reveal information relating to his state of health (Article 4, point 15, GDPR). This includes information on the natural person collected during his registration in order to receive health care services or the related provision referred to in Directive 2011/24 / EU of the European Parliament and of the Council; a specific number, symbol or element attributed to a natural person to uniquely identify him for health purposes; information resulting from tests and checks carried out on a part of the body or an organic substance, including genetic data and biological samples; and any information regarding, for example, a disease, disability, risk of disease, medical history, clinical treatments or physiological or biomedical status of the data subject, regardless of the source, such as, for example, a doctor or other healthcare professional, hospital, medical device or in vitro diagnostic test (recital 35 *GDPR*).

[16] And indeed, personal data is a dynamic concept, which must always refer to the context, in the sense that even isolated information can be used by crossing with other data. For example, advertising companies use various tracking techniques to be able to individually identify an individual among the many online browsers: these techniques do not allow the physical identification of the person, but more than anything else they identify the browser or digital device through which the person surfs the net. These data (cookies, fingerprint, add) are also considered personal data. The European Court of Justice has expressly defined the IP (Internet Protocol) address as personal data, in the Brever v. Germany 2016 and the European regulation on the protection of personal data (GDPR) expressly includes online identifiers in personal data, such as IP numbers, cookies and geolocation data. Location data, or position data (also mobility data) is information processed by an electronic communications network or electronic communications service that indicates the geographical location of the terminal equipment (e.g. smartphone) of a user of the electronic communication service. In particular are the data relating to: latitude; longitude; altitude; running direction; time of location registration. In most cases, these data derive from the devices that a user wears (smart band, fitness tracker, etc.) or carries with them (smartphone, tablet). If collected in sequence, they allow you to track the movements of people in space. They can include GPS-based data from smartphones, tablets and satellite navigators, but also from wi-fi equipment, for example installed on premises offering the public the connectivity service. Position data can be collected in various ways: first of all, via GPS (Global Positioning System, ie the satellite network). The devices are able to detect their position via the satellite network regardless of telephone reception or via the Internet, the accuracy varies depending on the situation and is affected by weather conditions or interference (in cities it is less accurate), so smartphones they use GPS in conjunction with other technologies to make the data more precise; through the cell towers used for the provision of the cellular communication service, so that the telephone operators always know approximately where a device is located because it constantly communicates with the towers (which constantly emit unique "Tower IDs", Open Cell IDs to know towers near your location), and this is necessary in order to be able to route communication (telephone or Internet). From the presence in a "cell" and from the signal strength the position of the device can be roughly deduced. The operator keeps a log of this tracking that can only be consulted by the police forces: via wi-fi networks, mobile devices can obtain their position by scanning nearby wi-fi networks (or access points) , there are many wireless router databases; via Bluetooth Beacon, where the "beacons" are small radio transmitters that use one-way Bluetooth signals, which can be connected to various objects (keys, wallet), installed in places (eg shops) and, if the user consents to the connection Bluetooth, they can transmit information, allowing to infer the location of the device; through a combination of signals: modern smartphones combine multiple signals from the sources indicated above to calculate the position more precisely, also by combining the information provided by the countless sensors (altimeter, accelerometer).

personal data "consisting in use of those data to evaluate certain personal aspects relating to the natural person, in particular to analyze or predict aspects concerning health [...] the location or movement of that natural person": this kind of automated decision-making process (profiling), from a legal point of view, pursuant to art. 22, par. 4, *GDPR*, involving particular personal data, especially health, would be allowed, concerning our purpose, due to reasons of relevant public interest, such as a health emergency, on the basis of Union or members Countries law. In this case, the risk would be represented by obtaining real "profiles", capable of allowing assessments, analyzes or even forecasts of behavior, through algorithms applied to the set of initial health data belonging to the interested party[17]: that appears even more risky if we consider that information captured by the *app* in question are more detailed than those daily reached by large corporations. In fact, it is possible through the "Immuni" *app* to collect and send accurate information to the server on the people with whom we came in contact: however, this would be founded if a centralized tracking system had been adopted, while our Government has opted for a decentralized protocol (even if not entirely, in any case), in which the data should not (the conditional is a must) transit outside the user's device, with consequent greater security and reliability for the interested parties and app users; moreover, according to what was reported by the Ministry of Health, the *contact tracing* software was only developed to record the proximity between cell phones of the people with whom a subject came into contact, through data not directly suitable for revealing the identity of a person, which should remain only in the mobile phone until the possible diagnosis of contagion[18].

The "Immuni" *app* should not collect any data that allow to trace the user identity[19] and all data, whether saved in the device or in the server, should be deleted as soon as it is no longer needed. The Ministry of Health collects user data, which will be used only to contain the Covid-19 pandemic or for scientific research and will be saved on servers in Italy and managed by public entities.

4. Guarantees for the interested party: purpose limitation, minimization and anonymization of personal data

After analyzing the legal basis of the "Immuni" *app*, it is now necessary to speak about the essential guarantees so that the treatment, as well as lawful, is compliant with the *GDPR* and, at the same time, able to ensure the necessary balance between the protection of public health and privacy protection against excessive compression or intrusiveness. In particular, the "Immuni" *app*, as well as any other tracking systems deemed legitimate, should be used in compliance not only with the principle of lawfulness, but also with that of purpose limitation, minimization and anonymization.

First of all, basing on the purpose limitation principle, through the "Immuni" *app*, personal data must be processed and collected for an explicit purpose, consisting in monitoring, containing and mitigating the contagion from Covid-19, in order to protect public health, and not certainly to control or stigmatize people, repressing or spying

[17] The primary interest of companies is essentially knowing who the user is, "profiling" him, and then showing him advertisements corresponding to their interests; the State could abuse information and personal data, with a consequent serious danger to the protection of privacy, in the name of a questionable and perhaps unfounded reason for public security.

[18] Wanting to exemplify, X and Y are two hypothetical users: once installed by X, the app makes sure that his smartphone continuously emits a Bluetooth Low Energy signal that includes a random code. The same applies to Y. When X approaches Y, the smartphones of the two users record the other's random code in their memory, thus keeping track of that contact. They also record how long the contact lasted and how far the two smartphones were approximately. The codes should be generated at random, without containing any information about the device or the user. In addition, they should be changed several times every hour to further protect user privacy. Suppose, subsequently, Y tests positive for Covid-19. With the help of a health care worker, Y will be able to upload cryptographic keys to a server from which it is possible to derive its random codes. For each user, the app periodically downloads the new cryptographic keys sent by users who tested positive for the virus from the server. The app uses these keys to derive their random codes and check if any of those codes match those recorded in the smartphone's memory in the previous days. In this case, X's app will find Y's random code, check whether the duration and distance of the contact were such as to have caused a contagion and, if so, warn X.

[19] Apparently, the system does not ask for name, surname, date of birth, address, telephone number or email address. The app asks only for the Region and Province in which you are located. The app does not even collect any geolocation data, including GPS data: the movements would not seem to be tracked in any way. The Bluetooth Low Energy code transmitted by the app is generated randomly, without any information about the smartphone or the person. Furthermore, this code should change several times every hour, to better protect privacy. The data saved on the smartphone are encrypted, as are the connections between the app and the server.

on their behavior. The processing purpose, determined *ex ante*, thus represents a specific guarantee for the subjects involved.

Specifically, pursuant to art. 5, par. 1, lett. b, health data must be collected for that particular "specific, explicit and legitimate purpose", and subsequently processed in a compatible way with this purpose: the essential core of the compliance of the "Immuni" *app* with the Regulation is therefore represented by the determination of the explicit collection purpose and the compatibility of the processing with this purpose. A compatibility problem could instead arise for "further processing" or reuse of "sensitive" data for a different purpose than that expressed, such as for scientific research: this kind of reuse is "considered itself compatible with the initial purposes" by art. 5, par. 1, lett. b) and by art. 110-bis [introduced by art. 28, paragraph 1, lett. b), law n. 167 of 2017)] of the Code about personal data protection (legislative decree n.196 of 2003), which precisely legitimize it for scientific research purposes, albeit with the authorization of the Guarantor and with the adoption of minimization and anonymization techniques deemed suitable to protect the interested parties[20].

In particular, the principle of minimization requires containing or limiting processed data through the "Immuni" *app* to those necessary and indispensable for achieving the stated purpose, the containment of the coronavirus pandemic. This affects the tracking period as well as data retention, which must be temporally limited to the minimum necessary, that is to the strictly indispensable period (in this case), identified with the end of the emergency by the Guarantor Authority: hence, the risk of an excessive temporal dilation due to the possible continuation of the emergency *sine die*, considering, albeit ex ante, a *dies ad quem* moved forward periodically. As recommended by the Guarantor Authority, the current health crisis cannot and must not turn into an opportunity to derogate from the principle of minimization and consequent limitation of data processing and storage: both (processing and storage) should be limited in light to real needs and medical relevance, i.e. exclusively for the crisis duration due to Covid-19, concerning also epidemiological considerations such as the incubation period. At the end, all personal data should be deleted[21].

Pursuant to art. 5, par. 1, lett. *c)*, the principle of minimization is therefore declined in the canon of "necessity": so that if, precisely, the purpose is the infections containment, personal data that should only be acquired are health data and such information can be used exclusively to reduce epidemiological risk. Any further data or any further

[20] Textually, "the Guarantor may authorize the further processing of personal data, including those of the special treatments referred to in Article 9 of the Regulation, for scientific research or statistical purposes by third parties who mainly carry out these activities when, due to for particular reasons, informing the interested parties is impossible or involves a disproportionate effort, or it risks making it impossible or seriously jeopardizing the achievement of the research objectives, provided that appropriate measures are taken to protect the rights, freedoms and legitimate interests of interested party, in compliance with article 89 of the Regulation, including preventive forms of data minimization and anonymization".

[21] o for example, if you request the release of a declaration certifying the non-origination from areas at epidemiological risk and the absence of contacts, in the last 14 days, with subjects who tested positive for Covid-19, remember to pay attention to the regulations on processing of personal data, since the acquisition of the declaration constitutes data processing. To this end, it is suggested to collect only the necessary, adequate and relevant data with respect to the prevention of contagion from Covid-19. If you request a statement on contacts with people who tested positive for Covid-19, you must refrain from requesting additional information about the person who tested positive; or, if a declaration is requested on the origin from areas at epidemiological risk, it is necessary to refrain from requesting additional information regarding the specificities of the places (Prot. April 24, 2020, note 2). With regard to the processing of personal data relating to location via mobile telephones, the EDPB warns that the legislative measures introduced to safeguard public safety must be exceptional and must be "necessary", proportionate and adequate. The EDPB and the Guarantor for the protection of personal data have also recommended compliance with the principle of transparency and accuracy of the data processed in the adoption of emergency technological measures towards the interested parties. As is known, the first, lacking an express statement in the previous legislation, is now explicitly mentioned in both general terms, in art. 5, where the obligation to process data in a "transparent" manner is imposed on the owner; is more specific, in art. 12, according to which the information and communications to which the interested party is entitled must be provided "in [...] transparent form". In particular, art. 12 identifies the methods and characteristics necessary to guarantee "transparent" information: the information must be concise and easily accessible, the language used must be clear and comprehensible even for non-experts (especially if it is a question of minors), structured in a simple way, avoiding complex sentences, abstract or ambiguous terms that leave room for multiple interpretations. The principle of accuracy requires that the data be correct, therefore updated, rectified and even deleted if inaccurate with respect to the purpose for which they are processed: on this point, see D. ACHILLE, Art. 12, in E. GABRIELLI (directed by), *Commentario del codice civile*, cit., p. 208.

use of personal data would result in a violation of the principle in question, and therefore of the *GDPR*, because it exceeds what is strictly "necessary" for the achievement of that purpose as predetermined and communicated to the interested party (i.e., the fight against Covid-19). This does not mean that other data may not be collected or the collected data can be processed in a different way, but in such cases, for each of them, it will be necessary to obtain the consent of the interested party or to rely on another of the conditions of lawfulness provided for by the Regulation, different from the one legitimizing the treatment of health data and identified in art. 9.2, lett. *i)* of the *GDPR*.

Concerning the use of data, and in particular the "Immuni" *app*, the *EDPB* and the *European Digital Right* association recommend the anonymous form, where "anonymization" means the use of a series of techniques aimed to eliminate the possibility of linking data to an identified or identifiable natural person with a "reasonable" effort[22]: this reasonableness should be assessed in the light of objective aspects (such as times and technical means, rarity of a phenomenon, population density, data nature and volume). In the event of a positive outcome of this assessment, the data will not be anonymised[23].

While location data from telecommunications operators and/or information society services are notoriously difficult to anonymize because their sequence allows us to reconstruct the movements of a specific person over time (eg. home-work), the "Immuni" *app* should not collect any data suitable for tracing the identity of a user. This processing system, for example, does not ask for nor it is designed to obtain name, surname, date of birth, address, telephone number or email address, geolocation data or GPS: the movements do not seem to be tracked or traceable. The "Immuni" *app* requires only the Region or Province in which you are located and the *Bluetooth Low Energy* code transmitted by the *app* appears to be randomly generated, without any information about the smartphone or person. Furthermore, this code changes several times, at short time intervals, just to protect privacy. The data saved on the smartphone are encrypted, as well as the connections between the *app* and the server[24]: all this should ensure the anonymization of the data.

The terms of the speech and the effectiveness of personal data protection would negatively change if the tracking data (instead of anonymised) were only pseudonymised[25]. Infact, although pseudonymisation is "ideal for

[22] Reasonableness is a relative and "reasonable" criterion means that the probability of the event occurring is higher than mere probability. The concept includes any process, even purely deductive, through which it is possible to arrive at identification. When this landing or connection is interrupted, we speak of anonymization. Recital no. 26 excludes the application of the data protection regulations to anonymous information, i.e. information that does not refer to an identified or identifiable natural person or to personal data made sufficiently anonymous to prevent or no longer allow the identification of the data subject: on the subject, v. G. M. RICCIO - G. SCORZA - E. BELISARIO (edited by), *GDPR e normativa Privacy commentario*, Vicenza 2018, p. 29 ss.

[23] E. PELINO, *Informazioni anonime, dati anonimizzati*, in L. BOLOGNINI - C. BISTOLFI - E. PELINO, *Il Regolamento Privacy europeo*, Milano 2016, p. 74: anonymization is a treatment to which personal data are subjected, aimed at obtaining the irreversible de-identification of the person to whom the information refers. "Anonymous" data is "data that originally, or following processing, cannot be associated with an identified or identifiable data subject": on the subject, see for everyone, FINOCCHIARO (a cura di), *Diritto dell'anonimato. Anonimato, nome e identità personale*, in GALGANO (directed by), *Trattato di diritto commerciale e diritto pubblico dell'economia*, XLVIII, Padova 2008.

[24] Nonetheless, since this is a system that is still running in, there are several unresolved issues. First of all, it seems legitimate to ask whether the data, given that they will reside in the single phone, albeit anonymously, can be taken from other apps that traditionally require access to use the single software and which, by crossing the data with others relating to the phone (IP , SIM card, photos, etc.), could use them improperly. It would seem that, although the individual data is encrypted, a de-anonymization and tracing to the identities of the individuals and to the health data on the infections cannot be excluded, carrying out a manipulation of millions of these crossed data.
Another risk seems to be represented by a possible intrusion via the so-called bluetooth. sniffers (interceptors) capable of intercepting data. It is known that bluetooth is a communication channel used not only to interconnect other devices such as earphones, but also for the passage of data between close people: hence the problem of the security of this communication channel used for the app " Immune ". Finally, a further question concerns the server that will be used to store the data: a server that, appropriately, should reside in Italy and managed by the PA, in particular by the Ministry of Health, and not by companies, especially foreign ones that could have access to it and collect data for other purposes.

[25] Art. 4, no. 5, GDPR defines pseudonymisation as the processing of personal data in such a way that personal data can no longer be attributed to a specific data subject without the use of additional information.

increasing data protection"[26], it would nevertheless allow people to be traced to discover their identity[27], especially where identity correspondence lists with the relative pseudonyms or bidirectional cryptographic algorithms are used[28]: unlike anonymization, this is essentially characterized by an irreversible "de-identification", as the one arising from the "Immuni" *app* seems to have to be qualified.

In terms of effectiveness, also in the light of the reflections carried out until now, the "Immuni" *app* has several issues still to be solved. In this regard, the Minister for Technological Innovation specified that the effectiveness threshold (also shared by the Privacy Guarantor) of the application is the adoption by at least 60-70% of Italian people[29]: the "Immuni" *app* works, only if a critical mass of application users is reached[30]. Since this is a completely voluntary tool and not all population groups have adequate familiarity with smartphones, it is clear that the main problem (on whose solution the success or failure of the application depends) is precisely to achieve this membership threshold, also through measures that incentivize the download of the application as long as they are lawful and compliant with the principles in force on the matter[31].

Another problem not to be underestimated concerns the complementary tools to support the *contact tracing* initiative. The efficiency of the technological solution, and in particular of the "Immuni" *app*, cannot be separated either from carrying out of checks, using swabs, to identify the positives and to isolate the less serious cases, for which healthcare should take place at home and ensuring a quick swab to those who have received the notification (*testing*); or from a broader tracing system, made up also by manual controls and management of epidemiological big data (*tracing*). The "Immuni" *app* proves to be ineffective if it's not accompanied and supported by positive actions (eg contact and swab all those who had contact with an infected person in the previous two weeks) [32].
In conclusion, once censored, as it would seem, the use of solutions that allow access to the individual position, the hope is that the purpose of the "Immuni" *app* - and any other future and/or different applications - remains discovering "events", that is, contacts with infected people, and not movements or behaviors of the interested subjects, avoiding also the spread of social alarm and the stigmatization of subjects who tested positive: the only purpose basing on which a compression of personal freedom, in abstract and concretely, should be legitimized, must be and will expressly remain only being able to go up the chain of potential infected and adopt the appropriate measures to contain the pandemic.

[26] Thus, G.M. RICCIO - G. SCORZA - E. BELISARIO (edited by), *GDPR e normativa Privacy commentario*, cit., p. 41.
[27] «Conversely, it is possible to disguise identity by making re-identification impossible, for example with one-way encryption that typically creates anonymous data»: thus, C. DEL FEDERICO - A. R. POPOLI, *Disposizioni generali*, in G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla* Privacy *e sulla protezione dei dati personali*, 2017, Bologna, 97.
[28] With pseudonymization, data are kept, which are replaced with a pseudonym and created with different techniques, such as cryptography, hashing, etc. In this case, unlike the "anonymized" data, it is possible to indirectly go back to the original content, if you have the decryption keys of the algorithm used. A pseudonymised data is mainly based on three characteristics: identification, i.e. the possibility of identifying the initial data of the persons, the correlation with the original data and the deduction, if for example the replaced attribute has similarities with the original, or by integrating different data we can deduce which is the source.
[29] According to some experts of the British national health system, however, 40% would give advantages in reducing the victims, even 30%.
[30] Only an effective app on this point, together with an equally effective communication of the solutions adopted, will be able to accompany users towards a gradual but massive adoption of this important tool for combating the spread of Covid-19.
[31] At present, the *contact tracing* app (available from June 15, 2020 throughout the country) just exceeds 4 million downloads. The contagion monitoring system has therefore not so far made inroads and, in the face of new Covid outbreaks that have broken out in the country, it satisfies very little, also due to the malfunctioning according to what the newspapers reported: hence the need, on the one hand, a single app rather than similar tracking systems at regional level (as in Lombardy, Sicily and Sardinia), with differentiated outcomes among citizens according to the spread of the infection; on the other hand, the improvement of the system and the possibility of installing it on all devices, increasing the trust of citizens in this monitoring system, who are still too suspicious and fearful of possible violations of privacy, despite the reassurances disseminated in this regard through the various media.
[32] These actions, however, cannot be particularly penalizing, otherwise, presumably, a drastic drop in adoptions would be obtained. This "detector" always at hand could induce you to change your behavior, perhaps moving to a distance greater than the safe distance from other people to avoid even brief irrelevant contacts (think of a passerby crossed on a sidewalk or sidewalk of a car in a parking lot) can "mark" us as positive, if on the one hand this can help in the effectiveness of the markings, it is an aspect that could generate tensions. Nor does it seem decisive, in this regard, to recall the principle of responsibility or "*accountability*": it is not a problem of clear definition or identification of the ownership of the processing of an app for tracing contacts, but rather the fact that an app for Contact tracking involves storing and/or accessing particular information. The Committee also believes that the national health authorities should be the owners of this treatment; however, other ownership configurations may be considered.