ISSN 2704-8012

European Journal of Privacy Law & Technologies

2020/1



G. Giappichelli Editore

European Journal of Privacy Law & Technologies

Directed by Lucilla Gatt

2020/1

G. Giappichelli Editore

European Journal of Privacy Law & Technologies
On line journal
Italian R.O.C. n. 25223

G. GIAPPICHELLI EDITORE - TORINO
VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it



The Journal is one of the results of the European project TAtoDPR (Training Activities to Implement the Data Protection Reform) that has received funding from the European Union's within the REC (Rights, Equality and Citizenship) Programme, under Grant Agreement No. 769191.

The contents of this Journal represent the views of the author only and are his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Published Online by G. Giappichelli in June 2020
www.ejplt.tatodpr.eu

FROM INFORMATION PRIVACY TO EMERGENCY PRIVACY

Valeria Manzo

Lawyer in Naples and Ph.D. (c) at Università della Campania Luigi Vanvitelli

Marco Bergamo

Lawyer in Naples

Abstract:

If before the creation and dissemination of computers made it possible to collect, organise and transmit an indistinct series of personal information, the right to privacy was linked to the concept of private property and the means for its protection and then, in a social dimension, came to coincide with the individual's ability to control the circulation of information relating to him – a power that often is essential to maintaining social relationship and personal freedom, With the development of technologies and the use of personal data processing, as well as the possibility of their exchange and aggregation through the Internet and the creation of databases, the needs have evolved (and are evolving) even more significantly towards a collective dimension of information privacy.

The innate mutability of the concept of privacy as a concept which is strongly affected by social, cultural and technological changes, pushes, in this way, to prepare a cautious legal schematization of the institution also in light of the emergency situation generated by the diffusion of the COVID-19.

It is necessary, therefore, to ask whether the existing legislation can be considered sufficiently malleable to the changed framework of protection of personal data or whether the solutions adopted can be considered legitimate and proportionally oriented to respect the new "emergency privacy".

Key-words: privacy, GDPR, contact tracing, COVID-19, Immuni app, data breach.

Summary: 1. The regulatory framework and compression of rights. – 2. The contact tracing and Immuni app. – 3. The data breach. – 4. Conclusions.

1. The regulatory framework and compression of rights

In our legal system [1], the protection of personal data is, today, entrusted to Legislative Decree no. 101 of 10 August 2018, concerning "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*".

As can be seen from a simple reading of the first reference standards, the above mentioned regulatory patchwork shows that there have been no formal amendments to Legislative Decree no. 196 of 30 June 2003 [2], which are based on a different and more modern approach to the protection of personal data, which is based on the tightening of penalties (including criminal penalties) that already characterized the beginning of the entire legislative system.

In the face of the epidemiological emergency from COVID-19, a series of regulatory acts have followed one another, the most important of which include personal data protection.

On 9 March 2020, the Government adopted Decree Law no. 14/2020, containing "*Disposizioni urgenti per il potenziamento del Sevizio sanitario nazionale in relazione all'emergenza COVID-19*", which came into force the following 10 March – with which, resuming the provisions of the Ordinance of the Head of the Department of Civil Protection (hereinafter O.C.D.P.C.) no. 630 of 3 February 2020, special provisions were dictated on the processing of personal data in the current pandemic context.

With the above mentioned O.C.D.P.C. it has been possible to carry out the processing of personal, particular and also judicial data necessary for the performance of the Civil Protection function, connected to the onset of pathologies deriving from transmissible viral agents, allowing, where necessary, a flow of data exchange between the subjects identified by the Legislative Decree of 2

[1] In relation to the right to privacy the following authors should be noted, among many: SD Warren-LD Brandeis, 'The Right to Privacy' (1890) IV Harvard Law Review 289-320; V Frosini, *Teoria e tecnica dei diritti umani: i diritti umani nella società tecnologica* (3rd edn, Edizioni Scientifiche Italiane 1998); A Giddens, *Il mondo che cambia: come la globalizzazione ridisegna la nostra vita*, (1st edn, Il Mulino 2000); S Rodotà, '*Diritto, diritti, globalizzazione'* (2000) I, *Riv. Giur. Lav*., 766; N Irti, '*Le categorie giuridiche della globalizzazione'* (2002) XLVIII n. 5 *Riv. di dir. Civile 625-635;* TM Ubertazzi, *Diritto alla privacy, natura e funzioni giuridiche* (1st edn, Cedam 2005); F Galgano, *La globalizzazione nello specchio del diritto* (1nd edn, Il Mulino 2005); A Bevere-A Cerri, *Il diritto di informazione e i diritti della persona. Il conflitto della libertà di pensiero con l'onore, la riservatezza, l'identità personale* (2nd edn, Giuffrè 2006).

[2] Bearing "*Codice in materia di protezione dei dati personali*".

January 2018, n. 1 (better known as the Civil Protection Code) in articles 4 [3] and 13 [4].

[3] **Componenti del Servizio nazionale della protezione civile: "***1. Lo Stato, le Regioni e le Province autonome di Trento e di Bolzano e gli enti locali sono componenti del Servizio nazionale e provvedono all'attuazione delle attività di cui all'articolo 2, secondo i rispettivi ordinamenti e competenze.*

2. Le componenti del Servizio nazionale possono stipulare convenzioni con le strutture operative e i soggetti concorrenti di cui all'articolo 13, comma 2 o con altri soggetti pubblici.

3. Le componenti del Servizio nazionale che detengono o gestiscono informazioni utili per le finalità del presente decreto, sono tenute ad assicurarne la circolazione e diffusione nell'ambito del Servizio stesso, nel rispetto delle vigenti disposizioni in materia di trasparenza e di protezione dei dati personali, ove non coperte di segreto di Stato, ovvero non attinenti all'ordine e alla sicurezza pubblica nonché alla prevenzione e repressione di reati".

[4] **Strutture operative del Servizio nazionale della protezione civile**: "*1. Oltre al Corpo nazionale dei vigili del fuoco, che opera quale componente fondamentale del Servizio nazionale della protezione civile, sono strutture operative nazionali:*

a) le Forze armate;

b) le Forze di polizia;

c) gli enti e istituti di ricerca di rilievo nazionale con finalità di protezione civile, anche organizzati come centri di competenza, l'Istituto nazionale di geofisica e vulcanologia e il Consiglio nazionale delle ricerche;

d) le strutture del Servizio sanitario nazionale;

e) il volontariato organizzato di protezione civile iscritto nell'elenco nazionale del volontariato di protezione civile, l'Associazione della Croce rossa italiana e il Corpo nazionale del soccorso alpino e speleologico;

f) il Sistema nazionale per la protezione dell'ambiente;

g) le strutture preposte alla gestione dei servizi meteorologici a livello nazionale.

2. Concorrono, altresì, alle attività di protezione civile gli ordini e i collegi professionali e i rispettivi Consigli nazionali, anche mediante forme associative o di collaborazione o di cooperazione appositamente definite tra i rispettivi Consigli nazionali nell'ambito di aree omogenee, e gli enti, gli istituti e le agenzie nazionali che svolgono funzioni in materia di protezione civile e aziende, società e altre organizzazioni pubbliche o private che svolgono funzioni utili per le finalità di protezione civile.

3. Le Regioni, relativamente ai rispettivi ambiti territoriali, e nei limiti delle competenze loro attribuite, possono individuare proprie strutture operative regionali del Servizio nazionale, in ambiti operativi diversi da quelli di riferimento delle strutture di cui al comma 1.

4. Le strutture operative nazionali e regionali svolgono, nell'ambito delle rispettive competenze istituzionali, salvo quanto previsto dal comma 5, le attività previste dal presente decreto. Con le direttive di cui all'articolo 15, si provvede a disciplinare specifiche forme di partecipazione, integrazione e collaborazione delle strutture operative nel Servizio nazionale della protezione civile.

5. Le modalità e le procedure relative al concorso delle Forze armate alle attività previste dal presente decreto sono disciplinate, secondo quanto previsto in materia dagli articoli 15, 89, comma 3, 92 e 549-bis del decreto legislativo 15 marzo 2010, n. 66, con decreto del Presidente del Consiglio dei ministri, sulla proposta del Capo del Dipartimento della protezione civile, di concerto con il Ministro della difesa, adottato ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400".

With art. 14 of the D.L. [5], referring to the principles enshrined in art. 5 of EU Regulation/2016/679 on data protection (so-called GDPR) of lawfulness, correctness and transparency, minimization, accuracy, limitation of storage, integrity and confidentiality, the following additional corollaries are crystallized with

[5] Disposizioni sul trattamento dei dati personali nel contesto emergenziale: "*1. Fino al termine dello stato di emergenza, deliberato dal Consiglio dei ministri in data 31 gennaio 2020, per motivi d'interesse pubblico nel settore della sanità pubblica e, in particolare, per garantire la protezione dall'emergenza sanitaria a carattere transfrontaliero determinata dalla diffusione del COVID-19 mediante adeguate misure di profilassi, nonché per assicurare la diagnosi e l'assistenza sanitaria dei contagiati ovvero la gestione emergenziale del Servizio sanitario nazionale, nel rispetto dell'articolo 9, paragrafo 2, lettere g), h) e i), e dell'articolo 10 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, nonché dell'articolo 2-sexies, comma 2, lettere t) e u), del Decreto Legislativo 30 giugno 2003, n. 196, i soggetti operanti nel Servizio nazionale di protezione civile dell'articolo 9, paragrafo 2, lettere g), h) e i), e dell'articolo 10 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, nonché dell'articolo 2-sexies, comma 2, lettere t) e u), del decreto legislativo 30 giugno 2003, n. 196, i soggetti operanti nel Servizio nazionale di protezione civile, e i soggetti attuatori di cui all'articolo 1 dell'ordinanza del Capo del Dipartimento della protezione civile 3 febbraio 2020, n. 630, nonché gli uffici del Ministero della salute e dell'Istituto Superiore di Sanità, le strutture pubbliche e private che operano nell'ambito del Servizio sanitario nazionale e i soggetti deputati a monitorare e a garantire l'esecuzione delle misure disposte ai sensi dell'articolo 3 del decreto-legge 23 febbraio 2020, n. 6, convertito, con modificazioni, dalla legge 5 marzo 2020, n. 13, anche allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, possono effettuare trattamenti, ivi inclusa la comunicazione tra loro, dei dati personali, anche relativi agli articoli 9 e 10 del regolamento (UE) 2016/679, che risultino necessari all'espletamento delle funzioni attribuitegli nell'ambito dell'emergenza determinata dal diffondersi del COVID-19.*

2. La comunicazione dei dati personali a soggetti pubblici e privati, diversi da quelli di cui al comma 1, nonché la diffusione dei dati personali diversi da quelli di cui agli articoli 9 e 10 del regolamento (UE) 2016/679, è effettuata, nei casi in cui risulti indispensabile ai fini dello svolgimento delle attività connesse alla gestione dell'emergenza sanitaria in atto.

3. I trattamenti di dati personali di cui ai commi 1 e 2 sono effettuati nel rispetto dei principi di cui all'articolo 5 del citato regolamento (UE) 2016/679, adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.

4. Avuto riguardo alla necessità di contemperare le esigenze di gestione dell'emergenza sanitaria in atto con quella afferente alla salvaguardia della riservatezza degli interessati, i soggetti di cui al comma 1 possono conferire le autorizzazioni di cui all'articolo

2-quaterdecies del decreto legislativo 30 giugno 2003, n. 196, con modalità semplificate, anche oralmente.

5. Nel contesto emergenziale in atto, ai sensi dell'articolo 23, paragrafo 1, lettera e), del menzionato regolamento (UE) 2016/679, fermo restando quanto disposto dall'articolo 82 del decreto legislativo 30 giugno 2003, n. 196, i soggetti di cui al comma 1 possono omettere l'informativa di cui all'articolo 13 del medesimo regolamento o fornire una informativa semplificata, previa comunicazione orale agli interessati della limitazione.

6. Al termine dello stato di emergenza di cui alla delibera del Consiglio dei ministri del 31 gennaio 2020, i soggetti di cui al comma 1 adottano misure idonee a ricondurre i trattamenti di dati personali effettuati nel contesto dell'emergenza, all'ambito delle ordinarie competenze e delle regole che disciplinano i trattamenti di dati personali".

regard to data interchange flow, limiting the scope of application of these rules having regard to the state of health emergency determined by the deployment of COVID-19:

– indispensability (data may be collected only for the purpose of carrying out activities related to the management of the health emergency in progress);
– reconciliation (understood as a balance between fundamental interests such as the need to manage the current epidemiological emergency with the right to protection and confidentiality of the data of the individuals concerned);
– temporariness (the data may be kept for a limited period of time, to be recognized with the cessation of the state of emergency or in the 60 days following the collection).

In view of the above, it is necessary to analyze to what extent it can be considered possible to compress the rights constitutionally protected by reason of the achievement of a superior good, such as public health.

The balance between the protection of the fundamental rights of the individual and the pursuit of collective needs is inherent to the very nature of human rights, which constantly conflict with each other and with general interests [6].

If it is true that the Government has directed its course of action towards the repression of the spread of the virus, this has been achieved through the enactment of measures that have had a profound impact on the individual sphere of human action by compressing rights such as those enshrined in Articles 13, 16, 17, 19 and 24 of the Constitutional Charter.

Let us analyze them individually.

The main *vulnus* of governmental measures has been constituted by the compression of personal freedom (constitutionally guaranteed by art. 13) as "irrepressible prerogative of the person" [7] with the consequence that, in order to trace the legitimacy or otherwise of the interventions of the Central Government, it is necessary to identify the way to understand the reservation of the law.

If, in fact, it is inclined to the relative character of the reservation of law in question, the same must be considered legitimate; illegitimate, if the reservation is intended as absolute.

The relationship between security and freedom has, thus, revealed how, in a balance between the right to freedom of movement and limits to the exercise of the same, it should be reviewed also in the light of the general criterion of "rea-

[6] M. Cartabia, '*I principi di ragionevolezza e proporzionalità nella giurisprudenza costituzionale italiana'. Atti del seminario svoltosi in Roma*, Palazzo della Consulta, 13-14 ottobre 1994.

[7] F.M. Stornelli, 'La graduale limitazione dei diritti e delle libertà fondamentali nella stagione del coronavirus' (2020), on https://www.iusinitinere.it/la-graduale-limitazione-dei-diritti-e-delle-liberta-fondamentali-nella-stagione-del-coronavirus-26470.

sonableness" understood as the right relationship of the act to the purpose [8].

The current epidemiological emergency has also led the Government to adopt some measures restricting freedom of movement and residence (protected by Article 16 of the Constitution).

The most important measure, from a general and abstract point of view, is Decree Law no. 6 of 2020, which includes a list of the measures that can be adopted in order to contain the spread of contagion, including Article 1, paragraph 2, letter. a) which provides for the "prohibition of removal from the municipality or area concerned", the following letter b) which provides for the "prohibition of access to the municipality or area concerned" and, lastly, letter m) which provides for the possible "limitation of access or suspension of the services of transport of goods and people on land, air, rail, sea and inland waters, on national network, as well as local public transport, even non-scheduled, unless specific exceptions provided by the measures referred to in Article 3", has given rise to many repercussions on the full enjoyment of freedom of movement.

Indirectly, the freedom of assembly (constitutionally guaranteed by article 17) has also been compressed by article 1, paragraph 2, letter c) of the D.L. in question with the introduction of the prohibition to create assemblies, suspending demonstrations or initiatives of any kind.

The same is true with regard to the limitation of freedom of worship (recognized by art. 19 of the Constitutional Charter) compressed by the same D.L. since the competent Authorities have been authorized to adopt measures aimed at suspending any manifestation or event of a religious nature.

Finally, the generalized postponement of hearings and the suspension of deadlines until April 15, 2020 and the provision of specific rules relating to the different types of trial with all the repercussions that have resulted, has produced direct effects on the right to take legal action for the protection of their rights and interests, as well as the right of defense (protected by Article 24 of the Constitution).

Well, from the analysis of what has been highlighted so far, it must be asked: where is the legal basis for the power of the State to limit the rights of individuals in order to pursue an aim of general interest?

If it is true that our Constitution does not contain any provision on the "state of emergency" [9], it is also true that, in our country, this state of emergency connected with natural calamitous events of natural origin that, due to their intensi-

[8] A. Candido, 'Poteri normativi del Governo e libertà di circolazione al tempo del COVID-19' *(2020) 1/2020, Forum di Quaderni Costituzionali,* 419 e ss.

[9] C. Blengino, 'Emergenze e diritti costituzionali' (2020) on *https://www.ilpost.it/carlo blengino/2020/03/19/emergenze-e-diritti-fondamentali/.*

ty/extent, must be faced with extraordinary means and powers, was declared on 31 January 2020 by a resolution of the Council of Ministers pursuant to the first paragraph of Article 24 of the Civil Protection Code.

In the absence of indications both in national legislation and in the Constitutional Charter, reference must be made to the relevant norms of international law and, in particular, to the European Convention for the Protection of Human Rights and Fundamental Freedoms of 1950 (ratified in Italy by Law no. 848 of 4 August 1955) [10].

Many provisions of the Convention in question provide for so-called "limitation clauses" with the possibility of limiting the rights guaranteed in them when this is necessary for the pursuit of objectives of general interest including, in particular, national security and the protection of health and rights.

These clauses are based on a reasoning of the concrete case and it is up to the national authorities to achieve a proportional balance between the limiting measure imposed and the general interest objectives pursued.

The measures adopted by the Government, although particularly restrictive, are proportional, given that the only rules that cannot be derogated from are the right to life and the prohibition of torture and that the prohibitions imposed seem to be the only possible and most effective responses to contain the pandemic.

2. The contact tracing and Immuni app

When and how can it be considered right to sacrifice the right to privacy of the individual for the health of the community?

Although many individuals are willing to give up their data on a daily basis (sometimes completely unconsciously) for purely recreational applications, can the same be said in the face of such a health emergency?

In order to manage unpredictability, is it necessary to develop a culture and education that recognises the value of data as a resource for dealing with critical situations?

Does EU legislation on GDPR contain rules that can be applied in the processing of personal data in particular contexts such as the COVID-19 pandemic?

These are some of the main questions that we will try to answer.

The Data Protection Regulations provide for this:

[10] G. Zagrebelsky, 'La prevista adesione dell'Unione Europea alla Convenzione europea dei diritti dell'uomo' (2007) on *www.europeanrights.eu/public/commenti/Adesione_Zagrebelsky.doc*.

– in recital 46 [11] the possibility that certain objectives, such as monitoring the development of epidemics and their spread, may find the right legal framework;

– in recital 54 [12] the possibility that the consent of the person concerned may be disregarded for public health reasons;

– in point (d) of the first paragraph of Article 6 and point (c) of the second paragraph of Article 9, the lawfulness of treatment only to the extent necessary to safeguard the vital interests of the data subject or of another natural person.

The term "necessary" in the European rules just mentioned is a clear reference to the regulatory principles governing all processing of personal data and, in particular, to the principle of minimisation according to which only personal data that are adequate, relevant and limited to what is necessary to fulfil the purposes for which they are processed may be processed.

On the basis of an analysis of the necessary balance between equally important rights such as personal freedom and the right to the protection of personal data on the one hand and the protection of individual and public health on the other, the question arises as to when a compression of the right to privacy can be considered a necessary, appropriate and proportionate measure within a democratic society, both on the usefulness of adopting ways of informing the public in order to avoid the unconditional dissemination of sensitive data concerning the state of health and, lastly, on the measures that will have to be taken, once the emergency has ceased and the purpose of the processing has been reached, in order not to convert the information collected to the satisfaction of further purposes.

---

[11] "*The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters*".

[12] Which reads: "*The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council (1), namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies*".

The contact tracing, or the tracking of the people encountered and the places frequented by infected persons, pursues the main purpose of monitoring the spread of the virus on the territory and, at the current state of the art, will be implemented via Bluetooth device, with applications, approved by the authorities, installed on citizens' devices, involving, on a voluntary basis, the analysis of transactions with credit cards or other means of payment, geolocation data available to mobile phone operators, or through the use of Big Data (data from, for example, companies producing "smart" devices, market loyalty cards, license plate detection or cameras with facial recognition).

Such a system of automated analysis and processing of information and personal data is clearly more efficient than the self-declaration of individuals, as it allows to intervene with targeted actions of prevention and containment.

If by order no. 10 of April 16, 2020 of the Extraordinary Commissioner for Emergency, Dr. Domenico Arcuri, the contact tracing app that will be used to counter the COVID-19, called "Immuni", on April 29, 2020 was approved the Justice Decree that introduces, ex multis, urgent provisions on the protection of personal data in the tracking of contacts and contagions from COVID-19 through the new "Immuni app".

The Decree provides, for the sole purpose of alerting people who have come into contact with individuals who have tested positive to COVID-19 and protect their health through prophylaxis measures related to the health emergency, that an IT platform be established at the Ministry of Health for the tracking of close contacts between individuals who install, on a voluntary basis, the Immuni app for mobile phone devices.

The Ministry will therefore have to identify the appropriate technical and organisational measures to ensure a level of security appropriate to the high risks to the rights and freedoms of the persons concerned by ensuring, in particular, the following:

– that users receive, before the application is activated, clear and transparent information in order to achieve full awareness of the purposes and processing operations, the pseudonymisation techniques used and the data retention times;

– that the personal data collected by the application are only those necessary to inform users of the application that they are in close contact with other users identified as positive to COVID-19 and to facilitate the possible adoption of health care measures in favour of the same persons;

– that the processing carried out is based on the proximity data of the devices, rendered anonymous or, where this is not possible, pseudonymised;

– that the confidentiality, integrity, availability and resilience of processing systems and services are guaranteed on a permanent basis, as well as appropri-

ate measures to avoid the risk of reidentification of data subjects to whom pseudonymised data undergoing processing relate;

– lastly, that data relating to close contacts are stored, including in users' mobile devices, for the period strictly necessary for the processing (the duration of which is determined by the Ministry of Health) and that they are subsequently deleted automatically upon expiry of the period.

It is also expressly provided for:

– that the data collected may not be processed for purposes other than those specified;

– that, in case of non-use of the application, there will be no limitation/consequence with regard to the exercise of the fundamental rights of the subjects concerned;

– that the platform must be realized exclusively with infrastructures located on the national territory and managed by administrations or public bodies or companies with total public participation and that the computer programs developed for the realization of the platform are of public ownership;

– finally, that the use of the application and of the platform, as well as any processing of personal data must be interrupted at the date of the end of the state of emergency, and in any case no later than 31 December 2020. By that date, in fact, all personal data processed must be deleted or made permanently anonymous.

Let's analyze, therefore, what are the characteristics, the data tracking mode and what seem to be the limits of the Immuni app.

It can be downloaded on a voluntary basis and free of charge; it will be initially tested, starting from the end of May, in some pilot regions and then adopted at national level.

With regard to the features, the app in question consists of two parts: the first is dedicated to contact tracing through Bluetooth technology [13], the second, however, is intended to host a sort of clinical diary where the individual user can write down all the most relevant information [14].

As far as the tracking mode is concerned, it should be noted that mobile phones will keep in memory (in the form of encrypted anonymous codes) the data of other mobile phones with which they have come into contact; associated

[13] Through the Bluetooth device it is possible to detect the proximity between two smart phones within one meter and retrace back all the meetings of a person who tested positive for COVID-19, so you can track and isolate the potential infected.

[14] Such as gender, age, previous illnesses, medication intake, health conditions and the presence of symptoms compatible with the virus.

with these codes there will be metadata that will come into play in the assessment of the risk of contagion.

In the event that one of the subjects who downloaded the app is positive for the virus, the health care workers will provide an authorization code with which he can download his anonymous code on a ministerial server.

If the app recognizes an infected person's code in its memory, it will display an appropriate notification to the user.

In relation to the limits, the first of an operational nature concerns the voluntary nature of the membership; in fact, as specified by the European Committee on the Protection of Personal Data (EDPB) and by our Guarantor Authority itself in principle, location data can be used by the operator only if made anonymous or with the consent of individuals.

This aspect alone raises perplexity because there is a risk of using an app that involves the processing of particular categories of personal data without having sufficient guarantees about its functionality with the risk of being faced with the "technological drift" mentioned by Rodotà.

Referring to the principles enshrined in the GDPR analyzed above, it is recalled that it is (already) allowed to the competent public health authorities to process personal data in the context of an epidemic, in accordance with national law and under the conditions laid down therein.

Consequently, where treatment is deemed necessary for reasons of overriding public interest in the field of public health, where there is a presumption of lawfulness, the consent of individuals may well be disregarded.

It goes without saying, therefore, that the question arises as to whether the tracking system is based on a different assumption from that of lawfulness; otherwise it would not explain the recourse to the expression of consent (which, however, significantly affects the actual functioning of the system).

Other limits are represented by the necessary adoption of adequate security measures on the entire processing chain in order to ensure compliance with data protection principles, such as the proportionality of the measure in terms of duration and scope, the reduced conservation of the same and the respect of the purpose limitation, as well as the replacement of geolocation at satellite level with Bluetooth connectivity, which has the criticality of not having a generic communication band (such as Wi-Fi).

On this point, the Secretary General of the Authority for the protection of the personal data, Dr. Giuseppe Busia, had underlined how it is necessary that the treatment of the personal data takes place on the basis of a transparent regulation (containing adequate guarantees), under the supervision of the competent public authorities, in respect of the principle of reasonableness at the base of the GDPR, and that the use of the same does not become an instrument aimed at in-

creasing the informative power of the platforms or of the large operators [15].

One wonders, therefore, whether what is contained in the Justice Decree can be considered sufficient to meet the above mentioned protection requirements.

3. The data breach

If and how can contact tracing lead to risks arising from the data breach?

In order to answer this question it is necessary to start from the definition of data breach.

This term refers to a security incident that may result, accidentally or illegally, in the destruction, loss, modification, unauthorized disclosure or access to personal data transmitted, stored or processed in the financial, health or industrial property spheres.

The phenomenon under consideration may occur as a result of:

– accidental loss (think of the data breach caused by the loss of a USB stick);
– theft (think of the data breach caused by the theft of a notebook);
– corporate infidelity (think of the data breach caused by an internal person who, having the authorization to access the data, produces a copy for public distribution);
– misuse of data (think of the data breach caused by unauthorized access to computer systems with subsequent disclosure of the information acquired).

With the Provision of the Guarantor for the Protection of Personal Data concerning the implementation of the discipline on the communication of personal data breaches of April 4, 2013, was implemented the European Directive 2009/136/EC which amended, in part, the Directive 2002/58/EC on privacy in the electronic communications sector.

In this way, the Guarantor has introduced the obligation to notify the Authority (see art. 33 GDPR [16]) and users (see art. 34 GDPR [17]) in case of serious vio-

[15] The full interview with the Secretary General of the Garante per la protezione dei dati personali can be found at *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9303684.*

[16] Notification of a personal data breach to the supervisory authority: "*1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.*

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

lations following cyber attacks or adverse events that may lead to loss, destruction or undue disclosure of data.

In the regulatory silence, what are the measures to be put in place in order to prevent, manage and resolve episodes of loss and/or destruction of personal data?

Among the organizational measures to be provided for in the procedure, particular importance is given to the preventive classification of risks, distinguishing between an absent (which does not justify any notification to the Guarantor), present (which requires notification) and high (which also requires communication to the parties concerned) risk situation.

In fact, it is evident that, in the event of a violation, it is essential to be able to resort to a prior classification of the risk in order to take the necessary decisions within the prescribed time limits.

It is understood that this prior analysis will also have to take into account the specific elements of context (not a priori preventable).

---

3. The notification referred to in paragraph 1 shall at least: (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article".

[17] Communication of a personal data breach to the data subject: "*1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.*

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met".

The risks thus identified can be mitigated through appropriate countermeasures such as:

– legal obligations (the protection of privacy and data security are addressed both in laws having a general scope, such as, for example, the GDPR, and in laws and regulations having a specific character for a specific field [think of the matter of health data or judicial data]);
– the data security policy (as a document concerning the storage of data, both physical and digital, their transport, access modalities, responsibilities, and so on);
– the policy for the use of company equipment (as a document in which all issues relating to the use of the tools that an entity makes available to its employees and consultants are addressed);
– user authorisations (which must be strictly necessary for the operations to be carried out);
– the automation of processes (it was, in fact, found that human error is the first responsible for data breaches and is, normally, the product of a low culture of security, inaccurate, negligent and uncontrolled management of data);
– the promotion of security awareness;
– the use of encryption (where possible);
– tracking and monitoring (access to data and all functions performed on it must be tracked in real time and the logs produced must be kept accurately for the time required by law and internal regulations);
– backup of data (which allows recovery in case of destructive events);
– lastly, patch management (or the adaptation of software and operating systems when new vulnerabilities are detected).

This explains in detail what is the link between phenomena such as the data breach of the INPS [18] website and the Dutch app Covid19 Alert! [19]?

And what is the legal significance of such events?

Both events are symptoms of a strong criticality in the system, where obvious technical and cultural shortcomings make the fundamental rights of individuals even more vulnerable.

[18] On April 1, 2020, on the occasion of the possibility to access the INPS port in order to request and obtain the bonus of 600 euros, the Social Security Institute reported the dispersion of thousands of personal data of users, thus foreshadowing the first data breach during the health emergency by COVID-19.

[19] The application proposed by the Dutch government for the management of contact tracing, Covid19 Alert!, suffered a serious data leak of individuals who tested positive for the virus with the consequence that what were (or should have been) encrypted personal data were irreparably made public.

The absence of a right to guarantee the integrity and confidentiality of computer systems (as a corollary of the more general right to dignity), together with a clear disproportion between the aims pursued and the means used, how can the expectation of full protection of the right to technological and telematic confidentiality of one's own data be generated in individual users?

The violation of personal data represents, once again, a manifestation of the legislator's anxiety to keep up with such a changing reality as the contemporary one characterized by incessant technological progress.

4. Conclusions

Although there is no doubt that the attempt to protect, at least formally, the correct processing and custody of personal data is being made, a detailed and constantly updated regulatory framework is not, and probably will not be, sufficient to incorporate the new values of the economic and social context.

We conclude, therefore, by adopting the thought of Prof. Mantelero according to which: "*occorre che si radichi una cultura della "privacy", fondata sulla consapevolezza dell'importanza dei dati personali e, più in generale, su un maggior rispetto per l'individuo. È questo un processo lungo, in quanto incidente su aspetti valoriali, che può tuttavia essere agevolato da una chiara e coerente applicazione della legge da parte degli organi deputati a vigilare sull'attuazione della stessa e, soprattutto, da una divulgazione più lata possibile dei principi che ne sono a fondamento* [20]".

[20] A. Mantelero, *Il costo della privacy tra valore della persona e ragione d'impresa* (1nd edn, Giuffrè 2007) 84-85.