Data Protection and Covid 19: Individual Rights and Public Interests in the time of Coronavirus

[Kostanza Tomaino(*)]

Summary: 1. Introduction. – 2. Data protection Regulations. – 2.1 Processing data concerning health in the health context. – 3. Processing data in COVID-19 emercency. – 4. Conclusion.

1. In recent months, COVID-19 emergency has generated a series of conflicts between individual rights and public interests also in personal data protection rules. An example among the many is represented by the various problems related to the immune app. This conflicts born from the fact that today the collection and use of data, particularly the ones concerning health, are crucial tools for the law enforcement action against the pandemic.

And if privacy restrictions due to public health protection motifs are allowed by the GDPR, along with the Data Protection Code, in accordance with the proportionality, precaution and temporariness criteria, it is precisely in the framework of these principles that the provisions and above all the exceptions to the data protection system are read.

The problematic issue concerns the identification of the level at which the limitation of rights is allowed for the health protection.

In other words, how far can the conflict created beetween privacy and pubblic health can go?(1).

While it is crucial to make clear that data protection can in no way be an obstacle to save human lives, it is equally crucial to reaffirm that the exercise

(*) Università degli Studi di Perugia.

(1) Gruppo di lavoro ISS Bioetica Covid-19. *Protezione dei dati personali nell'emergenza COVID-19*, ver. 28 maggio 2020, Roma, Istituto Superiore di Sanità, 2020 (Rapporto ISS COVID-19 n. 42/2020).

of human rights, and notably the rights to privacy and to data protection are still applicable. Infact, in this times of pandemic crisis, it's important that we don't forget that data protection and privacy laws still apply.

As recently said by President of Italian data protection authority, data protection is «*diritto inquieto perché in costante dialettica con una tecnica mai eguale a se stessa, ma anche con i molteplici interessi, individuali e collettivi, che di volta in volta ne lambiscono i confini. Se, dunque, la sua funzione sociale è la forza più grande della protezione dati, mai come oggi essa si rivela indispensabile, rappresentando il punto di equilibrio tra libertà e tecnica, tra persona e società, il presupposto della tenuta della democrazia anche in circostanze eccezionali*»[2].

Now, it is more significant than ever to place privacy and data protection at the center of public issues[3].

Data protection principles always allow for balancing the interests at stake. General Data Protection Regulation (EU) 2016/679 sets forth high standards for the protection of personal data which are compatible and reconcilable with other fundamental rights and relevant public interests.

Instead, now is the time to break this line of thinking and promote the idea that it's not "public health or privacy", it's "public health and privacy"[4].

The principles enshrined in several international and national instruments cannot be suspended but only restricted in a lawful manner, and so for a defined limited duration.

This paper analyses the impact of pandemic may have on protection of the fundamental rights involved and the necessity of correct balance of rights in compliance with European legislation on personal data protection, in the attempt to provide some possible solutions for the processing of personal data during the emergency.

---

[2] A. Soro, *Tracciamento contagi coronavirus, ecco i criteri da seguire*, in *garanteprivacy.it*.

[3] Council of Europe, *Joint Statement on the right to data protection in the context of the COVID-19 pandemic* by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe Strasbourg, 30 March 2020.

[4] P. Balboni (2020), *«Public health and privacy» vs «Public health or privacy» in the time of the covid-19 pandemic*. Available: *maastrichtuniversity.nl/blog/2020*.

In this prospective, emerges the importance of the relationship between science and law for the protection of fundamental rights, in which law finds itseft having to follow scientific progress, regulating and orienting the new scientific and medical technologies in accordance with the universal values and criteria that consider the human being at the center of the technological revolution[5].

2. To understand the legal issues behind the collection and utilization, and more general the processing, of personal data in an emergency context, it is necessary to first analyze the legal framework with particular reference to the underlying ethical and biolegal principles.

As it's well known, the right to the protection of personal data is a fundamental individual right in accordance with the art. 8 of EU Charter[6] and art. 16 of TFUE[7] as well as with the Convention of Straburgo (hereinafter referred to as "Convention 108")[8].

At present, it's regulated, in particular, by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on

---

[5] A. Bompiani, A. Loreti Beghè, L. Marini, *Bioetica e diritti dell'uomo nella prospettiva del diritto internazionale e comunitario*, Torino, 2001, p. 44.

[6] Art 8, Charter of fundamental rights of the European Union «*Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority*».

[7] Art. 16, Treaty on the functioning of the European Union «*Everyone has the right to the protection of personal data concerning them. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union*».

[8] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg, 28 January 1981, n. 108.

the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) as well as by various other Italian and International regulatory acts and by Code of personal data protection as supplemented and amended by Decreto legislativo 10 agosto 2018, n. 101 on provisions to adjust national with General Data Protection Regulation (EU).

For the purposes of this Regulation "*personal data*" means any information relating to an identified or identifiable natural person *data subject*; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person[9].

The art. 5 foresees principles relating to processing of personal data.

These are: (a) lawfulness, fairness and transparency – *personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*; (b) purpose limitation – *personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes*; (c) data minimisation – *personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*; (d) accuracy – *personal data accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*; (e) storage limitation – *personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights*

[9] See art. 4, § 1 of GDPR.

and freedoms of the data subject; (f) integrity and confidentiality – *personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*; (g) accountability – *the controller shall be responsible for, and be able to demonstrate compliance with principles mentioned above*[10].

Concerning to lawfulness of processing, the regulation states any processing of personal data must be based on a valid legal basis. The legal basis of a processing operation is in a way the justification of the existence of the processing operation.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data: (a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose. (b) Contract: the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. (c) Legal obligation: the processing is necessary to comply with the law. (d) Vital interests: the processing is necessary to protect someone's life. (e) Public task: the processing is necessary to perform a task in the public interest or in the exercise of official functions, and the task or function has a clear basis in law. (f) Legitimate interests: the processing is necessary to legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Regarding the processing of special categories of personal data – among which are included data concerning health – in general shall be prohibited (art. 9, § 1 GDPR) unless there are one of the conditions indicated in § 2 of same article.

---

[10] Art. 24, § 1 GDPR «Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary».

2.1. The general prohibition of processing special categories of data, including health data, allows for some exceptions, which make the processing of such data lawful.

The conditions for processing special category data are an *explicit consent* of data subject(a)[11]; processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of *employment and social security and social protection* law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject (b); *vital interests* where the data subject is physically or legally incapable of giving consent (c); *not-for-profit bodies* when processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subject (d); *made public by the data subject* (e); in case of *legal claims or judicial acts* (f); with a basis in law the purposes referred to *reasons of substantial public interest* (g); *health or social care* (h); *public health* (i); *archiving – research and statistics* (j).

---

[11] According to art. 7 GDPR, «Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract».

It is therefore evident that the exceptions of these conditions are referred to g) *Reasons of substantial public interest* on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; h) *Health or social care* for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional; i) *Public health* such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy[(12)].

Essential processing for specific purposes related to health care and carried out by a health professional subject to the obligation of professional secrecy (or other person subject to the obligation of secrecy), do not require the consent of the data subject.

According to principle of transparency [art. 5, § 1, lett. *a)*] the controller shall take appropriate measures to provide any information and communication under relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language,

---

[(12)] See also Recital n. 54: «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».

in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

When the storage period is not provided under specific rules, in addition to these information, the controller shall, at the time when personal data are obtained, provide the data subject with the information necessary to ensure fair and transparent processing the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.

For public bodies, the records of processing activities and the designation of a Data Protection Officer also and especially in the case of large-scale processing are mandatory.

As indicated by guidelines on Data Protection Officers adopted on 13 December 2016 as last revised and adopted on 5 April 2017, data processing of patients within a private hospital, nursing home or any extended care unit has also to be considered as large-scale data processing[13].

3. In the health emergency situation, such as the current one, the data processing activity falls within the hypothesis under art. 9, § 2, lett. *i)* of the GDPR, which, as seen in the previous paragraph, allows exceptions to the general prohibition of processing particular categories of data when *processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.*

In addition, it is important to specify that, as in other matters, the management of personal data has been the subject of several regulatory measures that

[13] Article 29 Data Protection Working Party, *Guidelines on Data Protection Officers ('DPOs')*, Brussels, on 13 December 2016 as last revised and adopted on 5 April 2017, in *De Jure*.

has led to the adoption of emergency measures that have either established revisions of former determinations, or provided de novo rules or guidelines for other circumstances in this continuously evolving scenario. In particolar, as far as this is concerned, it is worth nothing that ruling the ordinanza by the Chief of Civil Protection Department (O.C.D.P.C.) n. 630, on February 3, 2020, in conformity with the indications from the Data Protection Authority[14], has established that «*nell'ambito dell'attuazione delle attività di protezione civile connesse allo svolgimento delle attività di cui alla presente ordinanza, allo scopo di assicurare la più efficace gestione dei flussi e dell'interscambio di dati personali, i soggetti operanti nel Servizio nazionale di protezione civile di cui agli articoli 4 e 13 del decreto legislativo 2 gennaio 2018, n. 1, nonché quelli individuati ai sensi dell'art. 1 della presente ordinanza, possono realizzare trattamenti, ivi compresa la comunicazione tra loro, dei dati personali, anche relativi agli articoli 9 e 10 del regolamento del Parlamento europeo 27 aprile 2016, n. 2016/679/UE, necessari per l'espletamento della funzione di protezione civile al ricorrere dei casi di cui agli articoli 23, comma 1 e 24, comma 1, del decreto legislativo 2 gennaio 2018, n. 1, fino al 30 luglio 2020. 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 del Parlamento europeo 27 aprile 2016, n. 2016/679/UE è effettuata, nei casi in cui essa risulti indispensabile, ai fini dello svolgimento delle attività di cui alla presente ordinanza. 3. Il trattamento dei dati di cui ai commi 1 e 2 è effettuato nel rispetto dei principi di cui all'art. 5 del citato regolamento n. 2016/679/UE, adottando misure appropriate a tutela dei diritti e delle libertà degli interessati. 4. In relazione al contesto emergenziale in atto, nonché' avuto riguardo all'esigenza di contemperare la funzione di soccorso con quella afferente alla salvaguardia della riservatezza degli interessati, i soggetti di cui al comma 1 conferiscono le autorizzazioni di cui all'art. 2-quaterdecies, del decreto legislativo 30 giugno 2003, n. 196, con modalità semplificate, ed anche oralmente*»[15].

---

[14] Garante per la Protezione dei Dati Personali, Provvedimento n. 15 del 2020, *Parere sulla bozza di ordinanza recante disposizioni urgenti di protezione civile in relazione all'emergenza sul territorio nazionale relativo al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili*, 2 febbraio 2020.

[15] Art. 5, O.C.D.P.C. n. 630, 3 February 2020, *Primi interventi urgenti di protezione civile in relazione all'emergenza relativa al rischio sanitario connesso all'insorgenza di patologie derivanti da agenti virali trasmissibili*, G.U. n. 32, 8 February 2020.

Subsequently, this ruling has been first included in the art. 14 of the DL 4/2020 and then, after abrogation of the DL 14/2020 by the art. 1, co. 2, L. 27/2020 - converted to DL 18/2020, with some modifications - in the art. 17-bis of DL 18/2020 known as "decreto cura Italia".

Therefore, the art. 17 of the DL 18/2020 (as converted in the L. 27/2020) contains specific measures regarding the management of personal data (effective until the end of the present emergency state). In particular, it rules that«*1. Fino al termine dello stato di emergenza deliberato dal Consiglio dei ministri in data 31 gennaio 2020, per motivi di 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 codice di cui al decreto legislativo 30 giugno 2003, n. 196, i soggetti operanti nel Servizio nazionale della protezione civile, di cui agli articoli 4 e 13 del codice di cui al decreto legislativo 2 gennaio 2018, n. 1, e i soggetti attuatori di cui all'articolo 1 dell'ordinanza del Capo del Dipartimento della protezione civile n. 630 del 3 febbraio 2020, 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 2 del decreto-legge 25 marzo 2020, n. 19, 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 ad essi attribuite 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 citato regolamento (UE) 2016/679, sono effettuate nei casi in cui risultino indispensabili 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 mi-*

sure 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 codice di cui al 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 citato regolamento (UE) 2016/679, fermo restando quanto disposto dall'articolo 82 del codice di cui al decreto legislativo 30 giugno 2003, n. 196, i soggetti di cui al comma 1 del presente articolo possono omettere l'informativa di cui all'articolo 13 del medesimo regolamento o fornire un'informativa semplificata, previa comunicazione orale agli interessati dalla 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».

Therefore, it is evident that, as far as the health control is concerned, the healthy units and health workers, like the prefectures and municipalities, are not allowed to disclose the names of positive subjects or of those in fiduciary isolation, whether or not the ultimate end is to restrain spreading of the epidemics. In this regard, the Italian Data Protection Authority has stated that «*All health professionals may collect the information they consider necessary as part of the care of their patients, including information linked to the presence of symptoms due to COVID-19. This is without prejudice to the detection and collection of information on Coronavirus symptoms and of the information on the recent movements of each individual, which rest with healthcare professionals and the civil protection system, respectively, being the bodies responsible for ensuring compliance with the public health rules that were recently adopted. […] the public healthcare professional is required to trace back the close contacts of an individual tested positive to COVID-19 in order to determine the most appropriate containment measures*»[16].

The same measure has contributed to the definition of urgent guidelines in the menagement of research activity and clinical sperimentation during

[16] Garante per la Protezione dei Dati Personali, *FAQs – Data processing in health care in the context of the health emergency*, available: *garanteprivacy.it*.

health emergency by ruling that «*ferme restando le disposizioni vigenti in materia di sperimentazione clinica dei medicinali e dei dispositivi medici, al fine di migliorare la capacità di coordinamento e di analisi delle evidenze scientifiche disponibili, è affidata ad AIFA, la possibilità di accedere a tutti i dati degli studi sperimentali e degli usi compassionevoli di cui al comma 2. 2. I dati delle sperimentazioni di cui al comma 1 riguardano esclusivamente gli studi sperimentali e gli usi compassionevoli dei medicinali, per pazienti con COVID-19. I protocolli di studio sono preliminarmente valutati dalla Commissione tecnico scientifica (CTS) dell'AIFA, che ne comunica gli esiti anche al Comitato tecnico scientifico dell'Unità di crisi del Dipartimento della Protezione civile*»[17].

The Italian Data Protection Authority has also provided conclusive statements in this specific context. In particular «*Sponsors and testing centres may process personal data, also concerning the health of COVID-19 patients, to carry out clinical trials of medicinal products (such as investigational clinical studies on medicinal products, phase I, II, III and IV, observational studies on medicinal products and compassionate therapeutic use programmes), insofar as they are strictly necessary to combat and study the ongoing pandemic, on the basis of the data subjects' consent or by relying on another legal basis pursuant to Article 9 (2) of the Regulation, in accordance with Union or national law, for reasons of significant public interest, for reasons of public interest in the area of public health and for the purposes of scientific research (Article 9 (2), letters (a), (g), (i) and (j) of the Regulation). When, on account of particular and substantiated reasons, informing the data subjects proves impossible or involves a disproportionate effort or is likely to seriously impair the achievement of the objectives of the research, and it is therefore not possible to acquire the data subjects' consent for the processing of their personal data, the controllers are required, where possible, to obtain such consent, after providing the appropriate information, from the persons who have legal authority over those data subjects, or from a close relative, a member of their family, a cohabitee or, in the absence thereof, the manager of the facility where the data subject is staying. This is based on an analogy with the provisions of point 4.11.2 of the requirements relating to the processing of genetic data. Where, for specific and substantiated reasons, it is not possible to obtain informed consent for the processing of personal data, also from third parties, or*

[17] Art. 17 DL 17 March 2020, n. 18 as converted in the L. 24 aprile 2020, n. 27, *Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19*, G.U. n. 253, 13 October 2020.

where doing so risks seriously undermining the successful outcome of the research – e.g. when processing data relating to deceased patients or patients in intensive care units –, the data controllers intending to process personal data exclusively in connection with clinical trials and the compassionate use of medicinal products for human use with a view to the treatment and prevention of COVID-19 are not required, under the legislation relating to the current emergency situation, to submit their research project and the associated impact assessment for the prior consultation of the Garante as referred to in Section 110 of the Italian data protection Code»[18].

It is worth mentioning that the European Data Protection Board has adopted on April 21st 2020 the Guidelines 03/2020 related to the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak. These guidelines clearly state that the GDPR has already ruled about the treatment of health data for scientific research purposes, and this ruling is applicable even in the actual pandemic context. The document also states that it is nevertheless necessary to respect the principles declared in the art. 5 of the GDPR, i.e., art. 6 ruling on the lowfulness, and art. 9 dealing about particular categories of data as well as the entire part V of GDPR relative to the data transfer process. In particular, the art. 45 rules that transfer of the data is allowed in conditions in which the Commission has decided that the third-party country, or parts thereof, or an International agency warrant a strong enough level of protection.

Likewise, at workplaces specific measures have been released by the competent authorities: among others, it has been established that employers meet all the necessary requirements publicly issued so as to restrain viral diffusion. Also, as related to working by employers, a number of regulatory measures and subsequent guidance documents were adopted in the first place by the competent authorities in order to set out urgent measures for the containment and management of the epidemiological emergency. Accordingly, it has been determined that an employer whose activities are not suspended is required to comply with the measures for the containment and management

[18] Garante per la Protezione dei Dati Personali, *FAQs – Data processing in clinical trials and medical research in the context of the COVID-19 health emergency*, available: *garanteprivacy.it*.

of the epidemiological emergency as described in the in the *Protocollo condiviso di regolamentazione delle misure per il contrasto e il contenimento della diffusione del virus COVID-19 negli ambienti di lavoro tra Governo e parti sociali del 14 marzo 2020 così come integrato il 24 aprile 2020*[19]. In particular, the aforementioned document envisages measurment of the body temperature of employees for access to the premises of the organisation as part of the measures to combat the spread of the virus, which also apply to users, visitors and customers as well as to suppliers – where a separate access mode has not been envisaged for the latter. Since the measurment of the body temperature in real time, when associated with the data subject's identity, is an instance of processing of personal data (Article 4(1), No (2), of Regulation (EU) 2016/679), it is not permitted to record the data relating to the body temperature found; conversely, it is permitted to record the fact that the threshold set out in the law is exceeded, and recording is also permitted whenever it is necessary to document the reasons for refusing access to the workplace - in compliance with the principle of 'data minimisation' (Article 5(1)(c) of the Regulation). By contrast, where the body temperature is checked in customers (for example, in large department stores) or occasional visitors, it is not, as a rule, necessary to record the information on ground of refusal access even if the temperature is above the threshold indicated in the emergency legislation. Under the legislation on the protection of health and safety at work, the employee has a specific obligation to inform the employer of any situation of danger to health and safety at the workplace[20]. In this connection, it has

[19] All. 12, d.P.C.M. 13 ottobre 2020, *Ulteriori disposizioni attuative del decreto-legge 25 marzo 2020, n. 19, convertito, con modificazioni, dalla legge 25 maggio 2020, n. 35, recante «Misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19», e del decreto-legge 16 maggio 2020, n. 33, convertito, con modificazioni, dalla legge 14 luglio 2020, n. 74, recante «Ulteriori misure urgenti per fronteggiare l'emergenza epidemiologica da COVID-19»*, G.U. n. 253, 13 October 2020.

[20] See in particular art. 20 T.U.S.L., G.U. n. 180, 5 August 2009: «Ogni lavoratore deve prendersi cura della propria salute e sicurezza e di quella delle altre persone presenti sul luogo di lavoro, su cui ricadono gli effetti delle sue azioni o omissioni, conformemente alla sua formazione, alle istruzioni e ai mezzi forniti dal datore di lavoro. I lavoratori devono in particolare: a) contribuire, insieme al datore di lavoro, ai dirigenti e ai preposti, all'adempimento degli obblighi previsti a tutela della salute e sicurezza sui luoghi di lavoro;

been specified that a civil servant and persons who work in whatever capacity in the public administration are bound to report that they come from or have been in contact with persons coming from a risk area. Within this framework, the employer may invite employees to do so, where necessary, through dedicated channels. Among the measures to prevent and contain transmission employers are required to act based on the existing regulatory framework, that is the prohibition to access the workplace applying to those who have been in contact with COVID-19-positive individuals over the past 14 days or come from risk areas according to WHO indications. To this end, also in the light of the provisions adopted subsequently for the containment of transmission, a declaration regarding the above circumstances may also be requested from third parties such as visitors and users. In any case, only the necessary, adequate and relevant data will have to be collected in relation to the prevention of the transmission without requesting additional information about the COVID-19-positive person, the specific places visited or other details relating to that person's private sphere.

---

b) osservare le disposizioni e le istruzioni impartite dal datore di lavoro, dai dirigenti e dai preposti, ai fini della protezione collettiva ed individuale; c) utilizzare correttamente le attrezzature di lavoro, le sostanze e le miscele pericolose, i mezzi di trasporto, nonché i dispositivi di sicurezza; d) utilizzare in modo appropriato i dispositivi di protezione messi a loro disposizione; e) segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi di cui alle lettere c) e d), nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla lettera f) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza; f) non rimuovere o modificare senza autorizzazione i dispositivi di sicurezza o di segnalazione o di controllo; g) non compiere di propria iniziativa operazioni o manovre che non sono di loro competenza ovvero che possono compromettere la sicurezza propria o di altri lavoratori; h) partecipare ai programmi di formazione e di addestramento organizzati dal datore di lavoro; i) sottoporsi ai controlli sanitari previsti dal presente decreto legislativo o comunque disposti dal medico competente. I lavoratori di aziende che svolgono attività in regime di appalto o subappalto, devono esporre apposita tessera di riconoscimento, corredata di fotografia, contenente le generalità del lavoratore e l'indicazione del datore di lavoro. Tale obbligo grava anche in capo ai lavoratori autonomi che esercitano direttamente la propria attività nel medesimo luogo di lavoro, i quali sono tenuti a provvedervi per proprio conto».

With specific reference to the utilization of the personal information regarding contact tracing, this issued has been regulated by a subsequent regulatory action, i.e, by a decree ("decreto-legge" 30 aprile 2020, n. 28). This action consists of the creation of a national COVID alert system network, which is usually referred to as contact tracing, stating that «*Al solo fine di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza COVID-19, è istituita una piattaforma unica nazionale per la gestione del sistema di allerta dei soggetti che, a tal fine, hanno installato, su base volontaria, un'apposita applicazione sui dispositivi di telefonia mobile. Il Ministero della salute, in qualità di titolare del trattamento, si coordina, sentito il Ministro per gli affari regionali e le autonomie, anche ai sensi dell'articolo 28 del Regolamento (UE) 2016/679, con i soggetti operanti nel Servizio nazionale della protezione civile, di cui agli articoli 4 e 13 del decreto legislativo 2 gennaio 2018, n. 1, e con i soggetti attuatori di cui all'articolo 1 dell'ordinanza del Capo del Dipartimento della protezione civile n. 630 del 3 febbraio 2020, nonché con l'Istituto superiore di sanità e, anche per il tramite del Sistema Tessera Sanitaria, con le strutture pubbliche e private accreditate che operano nell'ambito del Servizio sanitario nazionale, nel rispetto delle relative competenze istituzionali in materia sanitaria connessa all'emergenza epidemiologica da COVID 19, per gli ulteriori adempimenti necessari alla gestione del sistema di allerta e per l'adozione di correlate misure di sanità pubblica e di cura. Le modalità operative del sistema di allerta tramite la piattaforma informatica di cui al presente comma sono complementari alle ordinarie modalità in uso nell'ambito del Servizio sanitario nazionale. Il Ministro della salute e il Ministro per gli affari regionali e le autonomie informano periodicamente la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano sullo stato di avanzamento del progetto*»[21].

[21] Art. 6, § 1, d.l. 30 April 2020, n. 28 as converted in the 25 June 2020, n. 70 (*Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19*), G.U. n. 162, 29 June 2020.

4. As per what epitomized above, it is clear that, in the face of the data collection system, individual privacy is preserved as detailed in the GDPR. This is due to the fact that, subregulatory measures should not be in conflict with higher order rights. In summary, the final scenario is that, although public health measures are a reason for derogation to the benefit of large scale communities, the primary objective of preserving privacy has not been derogated in general. This has been reached by a series of soft-law[22] measures that do not result in mandatory actions, yet suggest ways to combine opposing needs such as those posed by public health issues and individual rights as related to preservation of a person's health related information[23].

On the basis of the above-mentioned premises, it is clear that right and science are tightly interconnected. The language of science has to be clear and capable of decoding scientific discoveries and issues to legal professions. In so doing, the language of science needs to adopt elements of precision and accuracy of the legal language whereas the right needs to adopt a more general view of the different issues being examined.

To contrast the episodes of discrimination and hunting for COVID-19 infectors, reminiscent of the episodes of the plague in Milan as described by Manzoni[24], neither fear nor the indiscriminative processing of personal data are required but low and respect of the fundamental rights. In there, we can find the solution that legitimizes the use of new technologies to prevent and oppose the pandemic according with the principles of minimisation and limitation.

Infact, the EDPB also underlined that that one should not have to choose between an efficient response to the current crisis and the protection of our fundamental rights: we can achieve both, and moreover data protection principles can play a very important role in the fight against

---

[22] For a definition see: R.J. Dupuy, *The Protection of the Environment and International Law*, Hagu Accademy, Leiden, 1975, pp. 623-627.

[23] B. Pastore, *Soft Law, gradi di normatività, teoria delle fonti*, in *Lavoro e dir.*, 2003, p. 5 ss.

[24] F.P. Micozzi, *Le tecnologie, la protezione dei dati e l'emergenza Coronavirus: rapporto tra il possibile e il legalmente consentito*, in *BioLaw Journal*, Special Issue n. 1, 2020, p. 624.

the virus. European data protection law allows for the responsible use of personal data for health management purposes, while also ensuring that individual rights and freedoms are not eroded in the process [25].

On 7 April 2020 the Concil of Europe has send an information document to provided governments with a toolkit for dealing with the present unprecedented and massive scale sanitary crisis in a way that respects the fundamental values of democracy, rule of law and human rights [26]. In particular in this document it remembered that the respect for the rule of law and democratic principles in times of emergency: principle of legality, limited duration of the regime of the state of emergency and of the emergency measures, principle of necessity, the distribution of powers and checks on the executive action during the state of emergency regime, relevant human rights standards (right to life, right of right of access to health care and privacy and data protection). In particular, about data protection it said that *the new technologies of access to – and the processing of – personal data have the potential to contain and remedy the pandemic. Monitoring, tracking and anticipating are crucial steps of an epidemic surveillance. With the multiplication and over-abundance of available sophisticated digital technologies and tools (geolocation data, artificial intelligence, facial recognition, social media applications) such pandemic surveillance could be facilitated.*

At the same time, the intrusive potential of modern technologies must not be left unchecked and unbalanced against the need for respect for private life. Data protection principles and the Council of Europe Convention 108 (and its modernised version, referred to as "Convention 108+"28) have always allowed a balancing of high protective standards and public interests, including public health. The Convention allows for exceptions to ordinary data-protection rules, for a limited period of time and with appropriate safeguards (eg anonymisation) and an effective oversight framework to make sure that these data are collected, analysed, stored and shared in legitimate and responsible ways. Large-scale processing of personal data by means of artificial intelligence should only be

[25] EDPB, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, Adopted on 21 April 2020.

[26] COE, Information Documents SG/Inf(2020)11, *Respecting democracy, rule of law and human rights in the framework of the COVID-19 sanitary crisis. A toolkit for member states*, 7 April 2020.

performed when the scientific evidence convincingly shows that the potential public health benefits override the benefits of alternative, less intrusive solutions.

In conclusion, ideally, the processing of personal data to counteract the pandemia should balance the achievement of human benefits with the protection of fundamental human rights, such as equality, respect for human dignity and equal opportunities.