The Protection of Personal Data Concerning Health at the European Level

A Comparative Analysis

Editor

GUERINO FARES

IUSTITIAM COLIMUS

G. Giappichelli Torino

eleven international publishing

ISBN 978-94-6236-188-1

http://www.elevenpub.com

ISBN/EAN 978-88-921-3715-8

http://www.giappichelli.it

Sold and distributed
by Eleven International Publishing

P.O. Box 85576
2508 CG The Hague
The Netherlands
Tel.: +31 70 33 070 33
Fax: +31 70 33 070 30
e-mail: sales@elevenpub.nl
www.elevenpub.com

Sold and distributed in USA and Canada

Independent Publishers Group
814 N. Franklin street
Chicago, IL 60610, USA
Order Placement: +1 800 888 4741
Fax: + 1 312 337 5983
orders@ipgbook.com
www.ipgbook.com

Eleven International Publishing is an imprint of Boom uitgevers Den Haag.

Printed by Rotolito S.p.A. - Pioltello, Milano (Italy)

The processing of personal data concerning health according to the EU Regulation

Guerino Fares [*]

CONTENT: 1. Personal data concerning health and EU Law: the general framework. – 2. Conditions justifying the processing of personal data concerning health: Art. 9 of GDPR. – 3. Specific issues in the case law interpretation: omission of processing. – 4. Processing performed in the absence of legal basis. – 5. Artificial intelligence and data protection: learning from the Covid-19 experience.

1. *Personal data concerning health and EU Law: the general framework*

A particularly delicate context underlies the subject of personal data concerning health given the values involved and the relationship between patients, professionals and healthcare facilities that characterise it.

The legal, technological and social evolution has largely generated interest in this relationship, as well as in the intimate relation between patients and their health.

The change in the cultural perspective and the legal paradigm can be perceived in several sectors, of which at least three should be reported.

1. The new awareness of citizens with regard to their health needs, which is expressed by a longer life expectancy and claims for new care and better and more modern treatments: in fact, the choice made by many legislators (also at the constitutional level, see, for example, Art. 117 of the Italian Constitution) to not only provide minimum levels of healthcare but also more extended services than those that are basic is motivated by citizen's aspiration for demanding and obtaining something more than the minimum level. The latter implies ser-

[*] Full Professor of Constitutional Law. Associate Professor of Public Law at Roma 3 University. Lecturer of Health-Pharmaceutical Law and Administrative Law in the same University. Italian representative at the European Network on Health, Law & Bioethics (HeaLab EuroNet). Scientific Director of Ius & Law Journal.

vices appropriate to protect patient's dignity, while essential levels of such healthcare means something more in accordance with the regulator's willingness.

2. The diverse individual and social awareness of the system of responsibilities. The latter no longer involves just the healthcare operator but also the facility where professionals work, within a legislative framework that enhances more than before the standardisation of best practices and the prevention and management arrangements of the clinical risk.

3. The use of innovative diagnostic and surgical methodologies (telemedicine, medical app, robotic surgery, etc.), on the one hand, and the introduction and spread of tools for information collection and processing on digital media (e-health: electronic clinical record, electronic health record, paperless prescriptions, etc.), on the other hand, which impact the arrangements for personal data protection and the delivery of informed consent forms by the data subject.

In the legal analysis, when health encounters confidentiality, it gives rise to a cluster of supreme constitutional values and to a summation of absolute rights that could be described in terms of the 'health law of privacy': the result is a legislative sub-system, somehow interested by the three new elements presented above, that is called upon to find a balance between the values of the protection of health and the protection of personal data.

This dual set of values, gathered in the same field, should therefore aim towards balance and standardisation. Similarly, this is an occasion for the relevant, mutually influencing mechanisms of action and conceptual and terminological structures to update and increase the overall level of protection of privacy.

Such a structure of values and interests is required to face the most advanced boundaries of law and technology; in order to be effectively met, we need to begin from a concept of strengthened centrality of the patient.

At this point, the notion of 'patient empowerment' is relevant. It is used in medical literature to indicate 'a philosophy of health care that proceeds from the perspective that optimal outcomes of health care interventions are achieved when patients become active participants in the health care process. Under a patient empowerment philosophy, patients and clinicians jointly set goals, select interventions, and assess outcomes according to mutually-defined parameters. Employing patient empowerment as an information systems design philosophy leads to creation of computerized information resources, management systems and telehealth innovations in a manner that insures patients' abilities to participate as full partners in health care'. [1]

As someone underlined, this notion '[express a conceptual and organizational choice that puts the patients at the center of the care system and process,

[1] P. Brennan, C. Safran, 'Report of conference track 3: patient empowerment', in *International Journal of Medical Informatics* (2003) 69 (2-3) 301.

as the fundamental actors aware of the medical choices of which they are protagonists]'. [2]

From the perspective of our investigation, we can support the hypothesis of a transition from 'patient empowerment' to 'patient and data subject empowerment': an extension of the horizon that is useful to understand how the two core concepts go side-by-side in a logic of circular balancing of the personal rights.

A further step consists of analysing the approach of the Regulation EU 2016/679 (so-called GDPR) with respect to what we have defined as the health law of privacy, also known as the framework in the health field for processing personal data concerning health.

A necessary preliminary remark is linked to the definitional level: what do we mean, or should we mean, by data concerning health?

In the first European legislation on the subject, introduced by the so-called Strasbourg Convention, the essential elements of the definition are clear: [3] a) medical data represents a special category of data; b) its automatic processing is usually prohibited; c) its processing is allowed only under a domestic law providing appropriate safeguards for the purpose.

The prohibition of processing this kind of data is confirmed in the so-called Directive on *privacy*. [4]

On the content level, the Convention referred to 'personal data concerning state of health', while the Directive mentions this as 'data concerning health'.

Since health is a person's status or a human condition, it is obvious that the difference is slight.

In contrast, the common elements of the two texts are clear: (i) the relational connotation of the medical data (it is 'concerning' health, meaning that it relates to health) and (ii) the lack of a specific and more detailed definition.

Therefore, the choice made by the Italian state legislature with the privacy code [5] seems more innovative, since, on the one side, this specific (or 'special', as more recently defined by the GDPR) category of personal data [6] is signifi-

---

[2] P. Guarda, 'I dati sanitari', in V. Cuffaro, R. D'Orazio and V. Ricciuto (eds.) *I dati personali nel diritto europeo* (2019) 592.

[3] Art. 6, Convention of Strasbourg of 28 January 1981 no. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, entered into force on 1 October 1985.

[4] Art. 8, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

[5] Art. 4, para 2, lett. *e*), D.Lgs. 30 June 2003 no. 196, including personal data capable of revealing racial or ethnic origin; religious, philosophical or other beliefs; political opinions; and membership in political parties, trade-unions, associations or organizations with a religious, philosophical, political or trade-union character, as well as personal data capable of revealing health status and sexual life.

[6] The expression 'sensitive data' – or, according to some terminological variants, 'super-sensitive' or 'very sensitive' – appropriately testifies: a) the severity of precautionary and protective measures that

cantly labelled as 'sensitive'; and, on the other side, this data is identified as the information capable of revealing health status.

The conceptual nuance between a datum concerning health and a datum capable of revealing health status seems to be detectable in higher flexibility and elasticity of the second wording: information that (more or less tightly) concerns health evokes an area more restricted than information potentially revealing (in a broad sense and also in a mediated way) psycho-physical conditions of the individual. [7]

The mentioned GDPR takes a further step forward by introducing an even more mature definition in which personal data regarding physical or mental health of a natural person, including the provision of healthcare services, that reveals information concerning health status has a substantial health character. [8]

The scope of *data concerning health*, so redefined, confirms the tendency toward the extension of the concept while also resolving a set of interpretive uncertainties that had arisen over time because of the previous and more tentative formulation.

For a long time, debates had taken place about, for example, whether the expression 'data concerning health' alludes to any information in any way regarding the psycho-physical conditions of the data subject or only to information revealing pathological statuses or, however directly, immediately and expressly connected to the health of the data subject. [9]

Similarly, it has been debated whether only the information about the current health status, or even the information regarding the clinical history of the patient and past medical events, [10] were worthy of consideration from the perspective of the regulatory regime on *privacy*.

Although issues related to the interpretations of regulations never terminate completely, one of the commentators on the GDPR positively evaluated it as the first unfailing reference point, capable of providing '[a surely clearer defi-

---

have to be met by the processors of this type of information, assuming correlated technical and legal obligations; b) the intimate and very delicate nature of the values concerned and, especially, the extent and seriousness of the damage to the individual in the case of illegal processing.

[7] An example is the choice of a certain diet (that can mean special health statuses like, for example, diabetes or celiac disease) or of a particularly isolated location for a vacation period (that can be required for a psycho-physical stress condition).

[8] Art. 4, para 1, no. 15, of GDPR.

[9] See Recommendation (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data, adopted by the Committee of Ministers on 13 February 1997.

[10] For the broad view, Garante per la protezione dei dati personali, *Autorizzazione n. 2/2000 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale*, 20 September 2000, [doc. web no. 1151469]. *Recital* 35 of GDPR has, then, settled any discussion by referring to the 'past, current or future physical or mental health status of the data subject'.

nition, finally shared at European level, at least for what concerns the terminological expression]'. [11]

From the perspective of analysis for this study, the definition aspect can be closed as follows.

On the one hand, by acknowledging that the European Regulation, notwithstanding the definite listing of 'special' categories of data (i.e., the so-called 'sensitive' data), has traditionally included data concerning health, although envisaging a notion more comprehensive than in the past.

On the other hand, by recognising that such personal data is not suitable for exhaustive explanations valid for any possible case of application of the subject legislation because it is not possible to compress it within strict factual content limits that cannot be crossed: therefore, any investigation on the nature of the datum cannot disregard the context in which data is processed, the subjects allowed to process it and the purposes of processing. [12]

The 'health law of privacy' finds its core of statutes in Art. 9, para 2, of GDPR and, especially, in lett. h) and i).

In particular, it is about the processing necessary for the purposes of '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' (lett. h); or the processing necessary for reasons of public interest in the area of public health, including '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' (lett. i).

Obviously, caution should be observed. In the first case, personal data may be processed 'by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies' (Art. 9, para 3). In the second case, data should be processed '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' (lett. i)).

---

[11] P. Guarda (2) 597, for whom in the new formulation '[information collected during the recording or the healthcare services provision…]' can be considered included.

[12] In various ways, the following authors have expressed their opinion in favour of the enhancement of the context and the related minimisation of the importance of data content: G. Buttarelli, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione* (Giuffrè 1997) 391; A. Ciatti, 'La protezione dei dati idonei a rivelare lo stato di salute nella legge n. 67/1996', in *Contr. Impr. Europa* (1998) 368; V. Zambrano, 'Art. 75' in S. Sica, P. Stanzione (eds.), *La nuova disciplina della privacy* (2004) 305 et seq.

The assessment of the relations between data processing, on the one hand, and the safeguards for the rights of the data subject receiving health care, on the other, is the central subject of this work, built on the main perspective of informed consent.

However, the subject shall not be so exhausted.

An object of interest for the writer is, or could be, the processing for the purpose of scientific research, in our case, of medical and biomedical type under lett. j), which is allowed if it is proportioned to the aim pursued, respectful of the essence of the right to data protection and incorporating suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Furthermore, data processing for these particular purposes requires, under Art. 89 of GDPR, that appropriate safeguards are given for rights and freedoms of the data subject in terms of technical and organisational measures and notwithstanding the faculty to introduce derogations where such rights are likely to render impossible or seriously impair the achievement of the specific purposes, provided that such derogations are necessary to achieve the aforementioned purposes.

Beyond the mentioned processing for the purposes of preventive or occupational medicine, including the frequent disputes between employers and employees, for our aims, there is also the processing of genetic data and, more generally, the processing necessary to establish, exercise or defend legal claims (lett. f), the extent of which allows us to better frame the context in which we move.

Still from a general perspective, the analysis of the domestic and supranational case law on access to sensitive data is useful to frame the subject matter, followed by a specific deepening of cases that, especially thanks to European jurisdictional authorities, provide for a set of insights very precious in order to focus on the coordinates of the system and the complexity and delicacy of critical points distinguishing it.

A careful investigation of all aforementioned research profiles can allow a more mature and aware discussion on medical data in the system of fundamental rights: that is, on data concerning health processed for the purposes of care, diagnosis and treatment.

As we will see in the following paragraphs, the approach followed by the GDPR seems to be characterised by three essential elements:

1. the prohibition, as a general rule, of processing data concerning health (Art. 9, para 1: Processing [...] shall be prohibited ...) in line with the approach followed by Directive 95/46/EC (Art. 8, para 1: Member States shall prohibit the processing ...);

2. the preference for rules more of principle than of detail and, consequently, of a regulation more condensed in the *Recitals* (and, therefore, in the 'pre-

mises of the matter' that express orientations and auspices) than in articles that have a higher binding power;

3. the choice of leaving the application arrangements to the arbitrary decision of Member States that establish the extent of adaptation of their national regulations to the new European rules; thus, the Regulation renounces a unitary and unifying logic (in this sense, Art. 9, para 4 is emblematic for all the others; according to it, Member States can keep or introduce further conditions, including limitations, regarding the processing of genetic data, biometric data or data concerning health).

Among the others, reading *Recitals* 45, 52, 53 and 54 is essential if we want to fully reconstruct the willingness of the European legislature: which, after having suggested 'harmonized conditions for the processing of special categories of personal data concerning health in respect of specific needs' (*Recital* 53), acknowledges that '[t]he 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' (*Recital* 54). The latter has been interpreted according to the definition of the Regulation (EC) 1338/2008 of the European Parliament and of the Council.

Both the legitimacy conditions for processing in derogation and the relevant security measures to be adopted are, in any case, equally well defined. In accordance with *Recital* 52, 'a derogation from the prohibition on processing special categories of personal data may be made for health purposes, including public health and the management of health-care', also when provided for in Union or Member State law and subject to suitable safeguards.

Lastly, *Recital* 45 adds 'it should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association'.

2. *Conditions justifying the processing of personal data concerning health: Art. 9 of GDPR*

As seen, 'data concerning health' is defined by Art. 4, no. 15, of GDPR: 'personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status'.

Such notion is more extensively developed in *Recital* 35 of the GDPR. 'Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (1) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; [13] and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test'.

The notion adopted by the European Regulation provides for a greater breadth of the forerunner expression 'medical datum', originally used in Recommendation No. R (81) 1 of 23 January 1981 on regulations for automated medical data banks (then replaced by Recommendation No. R (97) 5 of 13 February 1997 on the Protection of Medical data).

It is an evolution linked to the change of the concept of health, transposed also at the international level, meant as a state of complete physical and mental wellbeing and no longer merely as the absence of diseases and preservation and possible recovery of the health status (as readable in the preamble of the Constitution of the World Health Organization).

Therefore, the boundaries of the datum concerning health include not only information regarding diseases or other pathology statuses but also any other information concerning the physical, mental and relational status of the individual, including pre-existing and potential health statuses, as well as the details of clinical and treatment paths followed or undergone.

Furthermore, the new frontiers of the medical datum go jointly with the technological evolution of medical sciences (a phenomenon known as digital health) [14] and the increased economic value that this kind of data has acquired.

The regulatory framework on the protection of medical data shows a feature of specialisation in respect to the whole body of provisions concerning so-called ordinary and common personal data. Such specialisation is linked to the

---

[13] *See* M. Shabani, P. Borry, 'Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation', in *European Journal of Human Genetics* (2018) 149.

[14] The implementation of various eHealth and telehealth options has enhanced access to care, including in patients' own homes. European Commission, *State of Health in the EU. Companion Report 2019* (Luxembourg 2019) in <*ec.europa.eu/health/state*> 60 accessed on 09.10.2020.

particular nature and delicacy that distinguish the data concerning health and to the real danger of using it for strongly discriminatory purposes, as evident in European regulations and case law.

The historical evolution of the European regulations on the protection of confidentiality must be considered. At the European level, the first attempt to introduce rules for the protection of the right to confidentiality was made by the 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data' (Convention No. 108, adopted in Strasbourg by the Council of Europe on 28 January 1981). Art. 6 identified 'special categories of data', which included that concerning health, and prohibited automatic processing of this data unless domestic law provided an appropriate system of safeguards. To further this aim, the Convention of Strasbourg provided guidelines for the protection of personal data concerning health status and sexual life, prohibiting in principle its automatic processing.

The contemporary Recommendation (R (81) 1 of 23 January 1981 on regulations for automated medical data banks then replaced by R (97) 5 of 13 February 1997 on the Protection of Medical Data) significantly invited Governments to apply a uniform regulation for medical data, inspired by some basic principles like public notice of the creation of data banks; the specific indication of the purposes and the framework of accessibility to the collection; the fairness, lawfulness and appropriateness of processing; the limitation of access to medical staff and other health care staff in relation to their relevant specific duties; and the storage of information for the time strictly required, except for the needs of medical, historical or statistical purposes.

The subsequent Directive 95/46/EC of 24 October 1995 then defined a more comprehensive architecture of the legislative framework. In particular, Art. 8 strengthens the indications of the Convention of Strasbourg, explaining a set of safeguards in the absence of which the processing of these 'special categories of data' should be prohibited.

Lastly, the European regulation was enriched by the Regulation (EU) 2016/679 – GDPR, adopted on 27 April 2016 and entered into force on 25 May 2018: today, we must refer to this act to identify the legal basis for the processing of personal data that is called sensitive (or belonging to special categories).[15]

The European legislator, and subsequently Member States, are required to search for the right balance between the values that are crucial in this field: a) movement of information, for the function of the protection of public and pri-

[15] Providing personal data to an automated system, scoring the data and profiling individuals based on the results is considered as processing of personal data; therefore, such a processing operation needs to be in line with the principles defined in the GDPR. For this reason, the Commissioner for Personal Data Protection (Cypriot SA), with a pronouncement adopted on 27 January 2020, fined a group concerning the lack of legal basis of an AI tool which was used to score employee sick leaves.

vate health and the best management of *welfare* systems, that should be granted with respect to the principles of public notice and transparency when – as is almost always the case – the datum is held by public administrations or any substantially public body; and b) the protection of the privacy and dignity of the human person.

The items of the Regulations evoke the multiple interests involved. The protection of natural persons, the processing of personal data and the free movement of data require the policymaker to search for a not easy squaring of the circle: by ensuring everyone, in a balanced manner, a space of implementation without compromising too much of the others.

The protection of data represents a hedge for the (uncontrolled) movement and the (undue or unlimited) processing of data itself. Substantially, we have to acknowledge – on the one hand – that the technological evolution unavoidably facilitates the fast spread of information, and – on the other hand – that the processing of personal data represents a valuable opportunity aimed at realising clear and creditable purposes (the movement of data becomes a piece of an actual 'freedom'). At the same time, the problem of regulating such freedom arises so that it does not jeopardise the rights of private subjects equally worthy of protection.

It is a given that the knowledge of information regarding natural persons is increasingly facilitated by technological tools of new generation and that it is useful for multiple objectives of a potentially undefined number.

Simultaneously, the old setting based on the secrecy of the information held by public administrations has been replaced by principles of accessibility to administrative acts and documents, as well as by the introduction of increasingly wider obligations of public notice and transparency.

The GDPR is relevant for several aspects of medical law. It is fundamental, above all, since it sets out limitations on the processing of medical data: such processing is allowed for the purposes of public interest in the field of public health in which the aim, *inter alia*, is to ensure high standards of quality, security, cost-effectiveness and continuity of healthcare, as well as of medical products and medical devices (see *Recitals* 52, 53 and 54; Art. 9 of the Regulation).

Processing of data, according Art. 4, no. 2, of GDPR, means 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.

The notion of informed consent given by the data subject is equally crucial and is meant as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a

clear affirmative action, signifies agreement to the processing of personal data relating to him or her' (Art. 4, no. 11, of GDPR). [16]

Informed consent has also been subject to a wide development in the area of case law. Significantly, by means of the person-centred approach that inspires several Constitutions of Western countries, it has been set up as an actual right of the person that constitutes the expression of the principle of self-determination and contributes to make medical treatment lawful, mitigating the information asymmetry between the patient and the practitioner: [17] a constitutive factor of the legitimacy and foundation of medical treatment, without which the action of the practitioner is – except for the legal compulsory treatment or when a state of necessity occurs – illegal also when put in place in the interest of the patient.

As a general rule *Recitals* 52, 53 and 54 establish, the prohibition of processing personal data capable of revealing the health status of individuals.

The prohibition of processing data concerning health provides exceptions when the treatment is instrumental to: a) the fulfilment of a purpose of public interest; b) the need for the establishment, exercise or defence of legal claims, in court proceedings or in an administrative or out-of-court procedure.

Limitations to exceptions are relatively established for both the above described hypotheses.

If processing is necessary for reasons of public interest in the sector of public health, the processing of personal data for other purposes is not allowed to third parties (like employers, insurance and banking companies) (*Recital* 54). More generally, it prescribes the adoption of suitable and specific measures to protect fundamental rights, data and freedoms of natural persons, even more in cases in which the consent of the data subject can be rescinded; while, according with *Recital* 53, professional secrecy should be kept by persons processing data for purposes linked to health, notwithstanding the power of Member States to introduce or keep further limitations to the processing of data, provided

---

[16] *Recitals* 42 and 43 add that 'for consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment' and, respectively, that 'in order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance'.

[17] Italian Constitutional Court, 23 December 2008 no. 438.

that this does not hamper the free movement of data within the EU when the mentioned limitations are applied to cross-border processing of such data.

Conversely, with regard to the other derogation to the general prohibition, the right to exercise or defend legal claims, the 'neighbour' of the right to the protection of personal data, it must rank *pari passu* with the latter.

The same *Recitals* 52 and 53 specify the reasons for public interests that justify the derogation of the prohibition of processing data concerning health, moving from a notion of public health that includes the financial and expenditure aspects, the provision of services and the universal access to health and social care.

For what concerns the notion of 'public health', *Recital* 54 clarifies that 'it should be interpreted as defined in Regulation (EC) 1338/2008 of the European Parliament and of the Council, 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 processing of personal data must be functional to the realisation of purposes linked to or regarding health if and because they are aimed at benefiting persons and the whole society to achieve a multiplicity of objectives: 1) ensuring the quality and continuity of procedures aimed at meeting the demands of benefits and services; 2) promoting an economic management of health care services; 3) ensuring health safety, prevention and control of communicable diseases and other serious threats to health; 4) facilitating the activity of storage in the public interest, scientific or historical or statistical research, as well as the implementation of studies in the field of public health; 5) safeguarding the continuity of cross-border treatments.

In addition, the delicacy and specialisation of the processing of data in the context of public health is at the base of the rule that allows Member States to require the obligation of prior consultation for the controller with the supervisory authority, even outside the conditions established by the same GDPR (Art. 36, para 1 and 2).

Recital 63 defines exactly the framework of the data subject's rights. 'A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing

information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing'.

Provisions establishing the arrangements for data concerning health are set out under Art. 9, focused on consent for processing (lett. a-e).

For our aims, the succeeding letters are relevant and, in particular, lett. f) which makes provision for the case of processing that is necessary for the protection of a right in legal claims or for the exercise of judicial capacities by the competent authorities (the limitation should constitute a necessary and proportionate measure in a democratic society to safeguard specific important interests: as per *Recital* 19); lett. g) which legitimises the processing necessary for reasons of a juridically relevant public interest by respecting the principles of proportionality and minor burden for the legal situation of the data subjects; lett. h) which concerns the processing necessary, *inter alia*, for the purposes of preventive medicine or medical diagnosis and health care or management of health or social services and requires, by virtue of the referral to the subsequent paragraph 3, that data are processed under the responsibility of a professional or another person subject to the professional secrecy; lett. i) which, among the factors that make processing necessary, lays down the reasons of public interest in the field 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 medical products and medical devices, notwithstanding the safeguard of rights and freedoms of the data subject and professional secrecy; and lett. j) which mentions the purposes of archiving and scientific, historical or statistical research, referring to Art. 89. This latter, in turn, completes the framework by subjecting this type of processing to technical and organisational measures that ensure the pseudonymisation or, in any case, the minimisation of data, and by authorising derogations to the rights acknowledged to the data subject by Artt. 15, 16, 18, 19, 20 and 21.

A specific remark should be made on the processing of personal data for the purposes of scientific research in the medical and biomedical fields, reporting that the Community objective to establish a European research area pursuant to Art. 179, par. 1, TFEU, is subject to the obligation of respecting also other relevant regulations, among which the one on clinical trials stands out. 'The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials' (*Recital* 156) and, in the same direction, 'for the purpose of consenting to the participation in sci-

entific research activities in clinical trials, the relevant provisions of Regulation (EU) 536/2014 of the European Parliament and of the Council should apply' (*Recital* 161). A link is so established between Regulation 536/2014 on clinical trials and Regulation (EU) 2016/679 on data protection.

The fourth and last paragraph of Art. 9 sets out that Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health [18]: taking into consideration historical and cultural traditions and ideological and political orientations as well as the constitutional, organisational and administrative structure of each Country.

Ultimately, the specificity of sensitive data clarifies the special attention it increasingly receives from legislators at the European level and at domestic levels in Member States.

Among personal data, sensitive data is characterised by its inherence to the most intimate individual sphere and by its capacity of affecting the development and free expression of the personality. In short, it relates to the dignity itself of the person.

Confidentiality, meaning the right not to incur intrusions into one's intimate sphere and regardless of one's willingness through the spread of personal information and, from our perspective, on the personal health status, requires an appropriate system of protections. The acquisition and movement activity of personal data is stimulated by reasons and interests of various natures, therefore it can be subjected to abuses if not correctly delimited, also taking into consideration the new computerised arrangements to collect information and the increasing demands for data by public and private institutions in order to track the data subjects' profile.

Equally, we should avoid or, in any case, reduce at most the risk of possible discrimination to the damage of natural persons on the basis, *inter alia*, of the 'genetic or health status or sexual orientation' [19]: this risk is taken into con-

---

[18] Whether biometric data constitute sensitive data must therefore be assessed on the basis of the particular processing purpose: *see* L. Feiler, N. Forgò, M. Weigl, *The EU General Data Protection Regulation (GDPR): A Commentary* (German Law Publisher 2018) 95.

[19] *See* ECHR, Section III, 15 March 2016, *Novruk and Others v. Russia*, nos. 31039/11, 48511/11, 76810/12, 14618/13 and 13817/14. In this case, all five applicants wished to obtain residence permits in Russia. To complete their application, they were required to have a medical examination which included a mandatory test for HIV infection. After they tested positive for HIV, the migration authorities refused their applications by reference to the Foreign Nationals Act, which prevents HIV-positive foreign nationals from obtaining residence permits. In particular, the applicants alleged that they had been discriminated against because they were HIV-positive. The Court held that there had been a violation of Art. 14 (prohibition of discrimination) read together with Art. 8 (right to private life and family) of the Convention. It notably stated that the legislation aimed at preventing HIV transmission which was used in the present case to exclude the applicants from entry or residence had been based on an unwarranted assumption that they would engage in unsafe behavior, without carrying

sideration, for example, in *Recital* 71 that imposes on the controller, when profiling, to adopt appropriate technical and organisational measures in order to ensure safety of personal data and rights of the data subject and to prevent the occurrence of the aforementioned discriminatory effects. [20]

The GDPR provides important answers to all these needs of the personal data, defining a mature and advanced framework of protections.

Processing and/or disclosing a datum about the health of a person, regardless of the aim – purposes of care and treatment, commercial, research or administrative management, expenditure control or the judicial protection of rights – integrates unlawfulness if it goes beyond the hedges established by the legislator for the systemic and automated collection of data and for the increasing research of data by public and private institutions.

When the object of the right to confidentiality is medical datum, the degree of responsibility of the guardians for balancing increases since they are called upon to prevent or effectively sanction the abuses of processing.

On the other hand, information is a good exclusively belonging to the data subject; in any case, it has to be appropriately protected. Only in this way can the useful and legal movement of data produce the various benefits, even in favour of the owners of the datum, who today are no longer required to give their consent when the datum is processed for the purposes of their treatment. [21] Hence, the non-absolute but relative character of the right to the protection of personal data in the framework of the standardisation with other values, principles and rights.

In particular, there will be no breach of confidence in situations in which the patient's interest in keeping information confidential from others, including relatives, is outweighed in the balance by broader 'public interest' considerations. [22]

---

out a balancing exercise involving an individualized assessment in each case. Given the overwhelming European and international consensus geared towards abolishing any outstanding restrictions on entry, stay and residence of people living with HIV, who constitute a particularly vulnerable group, the Court found that Russia had not advanced compelling reasons or any objective justification for their differential treatment for health reasons. Therefore, the applicants had been victims of discrimination on account of their health status.

[20] Furthermore, at the case law level, cases can be found of discrimination perpetrated to the damage of private subjects as a consequence of transfers, without their consent, of medical data concerning them: such conduct determined, in some cases, the withdrawal of the offer of employment (Court of Justice of the EU, sect. I, 5 July 2011, *V. Parliament*, F-46/09) and, in others, the denial to employ a person after having performed tests capable of giving rise to suspicions that he was suffering from the HIV virus, despite his opposition to undergo such tests (Court of Justice of the EU, 5 October 1994, C-404/92 *X v. Commission*).

[21] *See* C. Colapietro, F. Laviola, 'I trattamenti di dati personali in ambito sanitario' (2019), in <*www.dirittifondamentali.it*> (2) accessed on 08.10.2020.

[22] *See* J. Harris, 'Ignorance, Information and Autonomy', in *Theoretical Medicine and Bioethics* (2001) 24.

Nonetheless, the speed of processing and transmission of information and the possibility to take economic advantage of it explain the distrust of citizens: the technological progress, on the one hand, can increase the efficiency and quality of the medical system but, on the other, can paradoxically increase the fear for uncontrolled access to the clinical documentation of private subjects.

In conclusion, the objectives of the processing of personal data can be diverse and very valuable: suffice it to think of the endless potentialities of the electronic health record.[23] However, the trust of the individual in the system continues to be a solid pillar.[24] Patients' consent, although more blurred than in the past, even now constitutes one of the main conditions that make the movement of their data lawful, determining the acceptance of the purposes and the arrangements through which the processing is carried out.

3. *Specific issues in the case law interpretation: omission of processing*

The European Court of Human Rights has given some important clarifications – at the application of Art. 8 ECHR – beginning with the 'failure to process' data. The bond of accordance with the ECHR for the limitations that can be attributed to the rights of the data subject by the European law or individual States' law is generally affirmed by *Recital* 73 of the Regulation.

Art. 8 ECHR, in the item 'Right to respect for private and family life', establishes that 'Everyone has the right to respect for his private and family life, his home and his correspondence' (para 1).

The concept of 'private life' under Art. 8 ECHR is fundamental: it is a broad term not susceptible to exhaustive definition,[25] extensively and functionally interpreted by the Court in tune with the general purposes of protection pursued by the Convention, that is intended to guarantee not rights that are 'theoretical or illusory' but rights that are 'practical and effective'.[26]

The objective of the rulings of the Court on the matter is to increase the centrality of citizens and the protection of their legal sphere and their own

---

[23] See L.B. Harman, C.A. Flite and K. Bond, 'Electronic Health Records: Privacy, Confidentiality, and Security', in *Virtual Mentor – American Medical Association Journal of Ethics* (2012) 14(9) 712. C.K. Wang, 'Security and privacy of personal health record, electronic medical record and health information. Problems and Perspectives', in *Management* (2015) 13(4) 19-26.

[24] As pointed out by J. Harris, *Ignorance, Information and Autonomy*, p. 2, in medical practice from the earliest times, the need for honest information and the ethics of information giving have been central.

[25] ECHR, Grand Chamber, 4 December 2008, *S. and Marper v. The United Kingdom* [GC], no. 30562-30566/04.

[26] ECHR, Grand Chamber, 9 October 1979, *Airey v. Ireland*, no. 6289/73.

dignity upon a movement of personal data that is increasingly massive and facilitated by the new technological tools.

According to the constant case law of the Court, the scope of Art. 8 ECHR above all covers the physical and psychological integrity of a person.[27] Each State is required to ensure such protection, not only by refraining from intentionally causing damage to the physical and psychological integrity of whoever is subject to its jurisdiction (an obligation with essentially a 'negative' content) but also by adopting all the measures necessary to protect such good of life ('positive' obligation).[28]

Assessing the correct use by a State of its margin of recognition, the Court verifies if the decision-making process that has led to intervention measures has been fair and such to ensure the respect of the interests of the individual protected by Art. 8.[29]

For what relates specifically to the protection of health, the Court states that, although such right is not expressly enshrined in the Convention and its Protocols, State Parties are subjected not only to the positive obligations under Art. 2 ECHR but also to the positive obligations deductible from Art. 8 ECHR. These obligations consist, on the one hand, of the substantive obligation to provide legislation that imposes on health structures, both public and private, the adoption of appropriate measures for the protection of the physical integrity of patients and, on the other, of the procedural obligation to ensure to the victims of medical negligence the access to an internal remedy that allows them to obtain a fair compensation for the damage suffered.[30]

By applying Art. 8, the same Court has censured, on various occasions, the default of the respondent State in respect of the obligation to provide for an effective access to documents regarding the health of a person.

---

[27] ECHR, Section IV, 29 April 2002, *Pretty v. The United Kingdom*, no. 2346/02; ECHR, Section IV, 22 July 2003, *Y.F. v. Turkey*, no. 24209/94 (underlining that a person's body concerns the most intimate aspect of private life); ECHR, Section I, 5 March 2009, *Janković v. Croatia*, no. 38478/05.

[28] The Court stated that 'regard must be had to the fair balance that has to be struck between the competing interests of the individual and of the community as a whole' (ECHR, Grand Chamber, 9 December 1994, *Lòpez Ostra v. Spain*, no. 16798/90; ECHR, 7 July 1989, Grand Chamber, *Gaskin v. The United Kingdom*, 7 luglio 1989, no. 10454/83).

[29] The Court has the task of checking 'whether the decision-making process leading to measures of interference was fair and such as to afford due respect to the interests safeguarded to the individual by Article 8' (*See* ECHR, Section I, 23 March 2017, *A.-M.V. v. Finland*, no. 53251/13; ECHR, Section I, 27 May 2004, *Connors v. The United Kingdom*, no. 66746/01; ECHR, Grand Chamber, 29 September 1996, *Buckley* v. *The United Kingdom*, no. 20384/92).

[30] *See* ECHR, Section V, 15 November 2007, *Benderskiy v. Ukraine*, no. 22750/02; ECHR, Section III, 2 June 2009, *Codarcea v. Romania*, no. 31675/04; ECHR, Section II, 5 January 2010, *Yardımcı v. Turkey*, no. 25266/05; ECHR, Section IV, 25 September 2012, *Spyra and Kranczkowski v. Poland*, no. 19764/07; ECHR, Section III, 15 January 2013, *Csoma v. Romania*, no. 8759/05; ECHR, Section III, 23 September 2014, *S.B. v. Romania*, no. 24453/04.

For example, it has occurred that national judges illegally did not permit access to information regarding the clinical treatment administered at the internal hospital of the correctional facility. [31]

In other cases, claims were issued for the denial of the issuance of medical documentation regarding hospitalisation of some women at a health facility who had been found to suffer from infertility after receiving treatment: just because the access to clinical records would have allowed a legal-medical analysis of the causes of the pathology detected. [32]

As underlined by the Court, disputes like these regard the exercise of the right to effective access to information concerning one's health and reproductive status. The right under consideration is related to private and family life under Art. 8. It is violated even when authorities interpret in a restrictive manner the term 'authorized legal representative', denying access to the lawyer who has the proxy and limiting it only to the minor's parents or the legal guardian appointed to represent the incompetent. [33]

There was similarly a violation of the obligations weighing down on the respondent State in the legal claim in case of denied access to documentations of social and health services, containing information on the childhood and personal history of the requester. [34]

For what concerns the arrangements for protection, the Court has specified that, in order to ensure an effective exercise of the right, the positive obligations are fulfilled by making copies of personal data available to data subjects. The decision on the ways to extrapolate and copy their personal data is up to the data subjects, provided that they bear the relevant costs, and they cannot be obliged to justify their request for the copy of such data. [35]

Conversely, authorities are obliged to demonstrate any plausible reason for which the request should be refused. Only in this case, the right of the requesters to obtain copies of medical records regarding them can be considered re-

---

[31] Indeed, this is a case currently pending (case *Sokolow v. Germany*, no. 11642/11) in which framework the Court has notified the appeal to the German Government making then questions to the parties pursuant to Art. 8 of the Convention.

[32] ECHR, Section IV, 28 April 2009, *K.H. and Others v. Slovakia*, no. 32881/04. The applicants, eight women of Roma origin, could not conceive any longer after being treated at gynecological departments in two different hospitals and suspected that it was because they had been sterilized during their stay in those hospitals. They complained that they could not obtain photocopies of their medical records. The Court held that there had been a violation of Art. 8 (right to private and family life) of the Convention in that the applicants had not been allowed to photocopy their medical records. In addition, it found that, although subsequent legislative changes compatible with the Convention had been introduced, this had happened too late for the applicants.

[33] ECHR, Grand Chamber, 19 October 2005, *Roche v. The United Kingdom [GC]*, no. 32555/96.

[34] ECHR, Section II, 24 September 2002, *M.G. v. The United Kingdom*, no. 39393/98.

[35] ECHR, Section I, 20 December 2007, *Phinikaridou v. Cyprus*, no. 23890/02.

cessionary: in the trial that has taken place before Cypriot authorities, the claimants had obtained a judicial order against the hospital for the exhibition of the acts required through having the chance to consult their full and entire medical documents; however, the possibility to extract an integral copy of such documentation had been denied, and their access was limited to the study of the records and the manual reproduction of parts of their content. Nevertheless, the manual extracts do not represent an effective access to documents concerning health. Moreover, the original clinical records that could not be manually reproduced contained relevant information for the result of the judgement of compensation filed by the claimants who had appointed an independent expert to examine them in order to verify their integrity and completeness.

Particularly interesting is the part of the judgement dealing with the alleged abuse by the claimants of the information they received to exclude its existence in the hypothesis that an integral copy of the documents is required: according to the Court, the protection of data concerning health falls within the essential core of the right under Art. 8 ECHR and the respect of confidentiality of medical data constitutes 'a vital principle in the legal systems of all the Contracting Parties to the Convention' [36]: in any case, as the Court adds, the risk of such an abuse could have been prevented by different means, less invasive than the denial of the copies of records. For example, the communication or disclosure of personal data concerning health that is potentially incompatible with the safeguards under Art. 8 can be prevented by means such as the introduction in the national law of appropriate safeguards in order to strictly limit the circumstances in which such data can be disclosed and the group of people authorised to access such records.

The most recent pronouncements stress the States' positive obligation to provide an effective and accessible procedure enabling the person involved to have access to all relevant information that would allow him/her to understand his/her health state: that is, the assessment of his psychological fitness for a job position. [37]

---

[36] *See* ECHR, Section IV, 17 July 2008, *I v. Finland*, no. 20511/03, § 38: 'The protection of personal data, in particular medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. The above considerations are especially valid as regards protection of the confidentiality of information about a person's HIV infection, given the sensitive issues surrounding this disease. The domestic law must afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention'.

[37] *See* ECHR, Section V, 7 March 2018, *Yonchev v. Bulgaria*, no. 12504/09. This is the case: the applicant applied for a position as police observer in an international mission but his application was

In such a situation, it is up to the domestic authorities to show that any documents in the applicant's personnel file have been classified as State secrets. In any case, both the administrative and judicial procedures available to the applicant in order to protect his or her personal data must be inherently effective on the grounds that the applicable legislation expressly obliges the competent bodies to carry out a balancing exercise.

In these contexts, the Court held that the respondent State's positive obligation under Art. 8 required it to provide an effective and accessible procedure enabling the applicants to have access to all relevant and appropriate information necessary for the specific purposes described above. [38]

In other cases, the right to access documents containing sensitive data has been recognised since the relevant request was based on the principle of transparency, to be considered as prevailing on opposed interests with a commercial nature. This is the case of the clinical study report (CSR) created by a pharmaceutical company to which one of its competitors requests to access and that, according to the EU General Court, is not covered by a general 'presumption of confidentiality'. [39]

---

rejected because of the negative result of his psychological assessment. He was then refused access to personal data held by the Ministry of the Interior, despite having a particularly strong interest to get acquainted with his psychological assessments. Consequently, the Court stated that access to information about the reasons for his having been found unfit to participate in the international mission, especially taking into account the sensitive nature of such information, must be seen as sufficiently closely linked to his private life within the meaning of Art. 8 of the Convention.

[38] The Court would like to reiterate that it has recognized a vital interest, protected by Art. 8, of persons wishing to receive information necessary to know and to understand their childhood and early development or to trace their origins, in particular the identity of their natural parents, information concerning health risks to which interested persons have been exposed or information about a person's records created by the secret services during the period of a totalitarian regime.

[39] *See* EU General Court, 5 February 2018, *PTC Therapeutics International v. EMA*, T-718/15. In a synchronous way, see Court of Justice UE, Section IV, 22 January 2020, C-175/18. For a case law application of the principle for which the obligation of transparency does not justify the disclosure of personal data concerning health, see EU General Court, 3 December 2015, *CN v. Parliament*, T-343/1. In the latter case, the applicant, who was an official of the Council of the European Union, had submitted a petition to the European Parliament on the subject of the support granted to disabled family members of a European official by means of a form available online on the Parliament's website. At a later time, he requested that the notice be removed from the Parliament's website. He complained that Parliament's duty of transparency cannot justify the disclosure of personal data relating to the state of health and the presence of a person with disabilities in his family. Even assuming publication of a summary of petitions in order to provide information on the activities of the EU institutions to be a legitimate interest, the infringement of the applicant's rights is disproportionate. The Court verified that he had given his express consent to the publication of his sensitive personal data on the Internet. In the meantime, it pointed out that under Art. 10(1) of Regulation 45/2001, the processing of personal data revealing data concerning health is prohibited. However, Art. 10(2)(a) of that regulation provides that this prohibition does not apply, inter alia, where the data subject has given his or her express consent. Against this background, it should be observed that Art. 2(h) of Regulation 45/2001 defines the data subject's consent as 'any freely given specific and informed indication of his or her

Basically, it is a particular application of the so-called *pari passu* rank criterion used in many national laws, including the Italian one: the processing is allowed if the judicially relevant situation that is meant to be protected with the request of accessing administrative documents ranks at least *pari passu* with the data subject's interests or consists of a right of the personality or another fundamental right or freedom.

4. *Processing performed in the absence of legal basis*

There are many circumstances of non-authorised (or illegal 'for an excess') processing established by the European Court.

There is the case of a subject whose HIV condition was made public during a criminal trial against the partner, although the disclosure of the sensitive datum to the media was not supported by any valid motivation. [40] In this situation, the Court noted in particular that respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention and is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. The domestic law must, therefore, afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Art. 8 of the Convention.

Then there is the case of the communication during a hearing of confidential information concerning the mental status of a party in the case and the psychiatric treatment previously administered in which such information was determined irrelevant for the result of the dispute. [41] Therefore, obtaining from a psychiatric hospital confidential information regarding the applicant's mental state and relevant medical treatment and disclosing it at a public hearing had constituted an interference with the applicant's right to respect for his private life.

---

wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed'.

[40] ECHR, Grand Chamber, 25 February 1997, *Z. v. Finland*, no. 22009/93. The Court held that there had been a violation of Art. 8, finding that the disclosure of the applicant's identity and HIV infection in the text of the Court of Appeal's judgment made available to the press was not supported by any cogent reasons and that the publication of the information concerned had accordingly given rise to a violation of the applicant's right to respect for her private and family life.

[41] In this sense, ECHR, Section V, 29 June 2006, *Panteleyenko v. Ukraine*, no. 11901/02, where the interference in the right to the respect of the private and family life was sanctioned, since the request of information under consideration issued by the judge of first instance was to be considered unnecessary given the irrelevance of such data for the trial inquiry and for the ongoing preliminary investigations.

There is also the case in which a court made use of documents taken from the clinical records of a subject who was a party in a divorce case without his/her consent and without the prior appointment of an expert, when the reference to the medical report was made only alternatively so that the same conclusion could have been reached regardless: in this circumstance, the Court found a violation of Art. 8, considering the interference in the private life of the requester not justified in consideration of the fundamental importance of the protection of personal data. Moreover, the Court found that the domestic law did not provide for sufficient safeguards regarding the use of such type of data processing concerning the private life of the parties, therefore justifying, a fortiori, the need for a strict review of the need for such measures. [42]

There is also the case in which a woman in childbirth claimed against the non-authorised presence of medical students during her delivery, without the possibility to give a written consent for the awareness of being observed under the relevant clinical teaching programme, given that the brochure of the hospital informing the claimant about her potential involvement in the said programme was vague and the matter had been introduced to her as something for which she would not have had a choice: here, the Court found that the national legislation on the moment of the birth of the claimant's daughter did not contain any safeguard aimed at protecting the right to patients' privacy and, furthermore, such a serious gap was aggravated by the procedure of the hospital to obtain the patients' consent. [43]

Moreover, there is the case of Jehovah Witnesses who, after their refusal to undergo blood transfusions during their hospitalisation in public hospitals, regret the communication of their medical dossiers to the judicial authorities during an investigation on the lawfulness of the activities carried out by the religious organisation to which they belong: the violation occurs when there are no urgent collective needs for the disclosure of confidential medical information without prior notice and without the possibility to oppose such an invasive measure in their legal sphere. [44]

---

[42] ECHR, Section II, 10 October 2006, *L.L. v. France*, no. 7508/02.

[43] ECHR, Section I, 9 October 2014, *Konovalova v. Russia*, no. 37873/04.

[44] ECHR, Section I, 6 June 2013, *Avilkina and Others v. Russia*, no. 1585/09. In the circumstance, the judicial authorities had ordered all the hospitals in St. Petersburg to report any case of refusal of blood transfusion by Jehovah Witnesses. Ultimately, the Court found that there had been no pressing social need to disclose confidential medical information about them. Furthermore, the means employed by the prosecutor in conducting the inquiry, involving disclosure of confidential information without any prior warning or opportunity to object, need not have been so oppressive for the applicants. Therefore, the authorities had made no effort to strike a fair balance between, on the one hand, the applicants' right to respect for their private life and, on the other, the prosecutor's aim of protecting public health.

Then there is the case of the collection of medical personal data by a State agency (the Latvian Inspectorate of Quality Control for Medical Care and Fitness for Work) without the consent of the data subject, failing to indicate with sufficient clarity under the applicable law about the scope of the discretionary power conferred to competent authorities and the arrangements for exercising it, and missing any assessment on the relevance and indispensability of the data with respect to the institutional aims of the legal person, controller of such data: reaffirming the importance of the protection of medical data for the enjoyment of the right to the respect of private life by a person, the Court acknowledged that in such occasion, the national law had not limited in any way the extent of private data which could be collected by the Inspectorate and that determined the indiscriminate collection of the requester's medical data regarding a period of seven years without any prior assessment of whether these data were potentially decisive, relevant or important to achieve any aim that could have been pursued by the investigation under consideration. [45]

Furthermore, there is the case of an article published in 2001 on the front page by the leading Lithuanian newspaper about a threat of contagion from HIV in a remote region of Lithuania, on the basis of information on the HIV positivity of the claimants confirmed by the medical staff of a hospital: on this occasion, a failure of any form of legal protection of the patient's privacy and of any dissuasive measure for the undue processing of personal data was found. [46] In this case the medical staff of a centre for the treatment of HIV had been sued for having confirmed that the claimants were HIV positive. About the second claimant, defined as 'notoriously promiscuous', it was even said that the claimant had two illegitimate children with the first claimant. The Court, in addition to verifying the existence of a violation of Art. 8 ECHR because of the minimal compensation recognised to the claimants for the damage, took care to significantly highlight the negative impact of such a disclosure on the spontaneous availability of other subjects to voluntarily undergo the HIV tests and the appropriate treatments.

Lastly, there is the case of the woman who, after being involved in a car accident, had applied for invalidity pension and who, after the rise of a dispute with her insurer for the amount of such pension, had refused to undergo further medical examinations aimed at giving new evidence on her health status. For this reason, the insurance company appointed private investigators to secretly surveil the woman and use the results in the next judicial proceedings: here, the Court found that the provisions of the Swiss law on which the sur-

---

[45] ECHR, Section IV, 29 April 2014, *L.H. v Latvia*, no. 52019/07.

[46] ECHR, Section II, 25 November 2008, *Armonas v. Lithuania,* no. 36919/02; ECHR, Section II, 25 November 2008, *Biriuk v. Lithuania*, no. 23373/03.

veillance activity had been formally based were not sufficiently precise on the maximum period and arrangements for the purposes of archiving and consultation of data thereby obtained. Upon the censure of the claimant, according to which the surveillance had violated her right to the respect of private life and therefore should not be admitted in the jurisdictional proceeding, the Court ascertained a violation of Art. 8 on the notable fact that the actions of the insurer constituted a State responsibility under the Convention, since, according to the Swiss law, the respondent insurance company was considered a public authority. It acknowledged also that the secret surveillance that had been ordered had interfered with the private life of the requester, although carried out in public places, since the investigators had systematically collected and stored the data and had used it for a specific purpose. [47]

In other situations, the European Court has established, instead, that the interference suffered in the private sphere was legitimate as a consequence of a measure of the respondent State in the legal claim.

Thus, for example, in the case of archived information in the records of a psychiatric hospital which concerned the confinement of the claimant, afterwards acknowledged as illegal, the indefinite storage of patient's information in a central archive had been disputed. However, the recording of information regarding mental patients was considered suitable to fulfil not only the legal interest in ensuring the proper functioning of the service of the public hospital but also patients' rights, especially in case of compulsory hospitalisation. Moreover, in the circumstance, sensitive data resulted to be protected by appropriate confidentiality measures, so that documents were not accessible by the public but only for categories of people strictly listed outside the institution. In summary, the interference suffered by the claimant could not be considered disproportionate in respect of the legal purpose pursued, that is, the protection of health. [48]

The same happened in the case of the communication by a clinic to a social security body of clinical records containing information about an abortion of the claimant. The Court excluded the violation of Art. 8, considering such communication justified by the purpose pursued, that is to allow the social security body to establish if the conditions pursuant to law had been met in granting the compensation for the damages subsequent to an accident at work. More-

[47] ECHR, Section III, 18 October 2016, *Vukota-Bojic v. Switzerland*, no. 61838/10.

[48] European Commission of Human Rights, 9 July 1991, *Chave née Jullien v. France*. This case concerned the storing of records in a psychiatric hospital that contained information relating to the applicant's compulsory placement, the illegality of which had been recognized by the domestic courts. The applicant considered, in particular, that the continued presence in a central record of information about her confinement in a psychiatric institution constituted an interference with her private life and wanted such information to be removed from central records of this type.

over, the measure disputed was subjected to strict limitations and complemented by appropriate and effective remedies against any abuse. [49]

The most recent decisions reaffirm the need for the storage of data to take place in compliance with the law. [50]

At the same time, the provision of consent continues to play a crucial role [51]: when it is demonstrated that the disclosure of personal data has resulted in an interference in the private life of the data subjects, without an expression of their willingness to make the data public, it is necessary to verify the existence of a legal basis that justified the processing and if the interference could be considered proportionate. [52] In this occasion, the Court also reminded that for the purposes of the application of Art. 8 of the Convention, the legal nature of the subject processing the sensitive information or to which such information is communicated is irrelevant.

The Court clarified that the space of sensitive data should be meant in a particularly wide sense: for example, medical information must be qualified as confidential even if contains a reference to the standardised grounds for dispensation from military service rather than a personalised medical diagnosis. [53]

In the latter case, the applicant instituted civil proceedings against his employer because of the dissemination of information concerning the medical grounds for his dispensation from military service. The Court stated that, in general, health data constitutes personal data and could only be collected with the consent of the person concerned, unless otherwise envisaged by law. Specifically, the domestic judges should have established whether it had been lawful to collect and use the applicant's psychiatric health data in the manner and in the context in which it had been used; what the purpose of its processing had been

---

[49] European Commission of Human Rights, 27 August 1997, *M.S. v. Sweden*, no. 20837/92. In this pronouncement, the aim to protect the economic wellbeing of the country has been underlined.

[50] The storage of health or other sensitive data is of great importance: *see* ECHR, Section V, 30 January 2020, *Breyer v. Germany*, no. 50001/12; previously, ECHR, Section IV, 13 November 2012, *M.M. v. The United Kingdom*, no. 24029/07.

[51] *See* ECHR, Grand Chamber, 5 September 2017, *Bărbulescu c. Romania*, no. 61496/08.

[52] *See* ECHR, Section IV, 27 February 2018, *Mockutè v. Lithuania*, no. 66490/09. In this case, the Court found that the disclosure of highly personal and sensitive confidential information about the applicant, obtained during her involuntary hospitalization and treatment at Vilnius Psychiatric Hospital, by a hospital psychiatrist doctor to journalists entailed an interference with the applicant's right to respect for her private life guaranteed by par. 1 of Art. 8.

[53] *See* ECHR, Section V, 26 January 2017, *Surikov v. Ukraine*, no. 42788/06. The Court found that the employer in issue had acted unlawfully, on the one hand, in obtaining the file containing sensitive medical data from the military enlistment office without the applicant's knowledge or consent and, on the other hand, in including this information in the applicant's personnel file in spite of its retention patently having been excessive for the purposes for which it had been kept, what is more using the same information for a new purpose.

and whether it had been justified. So, the fair balance between the employer's interests and the applicant's privacy-related concerns was not sought.

Ultimately, on numerous occasions the Court has held that systematic storage and other use of information relating to an individual's private life by public authorities entails important implications for the interests protected by Art. 8 of the Convention and thus amounts to interference with the relevant rights. This is all the truer when the information concerns a person's distant past or when the processing affects highly intimate and sensitive categories of information, notably the information relating to physical or mental health of an identifiable individual.

Therefore, an interference breaches Art. 8 unless it is in accordance with the law, pursues one or more of the legitimate aims referred to in paragraph 2 of the same Article and, in addition, is necessary in a democratic society to achieve those aims. The fundamental data protection principles and the corresponding basic procedural safeguards must also be directed towards the goal of justifying the necessity of any possible interference.

By studying the case law, it's possible to extract the following fundamental criteria: a) the personal data must be relevant and not excessive in relation to the purposes for which it is collected; b) the data must be preserved for no longer than is required for the purpose for which it is stored; c) the retained data must be efficiently protected from misuse and abuse; d) minimum safeguards concerning, *inter alia*, duration, storage, usage, access by third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction must be equally put in place at each stage; e) domestic laws must be fully consistent with the international obligations of the same; f) the data retention must be proportionate in relation to the purpose of collection and envisage limited periods of storage; g) the interference has to be proportionate with the applicant's right to respect for private life; h) the margin of appreciation afforded to the member States in designing their respective legislative and administrative frameworks in this sphere is rather limited; and i) the question of necessity of interference may overlap with the question concerning quality of the requisite procedural safeguards afforded in the domestic law of the respondent State.

Summarising, most of the decisions made by the ECHR deal with claimed violations of Art. 8 of the Convention and apply with diverse combinations of: a) the principles of proportionality and strict indispensability of the measures of personal data disclosure pursuant to States' domestic laws; b) the principle of appropriateness of the safeguards set out by such laws to protect the private sphere of the subject to which data concerning health refer; and c) the principle of self-determination of the data subject.

At the same time, the criteria to measure the level of interference in the

subjective sphere of private subjects are both of quantitative types (represented by the invasiveness of the processing in respect to the private life of the data subjects, which is inviolable) and qualitative types (represented by the sensitive nature of the data processed).

5. *Artificial intelligence and data protection: learning from the Covid-19 experience*

Many different definitions of Artificial Intelligence have been given over time.

Among these, the one given by the European Commission is particularly worthy of mention: 'Artificial intelligence (AI) refers to systems that display intelligent behavior by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications). Many AI technologies require data to improve their performance. Once they perform well, they can help improve and automate decision making in the same domain'. [54]

Three main points are to be highlighted: 1) From personalised medicine to assisted diagnostics to genetic engineering, the possibilities of AI are really endless; 2) Big data and AI are leading to radical changes in decision-making processes; and 3) AI and machine learning are constantly evolving areas of research and practice, so the discussions about transparency, proportionality and accountability are consequently increasing.

About the role of the European Union, we acknowledge that EU competencies in health protection have been increasing throughout the years, although without affecting the powers of the Member States that remain responsible for the organisation and funding of health and social care. Reaffirming the greater adequacy and incisiveness of its actions in certain fields, the European Union has acquired competence in social and health matters that is cross-sectoral and horizontal.

As such, it is capable of justifying its influence on any other policy with the objective of 'ensuring a high level of human health protection' (Art. 168 TFEU). In particular, through its actions, the EU can complete the measures adopted

---

[54] *See Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee of the Regions about 'Artificial Intelligence for Europe'*, Brussels, 25.4.2018 COM(2018).

by individual Member States: promoting public health and disease prevention, encouraging cross-border cooperation in their services and stimulating the technological innovation of national welfare systems.

Therefore, through a considerable set of soft-law acts, the EU has supported the implementation of e-health projects, among them the realisation of health information networks, the use of electronic health records and digital health records, telemedicine services and portable monitoring systems. Most recently, building on Art. 16 and 114 TFEU, in addition to Art. 168 TFEU, the European Commission adopted a set of acts aimed at promoting the creation of a single digital market in the health and care sectors. The objective of these initiatives is to enhance digital health data to provide targeted and personalised treatments to citizens, making them active participants in the management of their health, as well as in a more efficient and effective use of the available resources.

About data protection, we can say that privacy issues, consent and access to personal data are some of the main issues identified in implementing digitalisation strategies and using digital technologies in healthcare services: starting from this premise, it could be interesting to focus on the measures required to face the health emergency caused by the spread of the virus known as Covid-19.

In general, we have to take into account that using AI could be a good way to fight coronavirus spread. [55] Of course, it seems impossible to renounce mechanisms that allow concerned people to be informed about the presence of people who tested positive or that facilitate the identification of asymptomatic people who should be subjected to quarantine. [56] In fact, apps can complement the other measures – swabs and protective devices (gloves, face masks, etc.) – capable of containing the spread of the virus and limiting its reproduction capacity. At the same time, the identification of infected individuals, their isolation and retrospectively reconstructing their interpersonal contacts should be considered as the basic steps in the operational chain. In other words, these kinds of tools have valuable potential for tracking the spread of the virus, but their compatibility with the supreme principles of modern constitutional orders have yet to be verified.

Regarding the impact of the GDPR, we must consider that in its evolution,

---

[55] See C.O. Buckee and others 'Aggregated mobility data could help fight COVID-19' in *Science* (23 March 2020).

[56] *See* X. He, E.H.Y. Lau, P. Wu and others, 'Temporal dynamics in viral shedding and transmissibility of COVID-19' in *Nat Med* (2020) 26/672-675 in <*https://doi.org/10.1038/s41591-020-0869-5*> accessed on 08.10.2020; Ferretti and others 'Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing' in *Science* (08 May 2020) 368/6491 <*https://science.sciencemag.org/content/368/6491/eabb6936.full*> accessed on 08.10.2020.

the multilevel legal order has been including the development of protections in the case of the processing of health data with the use of digital tools.

The purpose is to make the processing of sensitive data lawful. Among others, examples are provided by the following rules:

• In Recitals 6 and 7 of the GDPR, it is respectively underlined that '[r]apid technological developments and globalization have brought new challenges for the protection of personal data' and the technological developments 'require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced'.

• Art. 35, Par. 1, of the same EU Regulation states that when data processsing uses new technologies likely to produce a high risk to the maintenance of rights and freedoms of individuals, there should be an assessment of the impact of the same processing on the protection of personal data, with the arrangements described in detail in the following paragraph 2 of the same Article and in line with Art. 32 regarding the responsibilities borne by the controller (or the processor, if delegated by the latter) in order to set up the most suitable and appropriate technical and organisational measures (in the case of telemedicine, for example, the major issue is to ensure the safety of the health information that is processed). [57]

In the case of apps for contact tracing, the debate about data protection is mainly focused on public health purposes. From this perspective, the legislative act may represent the lawfulness of the data processing, especially if the collected data is processed in a basically anonymous and aggregated form, as well as if its confidentiality and integrity are preserved across the transmission procedure.

In this way, it's possible to find an alternative to the consent-centred approach. Indeed, data anonymising goes beyond the reach of the GDPR (see Recital 26), given that a legal authorization for data processing is a sufficient justification for the same processing when carried out for public interest reasons in the field of public health (Artt. 6, 9, Par. 2, lett. i), Art. 23, Par. 1, lett. e), Recitals 41, 46 and 50).

Furthermore, consent, in addition to being technically unnecessary, [58] may

---

[57] *See* G. Fares, 'Artificial Intelligence in Social and Health Services: A New Challenge for Public Authorities in Ensuring Constitutional Rights', in M. Belov (ed.), *The IT Revolution and its Impact on State, Constitutionalism and Public Law* (Hart Publishing 2021) Chapter 15.

[58] P. Quinn, 'The anonymization of research data – a pyric victory for privacy that should not be

sometimes also prove to be counterproductive: suffice it to say that providing for its acquisition at all costs corresponds to the exercise of the rights under Art. 7 GDPR, among which is the right to the withdrawal of the same consent, with the risk of deleting the data previously collected and enhanced, which would have easily deducible detrimental effects at the expense of the planned public health purposes.

On the contrary, statutory coverage can prevent this type of effect to the extent that lett. *i*) of Art. 9, Par. 2, GDPR allows data retention by the manager, still without prejudice to the appropriate and specific measures to protect the data subject's rights and freedoms, particularly professional secrecy.

The last challenge is to balance fundamental rights and personal data protection, on the one hand, and the use of artificial intelligence tools to fight the spread of Covid-19, on the other hand. Taking into account that the outcome is necessarily influenced by the three following conditions: 1) the system is efficient as a whole and in its various components; 2) the legal basis of the app policy is adequate; [59] 3) the data driven solution is used in a legally correct way to counter the spread of the virus, considering that digital technologies can be used not only for diagnosis and prevention purposes but also for control and punishment of individual behaviours, such as missed compliance with preventative isolation from others or mandatory quarantine.

In fact, lockdown and social distancing are not the only counter-measures useful to fight health emergencies like Covid-19. In theory, a vast range of technological solutions can be implemented, which can also be used with the aim of monitoring infections. Having in mind the scheme of the three Ts – test, treatment and tracing – a contact tracing app combined with telehealth could be a good complementary solution. [60]

In order to get a positive evaluation, a contact tracing app must be in compliance both with the European model outlined by the Consortium PEPP-PT (Pan-European Privacy-Preserving Proximity Tracing) and the following other documents: 1) the recommendation of 8 April 2020 of the European Commis-

---

pushed too hard by the EU data protection framework?', in *European Journal of Health Law* (2017) 24, 14.

[59] Seeking a legal basis for the data processing carried out by a contact tracing app, firstly we must consider Art. 52 of the Nice Charter which provides that when restrictions on the exercise of rights and freedoms are to be adopted, they 'must be provided for by law and respect the essence of those rights and freedoms'. In the meantime, according to GDPR and e-Privacy Directive (no. 2002/58), a choice between two models of legal basis is needed: either the consent of the data subject to be expressed at the time of the installation of the app (Art. 5 of e-Privacy Directive and Artt. 8 and 9 of GDPR); or to resort to the public interest (according to Art. 15 of e-Privacy Directive and Art. 6, par. 1, let. d) and e) and Art. 9, par. 2, lett. i) of GDPR).

[60] *See* G. Fares, 'Health systems, fight against Covid-19 and digitalization: is global law the main way?' (2020) in <*www.iusetsalus.it*> 2 accessed on 08.10.2020.

sion which stated the need to adopt a Toolbox of shared measures in compliance with the current legislation; 2) the letter of 14 April 2020 from the European Data Protection Board (EDPB) to the Commission as it was on the verge of adopting the aforementioned guidelines; 3) the same Guidelines of the European Commission of 16 April 2020 regarding the use of contact tracing apps in which the principles of the GDPR (such as proportionality, consent to processing and data minimisation) are explicitly mentioned; and 4) the EDPB Guidelines of 21 April 2020, relating to the use of locationing data and contact tracing tools in the context of the Covid-19 epidemic. [61]

In other words, promoting a model of human-centred technology use is recommended, in which fundamental human rights are always guaranteed and avoiding any unnecessary and disproportional restriction of the freedoms and rights on which democracy is based. [62]

Basic requirements of the technology are to be respected. The health emergency must be faced respecting the main principles set up by domestic constitutions, national law and international law, especially regarding the protection of privacy and personal data. At the same time, it must be clear that technology is not neutral, depending on how it's developed and applied, so AI has to be 'ethical, transparent, safe and inclusive' and, moreover, functional to the needs of the human being.

The range of guarantees provided by the law is crucial as well. A data pro-

---

[61] The need to trace the contacts of the infected has been affirmed by WHO, *Report of the WHO-China Joint Mission on Coronavirus Disease 2019 (COVID-19)*, 16-24 February 2020, *https://www.who.int/docs/default-source/coronaviruse/who-china-joint-mission-on-covid-19-final-report.pdf*, according to which '*Immediately expand surveillance to detect COVID-19 transmission chains, by testing all patients with atypical pneumonias, conducting screening in some patients with upper respiratory illnesses and/or recent COVID-19 exposure, and adding testing for the COVID-19 virus to existing surveillance systems (e.g. systems for influenza-like-illness and SARI'*.

[62] As underlined by C. Colapietro, in C. Colapietro, A. Iannuzzi, 'App di contact tracing e trattamento di dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali' (2020) in <*www.dirittifondamentali.it*> 2 accessed on 08.10.2020, in order to contain the pandemic, the data driven Italian working group for the COVID-19 emergency didn't disregard the general principles of law, convinced that 'digital technologies and personal data could be used in a democratic way, for the benefit of the health of the community, respecting fundamental freedoms and rights'. Therefore, the action of the same group was inspired by the following principles: a) principle of transparency (considered as a fundamental pillar of our democracies even in emergency situations in which it's necessary to account even more for the use of financial and technological resources and for the actions carried out); b) protection of fundamental rights (this is always central since 'in democracy, even in emergencies, extraordinary responses are legitimate precisely because they are provided for by the ordinary legal regime and respecting inviolable guarantees'); c) principle of a responsible innovation, involving public institutions and private entities, together called to collaborate by sharing data in full respect of fundamental rights and freedoms; and d) principle of the data driven approach to face the health emergency using, in any case, an ethical approach centred on the human being, keeping in mind that the issue relating to human and social values must always be preserved and pursued.

tection impact assessment is required according to Art. 35 of GDPR, after prior consultation of the Authority for data protection (Art. 36 GDPR) and after adopting all technical and organisational measures suitable to guarantee an appropriate level of security compared to the risk taken by the data subjects and his or her rights and freedoms. Furthermore, it's important to ensure that the processing of data transferred outside of European Union boundaries does not go beyond the scope of application of the GDPR.

In practice, any automated system based on an alert to be sent to those who have come into contact with infected subjects can be approved if it is in compliance with the three rules set by the European Union about a contact tracing app: 1) use of Bluetooth technology and not geo-locationing; 2) anonymising; and 3) voluntary participation of the citizens.

On its side, Art. 5 of GDPR sets out the principles of lawfulness, fairness, transparency, purpose limitation, accuracy, data minimisation, storage limitation, accountability, integrity and confidentiality, all of which represent fundamental points of reference.

Other important rules are to be mentioned: a) the privacy information to be provided to the users before downloading the application related to the processing purposes, the pseudonymisation techniques and data retention; b) data processing must be carried out in an anonymous way, excluding the geo-locationing of the users pursuant to Art. 26 of GDPR, in order to prevent the identification or the re-identification of the data subject; c) confidentiality, integrity, availability and resilience of the processing systems and services; adequate measures to avoid the risk of re-identification of the data subjects must also be provided; d) the data retention is allowed for the period of time strictly necessary; thus, at the end of the state of emergency, all processed data must be deleted or made definitively anonymous; e) personal data can't be processed for further purposes, unless it is used in an aggregate and anonymous form for health purposes only for public, prophylaxis, statistics or scientific research pursuant to Art. 5, par. 1, let. a) and 9, par. 2, let. i) and j) of GDPR. [63]

Three further aspects relating to the functioning of the app are to be highlighted: a) the contact tracing system must preferably be managed by public authorities as controller and processor; [64] b) the user has freedom of choice as

[63] About the principle of purpose limitation, D. Rűcker, T. Kugler, *New European General Data Protection Regulation. A practitioner's Guide* (C.H. Beck - Hart - Nomos 2018) 53-65.

[64] Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (art. 4 GDPR). Many other entities (for example, hospital and local health care services) play a role as a data processor. Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (art. 4 GDPR). *See* P. Voigt, A. Von Dem

to whether he/she will or will not download the app; [65] and c) the contact tracing app is useful for the identification of asymptomatic patients. [66]

In closing, the main goal is to find and break the chain of infections. In this context, AI tools are very useful for virus tracing and for identifying and isolating the main sites of the infection. Therefore, the automated processing of data through contact tracing is necessary, using simple algorithms. This conclusion is in compliance with the GDPR that subordinates the lawfulness of processing to two alternative requirements: the need for processing or, as an alternative, the consent of the person concerned.

Buscche, *The EU General Data Protection Regulation (GDPR). A Practical Guide* (Springer International Publishing 2017) 80.

[65] No harmful consequences must be entailed for people who don't download the app, in any case having to apply the principle of equal treatment. *See* C. Colapietro (62) 783, who affirms that digital contact tracing is allowed for the only purpose of alerting people who have come into close contact with subjects found Covid-19 infected and so protect their health through the planned prevention health measures while the download is voluntary.

[66] This is why the contact tracing is necessary. Regarding the problem of asymptomatic patients, it has been estimated that 44% of secondary cases were infected during the index cases' presymptomatic stage or when the primary cases were asymptomatic. After all, according to WHO guidelines adopted on 13 March 2020, it's very important to immediately expand surveillance to detect COVID-19 transmission chains by testing all patients with atypical pneumonias or with negligible symptoms as well as patients not having symptoms yet and therefore not yet swabbed nor self-isolated. In fact, the high incidence of pre-symptomatic transmission can make the isolation practice ineffective in controlling the epidemic; in the same way, the manual contact procedures are not fast enough to counteract the spread of the virus.