Preface

The relationship between the right to health and the right to privacy has always been one of the most delicate and complex in the universe of the right to the protection of personal data.

During the pandemy – that is the historical, social, political and legal context in which this book was born – the above mentioned relationship lived hard times.

From 2004 to today, Italians have never questioned Google so much as in these days in relation to death. The same goes for health.

That is what Google Trends data say, the Google service that measures the users' online searches. Thus, everyone both in the public and private sphere say "health first". This approach has so influeced the relationship between the right to health and every other right, all on the same lavel, both in internal and international law.

It so happened that the right to health often found itself in opposition – in the political dialectic – to other freedoms and rights, first of all, the right to the protection of personal data.

It is in moments like these ones that rights – and in same way democracy itself – are fragile. Fundamental rights, also the most important ones, are facing the risk of being renounced, derogable for the pursuit of urgencies, emergencies, public and private needs such as the right to wellbeing and the right to life.

Nevertheless, it is woth noting that this opposition or antagonism is only apparent because, in fact, no right is "tyrant" and prevail over others. This is especially true during an emergency like the current one, where a right seems to be receding before others in the context of the political choices adopted by the so called "good government".

It is especially in these time that fundamental rights run the highest risks. As Louise Brandesis, at the time the Judge at the Supreme Court of the United States, said in his dissenting opinion into the first wiretapping trial in history: "Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dan-

gers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding" (Olmstead v. United States, 277 U.S. 438).

It was 1928 but that teaching is today more relevant than ever.

Defending our privacy in the face of despotic "evil-minded" government is easy, natural and instinctive to feel while it is difficult, unnatural, almost counter-intuitive to do so in front of a government that acts for beneficient purposes, or as to guarantee, at the highest possible level, the right to health of its citizens.

So, is this contrast essential?

The proper functioning aid system, both in ordinary and in emergency seasons, really presupposes the compression of the right to protection of personal data or between the right to data protection and the right to health there can be a symbiotic relationship, virtuous, complementary?

This book is interesting also because of – among the other reasons and the fact it was written in the middle of this rare, if not unique, time of pandemy – its style, the contents, the words or the approach to address the issue through the "lens of the law" and with scientific rigor without falling under the easy temptation of the political, emotional and social tensions of the moment.

This book's goal is not to answer that question or to dispel doubts which, however, were energically spread from the scientific community to public opinion in recent months. Nevertheless the comparative approach to the application and impact of the General Data Protection Regulation (GDPR) in different legal systems – in a necessarily limited period of time due to the age of the new discipline and dominated, to a significant extent, by the pandemic – makes it the valuable guide on these issues.

Moreover, apart of the tension – today stronger than ever – between the right to health and the right to the protection of personal data, this book also talks about the tension between new technologies and data protection. This is also a difficult issue to handle.

New technologies have a very strong impact on the life of citizens and State itself and, above all, on healthcare. Indeed, in a few years Big data, artificial intelligence and algorithms revolutionized medical research and diagnostics and gave an extraordinary contribution in the treatment of diseases. However, at the same time they also created new problems and undermined the rule of law and especially data protection law.

All of this, in the past have already animated debates, comparisons and scientific researches in the most disparate fields of bioethics. That is the reason why this book goes deep inside the "Health Law and Bioethics european network" project.

Are the new medical technologies enemies of data protection law? Without hesitation, reticence or any sort of ambiguity the book responds in a negative

way. Also in this case there is no opposition or contrast between technology and the right to privacy.

There are problems that need to be faced and resolved using data protection by design and by default principles first.

Furthermore, data protection can surely be an excellent ally of technology in order to save human life. That is because the European discipline on protection of personal data raises the level of data quality, avoiding the risk that discrimination, inequalities or other attacks to the human dignity that could derive from certain technologies.

It is not easy to find a "red line" running across a book rich with interesting topics like these. However, if we have to find the most important one, this is the clear conviction that the GDPR is the best current proof of that the new data protection rules do not represent and cannot represent an obstacle either to the promotion and protection of the right to health nor, even less, to the growing and increasingly effective use of new technologies, big data and artificial intelligence on the top.

The most important evidence of this thesis is just the Covid-19 pandemy where data protection did not hinder the design, development and use of contact tracing technologies and rather than has allowed these solutions to become global champions of a balanced approach between privacy and health. All of this was made guaranteeing to millions of citizens the right to health without having to give up their right to privacy.

It is not true that the more tecnology and less privacy you have the more healthcare you have as, unfortunately, we read all around us. Rather the opposite is true: the health technology and greater respect for human dignity allow a higher quality of mankind's life and existence.

Likely, this book's greatest merit, that transcends even the subject matter of investigation, is pointing to a method and an approach towards the constitutional and fundamental rights through which the right to data protection becomes an accelerator and amplifier of other rights and not their enemy.

Avv. Guido Scorza
Member of the Italian Data Protection Authority
(Garante per la protezione dei dati personali)

Section I

The general principles of the new EU Regulation 2016/679 and their implementation in the healthcare sphere

The general principles of the EU Regulation 2016/679 as a legitimacy's parameter of Member States' national legislations on personal data in a multilevel system of sources of law

Carlo Colapietro [*]

CONTENT: 1. Preamble. – 2. Purposes of the Regulation. – 3. Territorial and material scope of the Regulation. – 4. The dynamic concept of personal data subject to protection and the right to informational self-determination. – 5. General principles relating to the processing of personal data within the Regulation. – 6. Implementation of the Regulation in the Member States. – 7. The European Regulation as a legitimacy parameter of the national legislation on protection of personal data.

1. *Preamble*

Personal data protection is an individual's fundamental right. This right has been codified for a long time in the European legal area and is reaffirmed and strengthened today with the approval of the new Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and free movement of such data. The Regulation repeals Directive 95/46/EC (General Data Protection Regulation), in order to ensure a higher protection of a fundamental right, not only for European citizens, but for all the individuals in the European territory. [1]

[*] Full Professor of Public Law Roma Tre University, Department of Law.

[1] C. Colapietro, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale* (2018, 22) in <*https://www.federalismi.it/nv14/articolo-documento.cfm?Artid=37442*> accessed on 20.07.2019.

2. *Purposes of the Regulation*

The new Regulation on privacy arises from the awareness that although the objectives and principles of Directive 95/46/EC remain sound still today, this has not prevented fragmentation in the implementation of data protection across the Union, legal uncertainty or a widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity, as specifically stated in the Regulation in recital (9) thereof.

Therefore, the need for such a change, through the transition from the Directive to the Regulation instrument, is not accidental.

The first baseline provision – also for systematic matters – is Art. 1 (actually entitled 'Subject-matter and objectives') which, in Paragraph 1, provides that '[t]his Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.' Thereby it indicates, from the very beginning, a special attention to the time of the movement of data. This latter conclusion is substantiated by the following Paragraph 3 of the same Art. 1, where it provides that '[t]he free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data'.

Such provisions show a crucial transition from the rules previously in force. As opposed to what could be appropriate approximately 20 years ago, when Directive 95/46/EC was approved, today the European legislator has decided to drift away from the essentially static notion of the right to the respect for private life, where a radical negative protection was sufficient, and consisting of the power to remove third parties interferences (the well-known '*right to be let alone*' mentioned, at the dawn of the privacy protection, by S.D. Warren and L.D. Brandeis in their paper '*Right to privacy*', in *Harward Law Review*, 15 December 1890). In the season of global interconnection, allowed by the daily use of the Internet, it is no longer a matter of just protecting natural persons, but also their data and information. In order to do so, powers of intervention are needed: protection is not static anymore, but dynamic, and it follows data during their movement. [2]

Indeed, today, in the midst of the digital era, there is a widespread feeling that our personal data are constantly at risk, with the subsequent need for ensuring a homogeneous implementation of the rules on privacy across the European Union. In doing so, the aim is to create a context of reliability for citizens and establish a climate of trust for the economic development, especially in the *online*

[2] S. Rodotà, *Il diritto di avere diritti* (Laterza 2012) 397 et seq.

space, with the final purpose of facilitating the existence of a single EU-law market, where, today, the free movement of personal data plays a vital role. [3]

Therefore, to create a context of higher legal certainty and uniformity across EU Countries, time had come to realize '*one continent*, *one law*'; a sort of *ius commune* on privacy, which European Institutions have chosen to govern through the most effective legislative instrument in order to standardise the different national legislations: the Regulation. Such a choice most likely represents the most relevant result of the new rules on protection of personal data.

Naturally enough, the European legislator's intent to pursue these objectives is not hidden. Instead, it is specifically laid down within the 99 Articles of the same Regulation, and earlier marked in the 173 recitals thereof. Thereby the '*legal reasoning*' of the new Regulation [4] is expressed, and the guiding principles of the precise legislative intervention can be found, in view of their undisputed interpretation orienting role.

The major innovation elements of the new European rules on privacy are based on this background. The logical steps which have led to the adoption of this new legislation are clearly marked right within the various recitals of the Regulation, in view of which the whole complex of articles of the Regulation on privacy shall be read.

3. *Territorial and material scope of the Regulation*

On the basis of the final purpose of standardising the legislation on privacy across the European Union, among the most relevant provisions of the Regulation, we can number Art. 3, addressing the identification of the territorial scope of the new rules. [5]

The Regulation, in Art. 3(1), indicates a significant extension of the territorial enforceability of the new rules, in accordance with some decisive decisions of the Court of Justice of the European Union, which have preceded this legislative change (among the most well-known ones, those regarding the Cases C-131/12 *Google Spain* and C-362/14 *Scherms*).

Consequently, the new Regulation seems to have absorbed the conclusions

---

[3] L. Califano, 'Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali', in L. Califano, C. Colapietro (eds.) *Innovazione tecnologica e valore della persona Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679* (Editoriale Scientifica 2017) 3 et seq.

[4] F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679* (Giappichelli 2016) 8 et seq.

[5] D. Rücker, T. Kugler, *New European General Data Protection Regulation. A Practitioner's Guide* (Beck/Nomos/Hart 2018) 37 et seq.

of the EU case law, providing, at Art. 3, that the European legislation on privacy is fully applicable to a controller or processor acting in the Union, regardless of whether such processing has taken place in the Union or not (Paragraph 1). Furthermore, the legislator has decided to ensure the general applicability of the Regulation also to any processing of data, related to the offering of services to data subjects or the monitoring of their behaviour, as far as their behaviour takes place within the Union, even if not established in the Union territory (Paragraph 2).

In addition to the provisions on the territorial scope, the Regulation provides also provisions on the material scope of the new European legislation on privacy.

With such provision (Art. 2(1)), the European legislator has not drifted away from the provisions of the Directive previously in force. Nevertheless, the material scope of the Regulation naturally enough cannot be considered identical to the one of the previous rules, in view of some significant differences existing among the same terms – as 'personal data' or 'processing' – for the way in which they were defined in Directive 95/46/EC in comparison with their current meaning expressed in the Regulation. [6]

Moreover, Art. 2(2) of the new Regulation provides a 'negative' limitation of the material scope, by identifying a set of areas to which the rules of the Regulation do not apply. By this provision, some important derogations have been provided to the application of the new rules on processing of personal data.

Beyond the general exclusion of those activities falling outside the Union's competences (situation referred to in Art. 2(2)(a)), it is also provided that the rules of the Regulation do not apply when the processing of data is by the Member States carrying out activities regarding common foreign and security policy, governed by Chapter 2 of Title V of the TEU (situation referred to in Art. 2(2)(b)). What provided in Art. 2(2)(c), on the other hand, leads to wider interpretation issues, since it excludes the application of the new European rules on privacy to any purely personal or household activity: it is the so-called '*household exemption*', already provided in the previous Directive. The interpretation issues related to this provision result from the difficulty in determining when, in practical terms, an activity is purely personal or household. Beyond this specification, in law doctrine there are concerns about the decision not to provide a more effective protection for the activities on social networks, given that, nowadays, these latter represent one of the major channels through which the use of technologies, and thus the source of the most hazardous risks for the protection of privacy, is expressed. Lastly, Art. 2(2)(d)

[6] S. Simitis, G. Hornung and I. Spiecker Gen. Döhmann, *Datenschutzrecht* (Nomos 2019) 252 et seq.

provides that the Regulation does not apply to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This provision raises various questions in terms of the balancing between the protection of security on one hand, and the protection of privacy on the other.

The conclusion of Art. 2 of the Regulation is the clarification that the new rules do not apply to the processing of personal data by Union Institutions, bodies, offices and agencies, for which the specific provisions of Regulation (EC) 45/2001 apply, however stating that such specific provisions shall be adapted to the principles and rules of the new Regulation (Art. 2(3)).

4. *The dynamic concept of personal data subject to protection and the right to informational self-determination*

That one-way logic of privacy – exclusively addressing the controller-data subject relation, and on which basis the most traditional right to privacy, meant as the *right to be left alone*, has been established – is in crisis. This is consequent to the acknowledgement of the effect of the technological revolution on the concept of private sphere itself, which is no more, or not only, about phenomena of information going outside the domain of control, but it also involves flows from the outside inwards. In other words, it is the well-known transition from the *habeas corpus* to the *habeas data*.

In this respect, a comparison between Art. 1 of Directive 95/46/EC and the first provision of the new European Regulation is particularly significant. The latter, by removing any reference to the traditional concept of privacy (meant as the right to private life), seals the central role of the new element underlying the current legislative rationale: personal data.

The need for a perspective change had already been recorded in the EU primary law. Specifically, Art. 8 of the Charter of Fundamental Rights of the European Union had already complemented the most traditional right to private and family life (Art. 7) with the right to the protection of personal data. Traditionally, the best law doctrine has been able to perceive the virtues of such 'constitutionalisation', expressing a full right to "informational self-determination", which going beyond the static, and negative, protection of privacy, vests the controller with control and intervention powers on their data. [7]

Perhaps, these remarks are insufficient to highlight the *ratio* of the innova-

[7] S. Rodotà (2) 397 et seq.

tions included in the new European Regulation on privacy: technology has imposed a deep legal debate on the concept of personal data and protection logic. Indeed, the new European Regulation on privacy introduces, at Art. 4, a very extensive concept of personal data, according to which personal data "means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly".

The two elements that are certainly more significant within this definition lie in the ["choice of a concept of personal data at the edge of generality, but actually with a comprehensive function on one hand, and an ability to attract new circumstances which are not predicted nor *ex ante* predictable by the legislator"], [8] as well as in an increase in the considered cases of data identifying a person or making them identifiable. Such an extension of the concept of personal data is definitely representative of the European legislator's intent to increase protection circumstances, making the core principle of the right to informational self-determination at the basis of the whole structure of the Regulation.

5. *General principles relating to the processing of personal data within the Regulation*

Regarding the general principles relating to processing of personal data, Art. 5 of the new European Regulation replicates the content of Art. 6 of Directive 95/46/EC, whose principles had already been laid down in Art. 5 of Convention 108/1981 and transposed, almost verbatim, within Art. 11 of the Privacy Code previously in force.

Nevertheless, it should be underlined that, although a first reading of the new European rules on privacy seems to leave the catalogue of the principles of processing unchanged, it is necessary to note that the new Regulation includes the European experience of the latest 20 years, particularly regarding the conclusions of the Court of Justice of the EU and, primarily, the progressive transformation of the approach of the European Institutions to the matter, moving from a mainly market-driven setting, to a different, mostly fundamental rights-oriented, perspective. [9]

Going through individual principles, it may be noted that Art. 5 begins by

---

[8] S. Sica, 'Verso l'unificazione del diritto europeo alla protezione dei dati personali?', in S. Sica, V. D'Antonio and G.M. Riccio (eds.), *La nuova disciplina europea della privacy* (Cedam 2016) 5.

[9] M. Bassini, 'La svolta della *privacy* europea: il nuovo pacchetto sulla tutela dei dati personali', in *Quad. cost.* (2006) 588 pointing out the transition from a basically market-driven European legislation on free movement of personal data to a different, mostly fundamental rights-oriented perspective.

stating that "[p]ersonal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')". In particular, the lawfulness principle of processing is anchored in two alternative requirements: the need for processing, or the data subject's consent, to be non-generally expressed, but in relation with "one or more specified purposes".

Art. 5(1) then focuses on the other pillars of the self-determination power: the fairness principle and the transparency principle, which have to be expressed by means of an adequate policy statement, that ["serves the consensus-building and expression for a truly free and informed processing, as well as any exercise of all data subject's rights"]. [10]

The lawfulness right is joined with a further pillar of the rules on protection of personal data: the purpose principle, which represents a ["limit, intrinsic to the lawful processing of data"], assuming that personal data are ["exclusively processed in the scope of the purposes intended to be pursued and about which data subjects shall timely be informed through the policy statement"]. [11] Indeed, Art 5(1)(b) rules that "[p]ersonal data shall be collected for specified, explicit and legitimate purposes", which have to explicitly result from the policy statement, thus excepting that personal date are collected for some stated purposes but then used for others.

Finally, Art. 5(1)(c) states the necessity principle, provided in our law in Art. 3 of the Privacy Code previously in force. Although, under Art. 5 of the Regulation, the listing of the different processing criteria seems to separate the data minimisation/necessity principle both from the accuracy principle (Art. 5(1)(d)) and the storage limitation principle (Art. 5(1)(e)), in our opinion the first of these latter has a more general value, suitable to include the other two.

Indeed, the necessity principle requires that data consist of a relevance and adequacy link in respect of the purposes, so that data falling outside the predetermined purposes may not be collected. Particularly, on the basis of this principle, the activities of data processing shall comply with a "minimalist" criterion, minimizing the use of personal data where the same objectives can be pursued through anonymous data or data not allowing the immediate identification of the data subject. [12]

As already underlined with reference to the national rules on privacy,

---

[10] L. Califano, *Privacy: affermazione e pratica di un diritto fondamentale* (Editoriale Scientifica 2016) 63.

[11] *Ibidem*, 55.

[12] R. D'Orazio, 'Il principio di necessità nel trattamento dei dati,' in V. Cuffaro, R. D'Orazio and V. Ricciuto (eds.), *Il Codice del trattamento dei dati personali* (Giappichelli 2007) 20 et seq., who – through a forward-looking view on the implications entailed by this principle – highlights that it is a "minimalist" criterion which the activities of data processing shall comply with.

thereby the European legislator has transposed in the new Regulation the precaution principle, which applies to a time prior to processing and requires the controller to assess, *ex ante*, the relevance of the data in respect of the purpose. At the same time, the necessity principle is also the expression of that more general proportionality principle rising to "interpretative criterion" for the whole legislation on privacy, in the new European rules as well in the Italian Code.

However, the new European framework on privacy results furthermore characterised by principles, and subsequent establishments, aiming at enhancing the controller's accountability. Precisely for this reason, along with the abovementioned most traditional principles in the matter of processing, Art. 5 of the Regulation makes it positive – in addition to the integrity and confidentiality principle (Art. 5(1)(f)), becoming thus an actual requirement of processing – also the controller's accountability principle (Art. 5(2)), according to which the controller shall be compliant with and, at the same time, shall demonstrate such compliance.

Therefore, as correctly noted, ["the real revolution entailed by the Regulation is not in the legislative point basically [...], but in the approach to be necessarily adopted by those establishing their economic or administrative activity on processing of personal data"]. They are thus required to stop keeping reasoning in bureaucratic or formalistic terms and finally start taking their responsibilities related to the adoption of measures on the basis of the assessment of risks concerning the processing of personal data, in terms of the adverse effects on data subject's rights and freedoms. [13]

Definitely, this decision represents the most relevant result of the new rules on protection of personal data. Through it we finally come out ["from the logic of the mere formal fulfilment of the legal obligations, to reach an important cultural change"]. [14] Such result – through a better clarification of the establishments aiming at making the individuals' fundamental right to informational self-determination concretely achievable (right to access to their data, right to rectification, right to delete, right to restriction, right to object the processing of their data, and the profiling itself), as well a significant innovation, by the introduction of the right to be forgotten on one hand, and the right to data portability on the other – complements a significant strengthening of data

[13] G. Busia, L. Liguori and O. Pollicino, 'Nota introduttiva', in G. Busia, L. Liguori and O. Pollicino (eds.), *Le nuove frontiere della privacy nelle tecnologie digitali. Bilanci e prospettive* (Aracne 2016) 12, according to which ["the risk should not be meant as exclusively linked to the safety of personal data, but also to the protection of data subject's fundamental rights and freedoms, which today are even more at risk due to the tremendous amount of data and processing which may result invasive, discriminatory and forceful for legal or factual circumstances"].

[14] L. Califano (3) 35.

subjects' rights, almost symmetrically and with a strong innovation against the past, with the obligations borne by controllers, first of all the setting of the processing providing, since the beginning, the essential guarantees for the fulfilment of the requirements under the Regulation and the protection of data subjects' rights and freedoms.

This new approach of the European legislator to 'risk', risk 'assessment' and the subsequent risk 'management' is based on an innovative accountability principle, referred to in Art. 32 of the Regulation. The principle implies the ability to account for, which does not only result in a form of accountability of controllers and processors (where they have not put in place all the legal, organisational and technical measures in the matter of personal data), but this provision is especially able to transform ["the general principles of data protection in concrete policies and procedures defined at controller level, in compliance with applicable law and regulations"]. [15]

This principle aims at enhancing the adoption by data controllers of proactive behaviours and measures suitable to demonstrate and ensure the proper application of the European rules. This, in a perspective of preventive protection, based on several establishments included in an accountability perspective. Herein, at least two of such establishments are remarked since they are a full expression of the minimisation principle of the personal data subject to processing:

– *data protection by design* and *data protection by default* (Art. 25), according to which the controller is required to ["implement appropriate measures to effectively protect personal data at the time of the design of the processing processes and models, and to ensure the compliance with the necessity principle, during the processing activity"]; [16]

– the preventive so-called *data protection impact assessment* (Art. 35), according to which the obligation of the assessment, where the processing represents a "high risk to the rights and freedoms of natural persons", shall relate *also* to the necessity and the proportionality of the processing in relation with the purposes. [17]

---

[15] G. Finocchiaro, 'Introduzione al Regolamento europeo sulla protezione dei dati personali', in *Nuove Leggi civ. comm.* (2017) 4.

[16] L. Califano (3) 34 et seq.

[17] P. Voigt, A. von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide* (Springer 2017) 47 et seq.