EUROPEAN PHOTONICS ROADSHOW

Rising to the challenge of entering the MedTech Market
20th November 2018, Marseille
Palais du Pharo, 58 Boulver

Health Data processing and protection

An approach to the European Multi-level data protection system

Prof. Dr. Joaquín Sarrión Esteve

RyC Senior Research Fellow
Academic Secretary of IMI-ENS (Mixed Institute of Research – Health National School)
Academic Secretary of the Master in Legal Practice, School of Law
Universidad Nacional de Educación a Distancia (UNED)

GRUPO SOBRE INNOVACIÓN, INVESTIGACIÓN Y DERECHOS FUNDAMENTALES

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES

SUMMARY

1.- Previous: Actual challenges and trends, objectives and Methodology

2.- Overview of the Health Data Processing International Legal Framework

3.- Overview of the Health Data Procesing EU Legal Framework

1.–Previous: Actual challenges and trends, objectives and Methodology

✓ Actual challenges and trends in processing of health data

UNED

➢ *Big data challenges,* according to the European Commission Directorate-General for Health and Consumers Unit D3 e-Health and Health Tecnology Assesment, *The use of Big Data in Public Health Policy and Research*, 2014.

- Interpretation, propensity, correlations (searching quality)
- Standards and Interoperability
- Data Governance and Trust

➢ IoT- Internet on Things

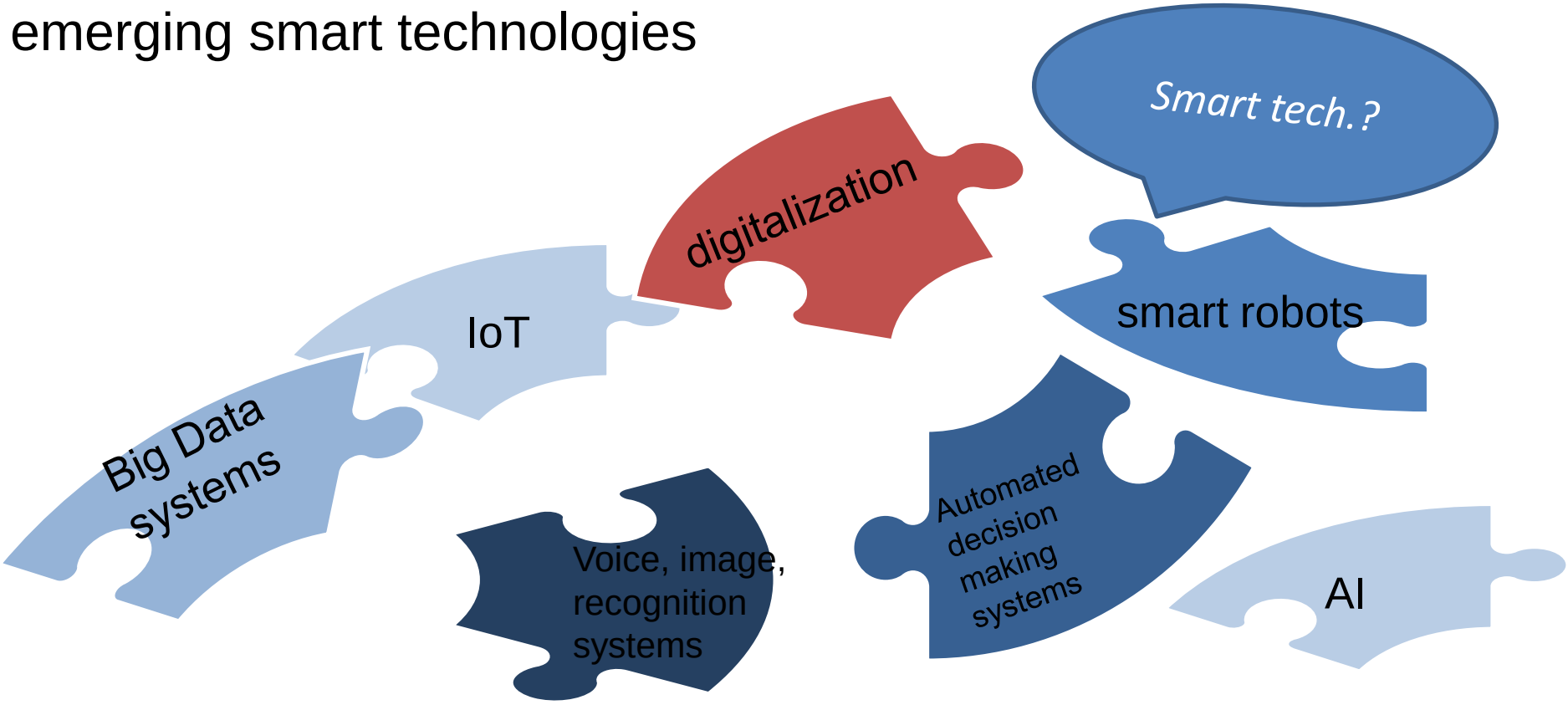
- m-Health (mobile- lifestyle and wellbeing apps)
- Mobile Medicine- The Internet of Things.

➢ Artificial Intelligence

Etc.

✓ Actual challenges and trends in processing of health data

➢We need to guarantee Fundamental Rights derived from emerging smart technologies



✓ Actual challenges and trends in processing of health data

➢ The EU has taken note of the challenges that AI (Artificial Intelligence) poses: *Resolution of 16 February 2017 on the need to draw up European civil legislation on robotics* (European Parliament, EP, 2017), that reflect *"the intrinsically European and universal humanistic values that characterise Europe's contribution to society"*.

➢The CoE outlined recently the complexity and rapidly evolving nature of the emerging technologies challenging regulation and human rights, in the Committee on Legal Affairs and Human Rights Opinion on 26 April 2017 (CoE, Committee on Legal Affairs and Human Rights , 2017:1) taking into account the *Report on Technological convergence, artificial intelligence and human rights* (Déaut, 2017), which exposed that:

✓ Smart tech. **can affect fundamental rights as Personal Data Protection, Rights to respect for private life, Human dignity, the Rights to Property, Safety, responsibility and liability, Freedom of expression, Prohibition of discrimination, Access to justice and the right to a fair trial**, etc.

✓ Actual challenges and trends in processing of health data

✓ **Searching for equilibrium**

❖ **Dignity (Personal Data Protection, Private life, etc.)**

❖ **Freedom of Research** (as a fundamental right), **Public Health…**

✓ Objectives

- To study the treatment or processing – including collection, recording, organisation, structuring, storage, and other uses – of personal data linked to health,
  - ✓under the International (European Council, like the Convention on Human Rights and Biomedicine) and European Union law framework (with reference to the European Charter of the European Union and EU legislation).

- Health treatment fields face ethical and legal problems regarding the use of personal data.
  - ✓Patients can benefit from having health or medical information available, and medical decisions can be more effective with a better understanding of clinical histories, medical and health data.
  - ✓But at the same time, we need to guarantee privacy rights – including data protection – and confidentiality, dealing with health data treatment challenges from a fundamental rights perspective.

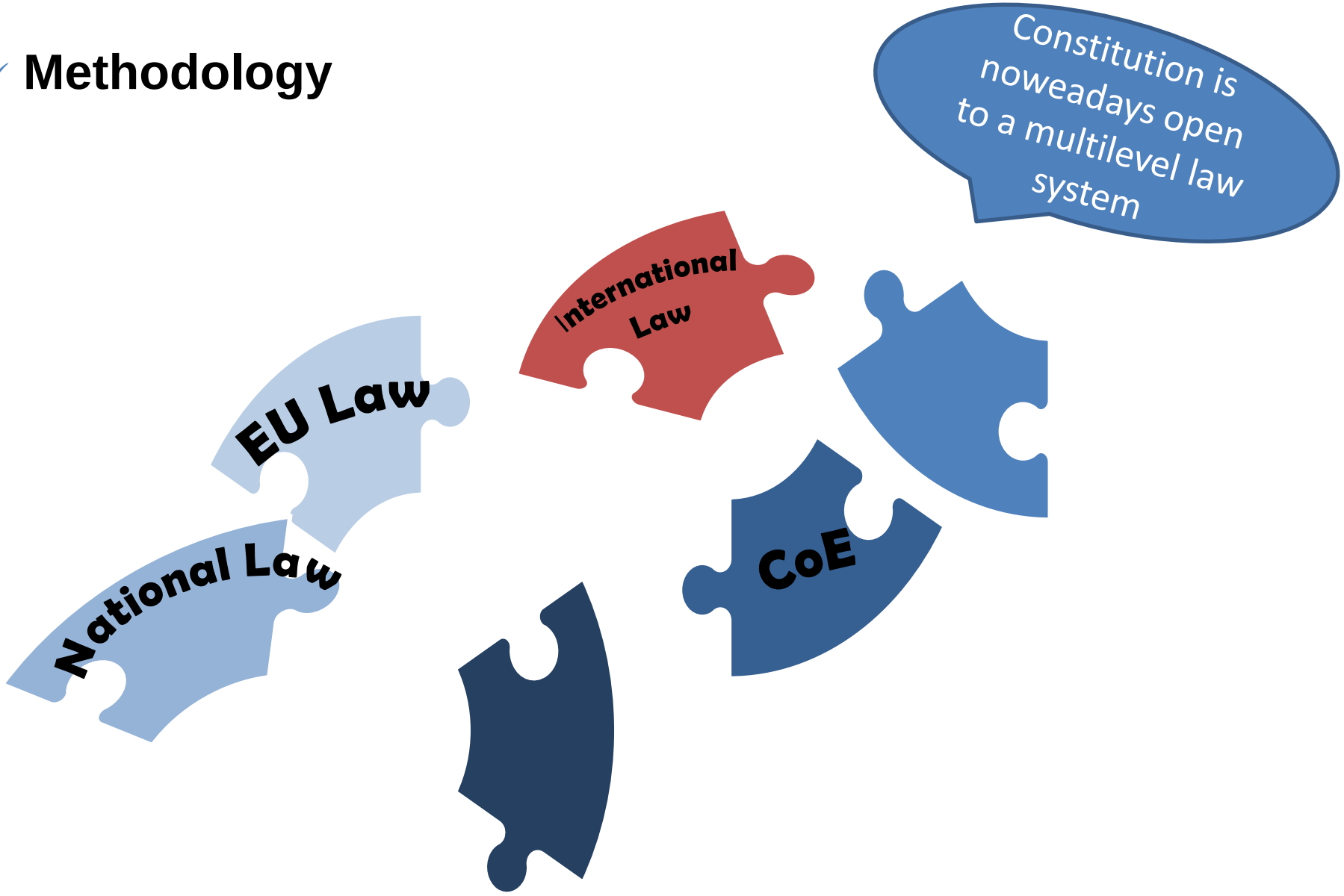
Methodology

- We live immersed in a European legal space based on a context of legal systems with different levels which are increasingly intervened (Gómez Sánchez, 2011: 20).

- Therefore we need a theoretical key to approach and try to study of any element or reality included in these legal systems, or better say, subsystems strongly related and integrated in a complex legal system.

- A good theoretical approach is the multi-level one, specially after the entry into force of Lisbon Treaty in 2009 when we can speak about a new constitutional horizon in the relations between EU law and national law, or rather a type of ***new constitutional and fundamental rights paradigm.***

✓ Methodology



Methodology

- Therefore we have:

  -External produced/approved Law (International as United Nations instruments, CoE instruments; and Supranational as EU law)

  -Internal produced/approved Law (national, regional, etc.).

- All this instruments and normative are part of the complex legal system wee need to apply.
- Fundamental rights standards application
  - International: **Coe Standard as Minimum standard of protection**
  - **National/EU Standard:** EU Fundamental Rights protection system is binding for EU member states not only when they implement EU law but in any case within the scope of EU law (*Åkerberg Fransson*, C-617/10), and the application of EU Fundamental Rights standard is binding, not allowing the application of the national one unless the EU law provides a margin to do so without questioning the primacy of EU law (*Melloni*, C-399/11; and *Åkerberg Fransson*, C-617/10) challenging the multilevel system.

2.-Overview of the Heath Data Processing International Legal Framework

Health Data Processing International Legal Framework

- ***United Nations***
  - ***Universal Declaration of Human Rights (UDHR),*** **10 December 1948. Article 12 (respect for private and family life).**

It is a milestone document in human rights protection adopted by the United Nations General Assembly. Although it is not a binding document, it can be an important source for the interpretation of the law. Article 12 provides for privacy:

'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'.

Health Data Processing International Legal Framework

- ***United Nations***
  - There are also other non-binding international instruments such as the **Universal Declaration on Bioethics and Human Rights** of 19 October 2005 (UDBHR) within UNESCO.

In particular, regarding privacy and confidentiality, article 9 UDBHR stipulates that:

'*The privacy of the persons concerned and the confidentiality of their personal information should be respected.* ***To the greatest extent possible, such information should not be used or discloses for purposes other than those for which it was collected or consented to****, consistent with international law, in particular international human rights law*'.

Health Data Processing International Legal Framework

- ***Coe***
  - ***ECHR*, 1950. Article 8 (right to respect for private and family life).** More importantly, due to its binding nature, provides in article 8 that:

    '1. Everyone has the right to respect for his private and family life, his home and his correspondence.
    2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

Health Data Proccesing International Legal Framework

- ***Coe***
  - ***ECHR*, 1950. Article 8 (right to respect for private and family life).**
    - ✓ The relevance of the ECHR is that any individual can ask for the protection of human rights recognised after the end of the national action.
    - ✓ EHRC had the opportunity to resolve questions on the issue of health data treatment under article 8 ECHR, as for example in the case *Z v. Finland* (1996) when EHRC called for a more careful scrutiny relating the disclosure of personal information from medical records without a patient's consent.
    - ✓ Privacy rights cannot restrict or limit the right to identity also covered by ECHR, case *Bensaid v. The United Kingdom* (2001). Privacy also includes the right to know the circumstances of those born and to establish the identity of the ascendants as a vital interest (*Jäggi v. Switzerland*, 2003).

Health Data Processing International Legal Framework

Coe

- **ECHR, 1950. Article 8 (right to respect for private and family life).**

  - ✓ The consent for health treatment or medical examination is essential (a precondition) to the implementation of health or medical treatment or examination unless it is a medical emergency. Therefore, it is also essential to the subsequent health data treatments.

  - ✓ Regarding persons not able to consent, such as minors or adults unable to consent, it is important to obtain the parent's or legal representative's consent. In this sense, the EHRC ruled in *M.A.K. and R.K v. United Kingdom* (2010) that a medical examination of a nine-year-old girl without the required parental consent was a violation of articles 8 and 13 ECHR.

Health Data Processing International Legal Framework

- ***Coe***
  - ***CoE Convention for the protection of individuals with regard to the automatic processing of personal data*** (No108), 1981.

- Based on article 8 ECHR, provides specific rules regarding the processing of personal data, it requires taking the necessary steps in the national legislation to apply its principles (art.4(1)), including:

1) Quality of data (art. 5): data shall be obtained and processed fairly and lawfully; **stored for specified and legitimate purposes and not used in an incompatible way; adequate, relevant and not excessive in relation to the sole purposes**; accurate and where necessary kept up to date; preserved in a way that permits identification no longer than is required for the storage purposes;
2) **Special safeguards for special categories of data, including personal data concerning health** (art. 6);
3) Appropriate security measures (art. 7);
4) **Safeguard rights for the data subject including access, rectification or erasure** of data (art. 8);
5) Special provisions for transborder data flows (art. 12).

Health Data Processing International Legal Framework

Coe

- *CoE Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine* (No. 164), 1994.

(Oviedo Convention)

- The purpose is precisely to serve as an instrument for the protection of human rights in the field of biomedicine
- One of the obstacles to its implementation is that **some relevant CoE States have still not signed it** (such as Germany, the United Kingdom or Russia) while others that have signed it have still not ratified it (Italy, Holland or Poland).
  - ✓ Notwithstanding, there was no obstacle for the EHRC to mention the Oviedo Convention in case law affecting those countries. EHRC 9 March 2004, *Glass v. UK*, Application no. 6187/00; 10 April 2007, *Evans v. UK* (GC), Application no. 6339/05, 23 March 2010, *M.A.K. and R.K. v. UK*, Application no. 45901/05 and 40146/06; 26 May 2011, *R.R. v. Poland*, Application no. 27617/04; 23 July 2015, *Bataliny v. Russia*, Application no. 10060/07; 27 August 2015, *Parrillo v. Italy* (GC), Application no. 46043/14

Health Data Processing International Legal Framework

- ***Coe***
  - *CoE Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine* (No. 164), 1994.

(Oviedo Convention)

- The Primacy of the human being (art. 2 Oviedo Convention).
- Equitable access to health care (art. 3 Oviedo Convention).
- Professional standards in the health field (art. 4 Oviedo Convention)
- **Free and informed consent in the health field** (arts. 5-9 Oviedo Convention).
- **Private life and right to information** (art. 10 Oviedo Convention).
- Non-discrimination on grounds of genetics (art. 11 Oviedo Convention).

Health Data Processing International Legal Framework

Coe

CoE Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (No. 164), 1994.

(Oviedo Convention)

- We shall only emphasise the relevance of free and informed consent as a requirement to health treatment, and therefore as a **previous precondition to subsequent health data treatment** (article 5 Oviedo Convention).

- **Persons unable to consent** (minors and adults without the capacity to consent) according to the national law, the intervention is only allowed if it is in their **direct benefit** (art. 6(1)Oviedo Convention) **with the authorisation of parents or legal representative**s, a person or body provided by the law (art. 6(2)and(3))

- **Private life** is protected in relation to the information about health (art. 10(1) Oviedo Convention), and **the patient is entitled to know any information collected about his/her health** (10(2) Oviedo Convention), **although this can be limited in the patient's interest** (art. 10(3) Oviedo Convention). Moreover, **there is no obligation to know the information** (art. 10(2))

3.-Overview of the Heath Data Processing EU Legal Framework

Health Data Processing EU Legal Framework

- **EU Law**
  - TEU, TFEU
  - EU Charter of Fundamental Rights
    - Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), OJ 1995 L 281
      - Regulation (EU) 2016/679 of EP and the Council on the protection of natural persons with regard to the processing of personal data on the free movement of such data (General Data Protection Regulation), **OJ 4.5.2016 L 119/1.** Art. 99: 1.This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. 2. It shall apply from **25 May 2018**.

Health Data Processing EU Legal Framework

EU Charter of Fundamental Rights

•The EUCFR recognises the principle of human dignity (article 1), the right to life (article 2), the right to the integrity of the person (article 3), the prohibition of torture and inhuman or degrading treatment or punishment (article 4), **respect for private and family life (article 7)**, **protection of personal data (article 8)**, the prohibition of all discrimination including that of genetic characteristics in an express way (article 21).

•It is particularly relevant to outline **article 3** EUCFR, since it recognises the right of everyone to respect his or her physical and mental integrity. Article 3(1) states that '**in the fields of medicine and biology**, the following **must be respected** in particular' (article 3(2)):

> ***'(a) the free and informed consent of the person concerned****, according to the procedures laid down by law;*
> *(b) the prohibition of eugenic practices, in particular those aiming at the selection of persons;*
> *(c) the prohibition on making the human body and its parts as such a source of financial gain;*
> *(d) the prohibition of the reproductive cloning of human beings'.*

A new Regulation: the General Data Protecion Regulation

Private Data Directive 1995

- Members States adopted the Directive, but there are important diferences in the implementation.
- It does not take into account new technologies.

New EU General Data Protection Regulation 2016

- It will apply directly to Member States
- Obj: Harmonization
- Takes into account new technologies
- 28 May 2018

Data Processing EU Legal Framework

General Data Protection Regulation

Definitions:

‘**Personal data**’ means **any information relating to an identified or identifiable natural person (‘data subject’)**; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

‘**processing’** 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;

‘‘**profiling**’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Data Processing EU Legal Framework

General Data Protection Regulation

Definitions:

‘**pseudonymisation**’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

‘**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;

‘**processor’** means a natural or legal person, public authority, agency or other body **which processes personal data on behalf of the controller**

General Data Protection Regulation

Lawfulness of processing (art. 6 GDPR)

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given **consent** to the processing of his or her personal data **for one or more specific purposes**;

b) processing is necessary for the performance of a **contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for **compliance with a legal obligation** to which the controller is subject;

d) processing is necessary in order **to protect the vital interests of the data subject or of another natural person**;

e) processing is necessary for the performance of a **task carried out in the public interest or in the exercise of official authority** vested in the controller;

f) processing is necessary for the **purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights** and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

General Data Protection Regulation

Conditions for consent (art. 7 GDPR)

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

Data Treatment EU Legal Framework

•The DPD and GDPR stipulate as a **general rule the prohibition of the processing of sensitive data** [revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of **genetic data, biometric data** for the purpose of uniquely identifying a natural person, **data concerning health** or data concerning a natural person's sex life or sexual orientation] (art. 8(1) DPD, art. 9(1) GDPR) except in some situations (art. 8(2) and (3) DPD, and art. 9(2) GDPR).

•The new GDPR introduces **genetic and biometric data**, as particular data (different from health data) and provides the same protection, and permits Members States to introduce further conditions about genetic, biometric and health data.

Data Treatment EU Legal Framework

✓‘**Genetic data**’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question (art. 4(13) GDPR).

✓‘**Biometric data**’ are defined as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (art. 4(14) GDPR).

Data Treatment EU Legal Framework

- The GDPR stipulates as a **general rule the prohibition of the processing of sensitive data** except in some situations, art. 9(2) GDPR).

(…)

'(h) processing ***is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services*** *on the basis of Union or Member State law* ***or pursuant to contract with a health professional*** *and subject to the conditions and safeguards referred to in paragraph 3;*

(i) processing ***is necessary for reasons of public interest in the area of public health****, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; L 119/38 EN Official Journal of the European Union 4.5.2016*

(j) ***processing is necessary for archiving purposes in the public interest****,* ***scientific or historical research purposes or statistical purposes*** *in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data* ***subject****'*. (Emphasis added by the author)

Health Data Treatment EU Legal Framework

General Data Protection Regulation

- Do we need a consent or authorization in order to the health data processing?

  - One might ask whether in these cases consent or authorisation is needed (art. 6.1(a) GDPR) or we should not apply this provision.

    ✓Beltran Aguirre (2017) argues that with independence of the anonymisation the consent is not necessary.

    ✓My interpretation is that the processing of health data for these purposes can be covered by consent (art. 6.1(a) GDPR), or any other principles of art. 6(1) but we need to be covered by one of them: art . 6(1) as the protection of the vital interests of the data subject or another person (art. 6.1(d) GDPR), legitimated interest of the medical centre or hospital (art. 6.1(f**) guaranteeing fundamental rights and interests** GDPR) , **for compliance with a contract** (6.1 (b) GDPR) **medical or health preventive treatment under employment contracts or health insurances contracts**, or a **legal obligation** (art. 6.1(c) covered by health or social management legislation, or for the performance of a task carried out in **the public interest or in the exercise of official authority** (art. 6.1(e) GDPR). But is is unclear.

    Article 3(2)a) EU Charter?

    ✓Bombillar Sáenz (2017) argues to introduce the consent requirement at national level to guarantee an adequate privacy protection security (art. 9.2.j) GDPR)

Health Data Treatment EU Legal Framework

General Data Protection Regulation

General principles when processing data in the same way (according to art. 5 GDPR):

1) **Principle of lawfulness, fairness and transparency**. Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (art. 5.1(a) GDPR).

2) **Principle of purpose limitation**. Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; **further processing for archiving purposes in the public interest, scientific or historical, research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purpose** (art.5.1(b) GDPR).

3) **Principle of data minimisation**. Processing shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (art. 5.1(c) GDPR).

4) **Principle of accuracy**. Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (art. 5.1(d) GDPR).

General Data Protection Regulation

5) **Principle of storage limitation.** Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (art.5.1(e) GDPR).

6) **Principles of integrity and confidentiality.** Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (art. 5.1(f) GDPR)

7) **Principle of accountability.** The controller shall be responsible for, and be able to demonstrate compliance with previous obligations, paragraph 1 art. 5 (art. 5(2) GDPR).

- ✓ It is important to outline that **the principle of accountability is a new principle, the controller has to prove that he or she respects the above principles** (the burden of the proof is with him or her).

Health Data Treatment EU Legal Framework

General Data Protection Regulation

On the processing of data, the patient or data subject has several **rights (art. 89 provides for limit this rations via national and EU law)**

1) **Right to access** (art. 15 and recital 63 GDPR). Access to your own personal data, including your medical record, and request a copy (the controller can charge a fee). The New General Regulation regulates remote ways to provide access to data, in this case the information shall be provided in a commonly used electronic form.

2) **Right to rectification** (art. 16 GDPR). Rectification of inaccurate personal data concerning him or her.

3) **Right to be informed** (arts. 13 and 14 GDPR). Right to be provided in a concise, transparent, intelligible and clear and plain language some information as the identity and detailed contact of the controller, -the purposes of the processing, the recipients of personal data, the period of storement, the existence of the rights to access, the existence of automated decision-making; and if the information has not been obtained from the data subject, the source of the data.

4) **Right to erasure** (including right to be forgotten) (art. 17 GDPR). Right to obtain the erasure of personal data when the personal data are no longer necessary –this provision, we think, is difficult to apply to health data, in fact we deal with an exception below –, have been unlawfully processed, for compliance with a legal obligation, etc.

Exceptions ex art. 17: the processing is necessary for legal compliance, for reasons of public interest in the area of public health, for archiving purposes in the public interest or historical or scientific research purposes or statistical purposes, for the establishment, exercise or defense of legal claims.

Health Data Treatment EU Legal Framework

General Data Protection Regulation

On the processing of data, the patient or data subject has several **rights:**

6)**Right to object** (art. 21 GDPR). Right to object to the data processing if the processing is based on public interest (art. 6.1(e), for the legitimate purpose of the controller (art. 6.1(f) GDPR), or in the context of direct marketing, or based on the ground of scientific or historical research purposes or statistical purposes unless the processing is necessary for public interest reasons.

7**) Right to communication of a personal data breach** (art. 34 GDPR).

8) **Right to lodge a complaint with a supervisory authority** (art. 77 GDPR).

9) **Right to an effective judicial remedy against a controller or processor** (art. 79 GDPR).

10) **Right to a compensation and liability** (art. 82 GDPR). Right to receive compensation from the controller or processor for the damage suffered (material and non-material damage) as a result of an infringement of the GDPR.

Health Data Treatment EU Legal Framework

General Data Protection Regulation

DPO

•One of the most interesting parts of the new GDPR is the binding figure of the **Data Protection Officer** (DPO). Certainly, the DPD allows the possibility for national law to provide that controllers may appoint an official to act as a personal data protection officer (art. 18(2) DPD). The objective is to ensure the respect to the rights and freedoms of the data subjects in the processing operations. However, this figure was only included (as far as we know) in the German Federal Law on Data Protection.

•Actually, the new regulation (GDPR) introduces this interesting figure in arts. 37, 38 and 39. The controller, and as far as we know, the processor shall designate a DPO in any case where (art. 37):

a) The processing is carried out **by a public authority or body**, except for courts acting in their judicial capacity;

b) **The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data** subjects on a large scale; **or**

c) **The core activities of the controller or the processor consist of processing a large scale of special categories of data pursuant to art. 9 GDPR (including health data)** and personal data relating to criminal convictions and offences referred to in art. 10 GDPR.

General Data Protection Regulation

DPO

• The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks of art. 39 (art. 37(5) GDPR). And may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract (art. 37(6) GDPR).

• The DPO will be a very relevant figure in the future from the point of view of fundamental rights protection regarding the processing of data, including health ones, and it will be very important to guarantee the highest position in the structure to allow him or her to develop the assigned attributed tasks

Codes of conduct

•The promotion of codes of conduct regarding the processing of personal data, including health ones, are included both in the Directive (art. 27 DPD) and in the GDPR (article 40).

•However, the GDPR goes further including the promotion, in particular at the EU level, of the establishment of **data protection certification mechanisms and of data protection seals and marks for the purpose of demonstrating compliance with this Regulation** (art. 42 GDPR) **with a voluntary character** and a transparent process.

Many thanks for your attention.

Prof. Dr. Joaquín Sarrión Esteve

RyC Senior Research Fellow ,
Universidad Nacional de
Educación a Distancia (UNED)

Twitter: @joaqsarrion
https://about.me/joaquinsarrion