



Health and Artificial Intelligence in the context of COVID-19 and beyond

Susana Navas Navarro*

ABSTRACT: This article introduces the main relevant aspects of ehealth or “digital health.” In this regard, by way of an introduction, the concept of health is addressed. In the second section, the core of this article, different aspects regarding the relationship between health and technology (HealthTech) are highlighted. Next, the importance of technology in order to deliver a preventive and personalized medicine, tailor-made to each patient, is addressed. Then, in the fourth section, some discriminatory situations that may arise due to not being able to access technology are discussed. Finally, I make some remarks regarding the so-called “Internet of Bodies.”

KEYWORDS: Health – technology – Artificial Intelligence – discrimination – civil liability.

*Professor of Civil Law at Universitat Autònoma de Barcelona (Barcelona, Spain).

1. Introduction. What is “health”?

The term “*health*” presents two different meanings. First, “*health*” can mean “*the state of complete physical, mental and social well-being and not merely the absence of disease and infirmity.*” This definition was developed by the World Health Organization (WHO) in its founding Charter in 1946.¹ The second meaning of “*health*” concerns all the activities aimed at preventing diseases, promoting recovery, and preventing both individual and collective diseases. In other words, it refers to what has traditionally been known as “*healthcare services*”, which can be delivered in national or private settings. The expression “*healthcare services*” embraces all services concerning “*healthcare*,” that is, “*health-related services provided by health professionals to patients to assess, maintain or restore their health, including the prescription, dispensation and provision of medicinal products and medical devices*” (Art. 3 lit. a Directive 2011/24/EU, of the European Parliament and of the Council, of 9 March 2011, on the application patients’ rights in cross-border healthcare²).

On the other hand, “*health services*” are excluded from the scope of application of Directive 2006/123/EC, of the European Parliament and of the Council of 12 December 2006, on services in the Internal Market³ (Art. 2 lit. f). Recital no. 22 of this Directive states that: “*The exclusion of healthcare from the scope of application of this Directive should cover healthcare and pharmaceutical services provided by health professionals to patients to assess, maintain or restore their state of health where those activities are reserved to regulated health profession in the Member States in which the services are provided.*” The exclusion applies regardless of the healthcare facilities, in which services are provided, how they are organised and financed at a national level, or whether they are public or private.

2. HealthTech

2.1. Definition of eHealth

The so-called “*eHealth*” or “*electronic health*” has been defined in different ways.⁴ At present, it is a term that enables the understanding between health professionals and the health technology industry.⁵ The different meanings that have been suggested, represent a new way of thinking, understanding, and living health on the side of individuals, whether they are citizens, health professionals, or public authorities.⁶

Electronic health can be defined as the set of health services provided remotely using information and communication technologies and and Artificial Intelligence (hereinafter, “AI”) systems that are compatible and interoperable.⁷ In fact, even without having fully implemented electronic health, we are already transcending it, moving

¹ The quote comes from the Preamble to the Constitution of the World Health Organization, which was adopted by the International Sanitary Conference, held in New York from June 19 to July 22, 1946, signed on July 22, 1946 by the representatives of 61 States (Official Records of the World Health Organization, no. 2, 100), and entered into force on April 7, 1948. The definition has not been modified since 1948 www.who.int, accessed February 2021).

² OJ L 88/45, 4.4.2011.

³ OJ L 376/36, 27.12.2006.

⁴ Hans Oh *et al.*, “What is eHealth (3): A systematic review of published definitions”, *J Med Internet Res*, v. 7, no. 1 (2005): e1.

⁵ eHealth Taskforce, “Accelerating the development of the eHealth Market in Europe”, eHealth Taskforce Report, 2007, 10.

⁶ Gunther Eysenbach, “What is e-health?”, *J Med Internet Res*, v. 3, no. 2 (2001): e20.

⁷ Jelena Madir, “Using technology to deliver health services”, in *HealthTech. Law and Regulation*, ed. Jelena Madir (Cheltenham: Edward Elgar, 2020), 3; Juan Alejandro Martínez Navarro, *El régimen jurídico de la salud electrónica* (Tirant lo Blanch: Valencia, 2018), 39.

towards what we could call “*digital health*,” in which AI and its different applications will have much more weight. This scenario’s benefits permit us to see AI as an essential tool – almost as a “*colleagué*” – for physicians or healthcare services.⁸ AI is already becoming a reality in radiotherapy, imaging, tomography, ultrasound, digital pills,⁹ and many other examples.¹⁰

Two aspects, in my opinion, are key in order to understand the success that the application of technologies to health is having: the first deals with the cost savings (*efficiency*) that these technologies mean for the National Health Services without diminishing the quality of service,¹¹ and the second aspect concerns the possibility of health reaching areas, where access to medical care is greatly difficult (e.g., rural areas, developing countries), thanks to the presence of devices and, particularly, mobile phones.¹² Therefore, health services can even be delivered beyond the borders of the country where the services and patients are located.¹³

A feature that stands out in electronic health is the fact that it is clearly focused on the individual user of the health service becoming an active subject, who takes control of his or her own health, in a kind of *peer-to-peer* communication with the professional who attends him. The use of the most varied communication and information technologies in healthcare means that the individual (*e-patient*) must take responsibility for their own health insofar as she should know, on the one hand, how the technology works and, on the other hand, should make decisions based on the information that the technology, applied to his or her specific case, provides. In this regard, electronic health “*empowers*” the user of the healthcare system.¹⁴ The European Data Protection Supervisor has stated, in its Opinion 1/2015, regarding mobile health, that better services are delivered at a lower cost, patients are empowered, and they get access to medical services and medical records in an easier and faster way.

⁸ COCIR, “Artificial Intelligence in EU Medical Device Legislation”, September, 2020, https://www.cocir.org/fileadmin/Position_Papers_2020/COCIR_Analysis_on_AI_in_medical_Device_Legislation_-_Sept_2020_-_Final_2.pdf. accessed: February 2021. See: Roland Wiring, “Artificial Intelligence in Healthcare”, in *HealthTech. Law and Regulation*, ed. Jelena Madir (Cheltenham: Edward Elgar, 2020), 144-166.

⁹ In November 2017, the FDA had approved the first use of a “digital pill” that communicates from the patient’s stomach through sensors to their *smartphone* or via the internet with the physician. A year earlier, the same institution had approved the use of an “artificial pancreas” [Andrea M. Matwyshyn, “The Internet of Bodies”, *Wm. & Mary L. Rev.*, v. 66, no. 77 (2019): 81-82].

¹⁰ COCIR, “Use cases – Artificial Intelligence in Healthcare,” <https://www.cocir.org/media-centre/publications/article/cocir-use-cases-artificial-intelligence-in-healthcare.html>, accessed February 2021.

¹¹ In the resolution of WHO, WHA58.28, it is stated that “*eHealth is the cost-effective and secure use of information communication technologies (ICT) in support of health and health related fields, including healthcare services, health surveillance, health literature, and health education, knowledge and research*” (Global Observatory for eHealth OMS, “Global diffusion of eHealth: Making universal ehealth coverage achievable”, December 2016, https://www.who.int/goe/publications/global_diffusion/en/, accessed February 2021).

¹² Global Observatory for eHealth OMS, “Atlas of eHealth country profiles 2015. The use of ehealth in support of universal health coverage: based on the findings of the third global survey on eHealth 2015”, accessed February 2021, <https://www.who.int/publications-detail/atlas-of-ehealth-country-profiles-the-use-of-ehealth-in-support-of-universal-health-coverage>. Also, see: Sojib Bin Zaman *et al.*, “Contexts and opportunities of e-Health technology in Medical Care”, *Journal of Medical Research and Innovation*, v. 1, no. 2 (2017): AV1-AV.

¹³ At least this is one of the purposes of the European Commission in its *Communication regarding the achievement of the digital transformation of health and care services in the Digital Single Market, the empowerment of citizens and the creation of a healthier society*, COM (2018) 233 Final.

¹⁴ There are, however, some other concerns that I address in my book: *Salud e Inteligencia Artificial desde el Derecho Privado* (Granada: Comares, 2018), 83-86.

The application of technology to health focuses on three fields: (a.) firstly, on health professionals; (b.) secondly, on hospitals and healthcare centers and, (c.) finally, on the relationship between the professional and healthcare service users.

a) The former embraces a whole series of tools concerning clinical information systems to be managed within the institutions in which health professionals work, such as, for example, digital radiological information systems, computer programs for diagnosis and treatment proposal in case of certain diseases using AI (e.g., Watson from IBM), or electronic pharmaceutical information systems. It also includes the training of health professionals, who are challenged by emerging technologies (*e-learning*). Some of these, up to now, have significantly improved their results due to the application of AI, which has allowed, among other aspects, the communication between machines (internet of things, IoT), the sending of personal health data to a data center located in a hospital, clinic or public institution or the transfer of these data between healthcare centers for a better diagnosis and treatment proposal, the existence of virtual assistants or chatbots, robotic surgery, nanotechnology and the use of 5G infrastructure in remote surgical operations. It could be argued that AI application and, particularly, *machine learning*, in the healthcare field, can serve, on the one hand, as a tool that proposes, recommends, analyses images, distributes resources, or acts as a second opinion for diagnosis and treatment of diseases with control remaining with the health professional and, on the other hand, as his or her substitute¹⁵ such as the image recognition algorithm, which can carry out the work currently performed by pathologists and radiologists.

b) The second referred area includes the electronic integration of information and distribution systems, both at a regional and national level, including the patient's digital records,¹⁶ the electronic prescription for drugs, or the request for electronic medical certificates. Likewise, the secondary use of health systems should be included, that is, systems related to access to medical information, education, for instance, online portals where it can find reliable medical information (such as the relevant Medscape),¹⁷ intermediary platforms, call centers for citizen assistance in case of emergencies or administrative procedures related to health carried out electronically and remotely.

c) In relation to the third highlighted area, telemedicine¹⁸ and the remote care of the patient, who is at home, are crucial.¹⁹ Particularly, it handles mobile health (*mHealth*)

¹⁵ Christian Katzenmeier, "Big Data, E-Health, M-Health, KI und Robotik in der Medizin", *MedR*, v. 37 (2019): 270; Heinz-Uwe Dettling, "Künstliche Intelligenz und digitale Unterstützung ärztlicher Entscheidungen in Diagnostik und Therapie -Arzt- arzneimittel- und medizinerrechtliche Aspekte", *PharmR* (2019): 633 et seq.; W. Nicholson Prize II, "Artificial Intelligence in Health Care: applications and Legal Implications", *The Scitbec Lawyer*, v. 14, no. 1 (2017), <https://ssrn.com/abstract=3078704>.

¹⁶ The EU has established the *European Health Data Space*, one of whose aims is to create a standardized electronic medical record system common to all member states. In addition, it is developing principles, which manufacturers of AI-based systems must comply with in order to be considered these systems "medical devices" (COCIR, European Health Data Space. Towards a better patient outcome, November 2019, https://www.cocir.org/fileadmin/Publications_2019/19106_COC_EU_Health_Data_SPACE_web.pdf).

¹⁷ See: www.medscape.com, accessed February 2021.

¹⁸ According to WHO, telemedicine is defined as: "the delivery of healthcare services, where distance is a critical factor, by all healthcare professionals using information and communication technologies for the exchange of valid information, for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of healthcare providers, all in the interests of advancing the health of individuals and their communities" (WHO Guidelines, "Recommendations on Digital Interventions for Health Systems Strengthening", 2019).

¹⁹ European Commission, Communication from the Commission to the European Parliament, the

using medical (or non-medical) *apps*, that is, *apps* for health purposes on *smartphones*, *wearables* and other devices, teleconsultation, teleradiology, and, in general, remote patient monitoring.²⁰ Recently, remote monitoring of patients has been used in the fight against COVID-19. As an example, California-based start-up VivaLNK has designed a multifunctional remote patient control system together with Alibaba to monitor temperature, electrocardiogram, respiration, heart rate, movement, reducing the possibility of infection for healthcare practitioners who are found in health centers, hospitals, or clinics.²¹

On the other hand, all the data obtained in an unstructured way, conveniently anonymised and aggregated, are the raw material of data analysis (*Big Data*) that, in the field of medicine, has the purpose of preventing future health risks based, among other aspects, on the individuals' lifestyle, giving birth to the so-called "*predictive and preventive medicine*."²² Smart devices' data are the raw material from which AI-based systems with learning capability, analysing a large data volume, can predict some diseases or extract several behavior patterns in relation to, nowadays, COVID-19. They can also analyse the results of experiments that have been carried out in search of an effective vaccine or for the production of new drugs.²³ The importance of *Big data* is unmatched, for several reasons, due to the speed at which it allows scientists to work and to the reduction in time in order to get a diagnosis.²⁴ In this regard, it should be mentioned that 5G technology, which provides a technological infrastructure, is more than necessary, in times of COVID-19.

2.2. Approaching *mHealth*

Electronic health embraces mobile health or *mHealth* as one of its poles.²⁵ It can be described as the implementation of digital health services through mobile devices, including *smartphones*, *tablets*, and other *wearables* (also called "*wearable technology*") such as bracelets, glasses,²⁶ footwear or clothing, in which an *app* is downloaded. *Apps* are specific computer programs that may or may not have a medical or health purpose.²⁷ One of the defining features of *mHealth* is its "*mobility*," that is, the availability, anywhere and at any time, of health data for the user (patient), even for healthcare professionals and

Council, the European economic and social Committee, and the Committee of the regions, on telemedicine for the benefit of patients, healthcare systems and society, COM (2008) 689 final.

²⁰ Frederic Vannieuwenborg *et al.*, "Bringing eCare platforms to the market", *Informatics for Health and Social Care*, v. 42, no. 3 (2017): 207-231.

²¹ Tony Bitzonis, "VivaLNK Partners with Alibaba on Remote Patient Monitoring System", FindBiometrics, March 3, 2020, <https://findbiometrics.com/biometrics-news-vivalnk-partners-alibaba-offer-remote-patient-monitoring-system-030301/>.

²² Ziad Obermeyer and Ezekiel J. Emanuel, "Predicting the future – Big Data, Machine Learning and Clinical Medicine", *N Engl J Med.*, v. 375, no. 13 (2016): 1216-1219; Alberto Urueña López *et al.*, "Big Data en salud digital. Informe de resultados," REDES, accessed February 2021, <https://www.ontsi.red.es/sites/ontsi/files/Informe%20Big%20Data%20en%20Salud%20Digital.pdf>.

²³ This is the case of the start-up *Insilico Medicine*, which, using Artificial Intelligence, is developing molecules that allow creating drugs to fight COVID-19 (see www.insilico.com, accessed February 2021).

²⁴ Thus, the *start-up* Infervision has developed a tomography system using machine learning that allows detecting the existence of coronavirus very quickly.

²⁵ Jelena Madir, "Using", 7-9.

²⁶ *Wearables* with sensors (VivaLNK) have been used by the Shanghai Public Health Clinical Center to combat the spread of the coronavirus in China.

²⁷ Tom Chakraborti, "Regulation and Governance of HealthTech", in *HealthTech. Law and Regulation*, ed. Jelena Madir (Cheltenham: Edward Elgar, 2020), 26.

healthcare centers.²⁸ The other characteristic is connectivity. In fact, it is often referred to as “*connected health*,” “*wireless health*”²⁹ or even “*digital health*,” one of its components being “*mobile health*,” to refer to remote health services including “*assisted living*.”³⁰

In this day and age, mobile health allows the user to monitor the heart rate, blood glucose level, blood pressure, body temperature (as seen in the case of COVID-19), and brain activity. There are also *apps* in the field of health applied to remembering taking of medicine prescribed by a physician, aiming to help to manage emotions³¹ or apply to fitness (e.g., such as those that measure the steps taken or the daily kilometers walked), to our well-being (e.g., the number of cigarettes smoked) and nutrition. *Apps*, which monitor the lifestyle and well-being of the user or wearer can be connected to a health service, or they can possess some sensors that allow the communication of data to the health service, to personalised medical guidance, or enable access to telemedicine throughout a wireless connection.³²

In general, these *apps*, provide quick and agile information to the data carrier about his health, in addition to speeding up medical treatment, where appropriate, and the interaction between health professionals and health service users.³³ Consequently, it implies the management of health data, with different objectives, such as the provision of medical, public health, research, educational, economic, and social services, the traceability of people, or the management of the health national system quality.³⁴

The WHO has defined the health mobile or *mHealth* as “*medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices.*”³⁵ On its own, in 2014, the EU drew up the *Green Paper on Mobile Health*, where it carried out an extensive study and established relevant guidelines in this matter,³⁶ including the security and privacy of the health user’s personal data.

On the one hand, mobile health comprises the hardware constituted by the mobile device in question with wireless connectivity, and, on the other hand, the software, that is, the specific computer program that we call “*app*.” In this regard, a distinction should be made between those various types of *apps* that are installed on smartphones and refer to the field of health, and those *apps*, which only work on a certain device such as a bracelet, a heart rate monitor and that have specific functionality, such as, measuring

²⁸ Jesús Salido *et al.*, “Desarrollo de Aplicaciones de Salud para dispositivos móviles”, *I+S: Informática y Salud*, no. 110 (2015): 8.

²⁹ Ida Sim, “Mobile Devices and Health”, *N Eng J Med*, no. 381 (2019): 956-968.

³⁰ Elizabeth Bemis, “10 Useful Apps For Seniors in Assisted and Independent Living”, UMH, March 13, 2013, <https://www.umh.org/assisted-independent-living-blog/bid/270671/10-Useful-Apps-For-Seniors-in-Assisted-and-Independent-Living>.

³¹ Some cases we can bring up: the emotional management *app* developed by the Department of Health of Catalonia to help during confinement due to the pandemic caused by COVID-19 (GestioEmocional.cat) and the okencasa *app* (www.okencasa.com), the *app* designed for caregivers of sick people; *apps* related to mental health (<https://www.psycom.net/25-best-mental-health-apps>).

³² See more about this topic at: Susana Navas Navarro, “Salud móvil”, in *Salud e Inteligencia artificial desde el Derecho privado*, ed. Susana Navas Navarro (Granada: Comares, 2021), 51-69.

³³ This is the case of the *mediktor app* (www.mediktor.com).

³⁴ Marcial García Rojo, “mHealth (mobile health)”, *I + S Magazine: Informática y Salud*, no. 110 (2015): 6.

³⁵ WHO, “mHealth: new horizons for Health through Mobile Technologies: based on the findings of the second global survey on eHealth”, *Global Observatory for Health*, v. 3 (2011), www.who.int/goe/publications/goe_mHealth_web.pdf.

³⁶ COM (2014) 219 final. This paper is part of the Digital Agenda for Europe (European Commission, Resolution, 14.01.2014).

the wearers' heart rate. Moreover, the former or, at least, some of them, can have a health purpose.

The COVID-19 pandemic has meant a decisive push for the advancement of *mHealth*. Precisely, *apps* are proving to be useful in the COVID-19 pandemic since they have been, among other functions, a way to decongest the consultation and emergency call centers in case of possible symptoms. Thus, *apps* like the one set up in Singapore, South Korea³⁷ or, Spain – the recent Covid Radar³⁸ – could help to prevent new infections by transmitting information about possible symptoms and, in this regard, appropriate measures could be taken by the competent authorities.³⁹ Likewise, an interesting *app* is being developed by Prof. Brian Subirana, in collaboration with MIT, to diagnose COVID-19 based on the individual's cough.⁴⁰ Recently, the *app*, created and marketed by LegitHealth – a Spanish start-up – for the detection of skin cancer and 130 dermatological pathologies, has been released.⁴¹

Crucial to this work, for deep analysis of billions of unstructured data, is the existence of an open science⁴² sharing information, so that every scientist and *start-up* can get access to the same data. Thus, the outcomes of the research will be more reliable than when they can get just a part of them or a small sample. In this regard, the launch of platforms where data is shared is key for the system.⁴³ What really matters however, is the collective intelligence.⁴⁴ Precisely, the appeal to the community and the citizens' collaboration is vital in the fight against COVID-19.

In conclusion, it should be noted, that, at the basis of any of these technologies, there is an algorithm written in computer language, that is, a computer program, a core element for electronic health. Secondly, it should be emphasised that, in a few cases, hospitals or healthcare centers, depending on the electronic services they deliver to

³⁷ Concerning these *apps* applied in Asia, see: Josep Cañabate Pérez and Albert Castellanos Rodríguez, “Análisis de las aplicaciones para seguimientos de contactos COVID-19 en los países de Asia oriental a la luz del reglamento General de Protección de datos”, in *Salud e Inteligencia artificial desde el Derecho privado*, ed. Susana Navas Navarro (Granada: Comares, 2021), 217-236.

³⁸ Laura Sacristán, “La app Radar COVID será compatible con otras aplicaciones europeas próximamente: el periodo de pruebas comienza el 15 de octubre”, September 9, 2020, <https://www.xatakamovil.com/aplicaciones/app-radar-Covid-sera-compatible-otras-aplicaciones-europeas-proximamente-periodo-pruebas-comienza-15-octubre>.

³⁹ eHealth Network, Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States, Brussels, April 15, 2020, https://ec.europa.eu/health/sites/health/files/ehealth/docs/COVID-19_apps_en.pdf.

⁴⁰ “Científicos catalanes del MIT ensayan con una app que detectará quién tiene coronavirus por la tos”, Lavanguardia, April 17, 2020, <https://www.lavanguardia.com/vida/20200417/48568590791/cientificos-catalanes-mit-app-coronavirus-tos.html>.

⁴¹ “Estos 3 jóvenes españoles han desarrollado una app capaz de detectar el cáncer de piel y otras 130 patologías dermatológicas con un móvil que no cuesta más de 350 euros”, Carlota G. Velloso, <https://www.businessinsider.es/legit-xiaomi-alian-detectar-cancer-piel-movil-721605>, accessed February 2021.

⁴² Jean-Claude Burgelman *et al.*, “Open Science, Open Data, and Open Scholarship: European Policies to Make Science Fit for the Twenty-First Century”, *Front. Big Data*, v. 2, no. 43 (2019), doi: 10.3389/fdata.2019.00043.

⁴³ “Global Health Drug Discovery Institute (GHDDI) and School of Pharmaceutical Sciences (SPS), Tsinghua University jointly announced on January 27th to make internal drug discovery platforms and resources available to external researchers to accelerate drug discovery efforts against the novel coronavirus (2019-nCoV) outbreak”, Targeting COVID-19: GHDDI Info Sharing Portal, accessed February 2021, <https://ghddi-ailab.github.io/Targeting2019-nCoV/>.

⁴⁴ Don Tapscott and Anthony D. Williams, *Wikinomics. La nueva economía de las multitudes inteligentes* (Barcelona: Paidós, 2010), 393 *et seq.*

patients, can be classified as services providers of the information society, both in the private and public health sector, having to comply with the legislation of this sector.⁴⁵

2.3. AI-based systems and Healthcare

2.3.1. Legislation overview

a) Medical devices

The EU, within its strategy for creating a single Digital Market, considers electronic health (“eHealth”), insofar as it intends to develop an interoperable environment, with clear protocols and standards that benefit all stakeholders in health services, including industry. Accordingly, it published an Action Plan 2012-2020⁴⁶ and, almost simultaneously, in 2016, the WHO published a report on eHealth for the European environment.⁴⁷ First of all, there is enormous and growing interest from national, European, and international public authorities in extending health systems to all citizens. Secondly, interest in quality improvement using the internet and related technologies and thirdly, in rationalising the attribution of resources both human and economical to health; and, finally, in gradually implementing high technology in the medical-health field aiming at delivering a predictive, precise, and more personalised healthcare focusing on the patient.⁴⁸

In this regard, one of the main regulations concerning eHealth is the Regulation (EU) 2017/745, of the European Parliament and of the Council of 5 April 2017, on medical devices,⁴⁹ in which the computer program is addressed. The computer program⁵⁰ is the key element in eHealth. In fact, it is the axis on which it pivots. The computer program, which is not incorporated into any medical device, at the time of its release on the market (*stand-alone-software*),⁵¹ in the field of health, is to be classified, in accordance with the Regulation (EU) 2017/745 on medical devices (Art. 2 para. 1), as a medical device.⁵² Indeed, the medical device definition embraces: “*any instrument, device,*

⁴⁵ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, particularly electronic commerce, in the Internal Market (OJ L 178, 17.7.2000) and the prospective Digital Services Act.

⁴⁶ Communication from the Commission to the European Parliament, the Council, the European economic and social committee and the committee of the regions, *eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century*, COM (2012) 736 final.

⁴⁷ This report can be accessed at: <http://www.euro.who.int/en/publications/abstracts/from-innovation-to-implementation-ehealth-in-the-who-european-region-2016>.

⁴⁸ Ángel Durántez Prados, *Joven a los 100* (Madrid: La esfera de los Libros, 2020), 72-80.

⁴⁹ OJ L 117/1, 5.5.2017. The application of this Regulation is postponed until 26 May 2021. In this contribution I focus just on this Regulation leaving aside the Regulation (EU) 2017/746 on in-vitro medical devices that will replace Council Directive 98/79/EC on in-vitro Diagnostic Medical Devices on May 2022. Regarding the Regulation (EU) 2017/745, see Magali Contardi, “An overview on the EU Regulation in the field of medical devices” in *Changes in the Medical Device’s Regulatory Framework and its impact on the Medical Device’s industry: from the Medical Device Directives to the Medical Device Regulations* *Erasmus Law Review*, v. 12, no. 2 (2019): 166-177; Gianluigi Passarelli, “Legal aspects of the path towards a true EU Medical Devices innovation”, *Le Nuove Leggi Civili Commentate*, v. 2 (2020): 309.

⁵⁰ About the concept of “computer program,” see: “*Guidelines on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices*” by the European Commission DG Internal Market, Industry, Entrepreneurship and, SMEs Directorate Consumer, Environmental and Health Technologies Unit Health technology and Cosmetics (Meddev 2.1/6, July 2016): “*set of instructions that processes input data and creates output data*”.

⁵¹ The Guidelines Meddev 2.1/6 already mentioned defines a “*stand-alone-software*” as “*software which is not incorporated in a medical device at the time of its placing on the market or its making available*”.

⁵² Allison Dennis, “Healthcare Technology Regulation in the EU and the UK: from Medical Devices to

equipment, computer program, implant, reagent, material or other article intended by the manufacturer to be used in people, separately or in combination, with any of the following specific medical purposes:

Diagnosis, prevention, monitoring, prediction, prognosis, treatment, or alleviation of a disease

Diagnosis, monitoring, treatment, alleviation or compensation of an injury or disability

Investigation, replacement, or modification of the anatomy or of a physiological or pathological process or state

Obtaining information through the in-vitro examination of samples from the human body, including organ, blood and tissue donations.”

According to Recital no. 19 of this Regulation, computer programs, when they are specifically intended by the manufacturer for one or more of the medical purposes (e.g., a software detecting an illness), taking into consideration the previously mentioned definition of medical devices settled by the Regulation (EU) 2017/745, are medical devices.⁵³ In this case, the computer program may only be placed in the market if it has the CE certification and has been checked in a conformity assessment procedure (Art. 10 para. 6).

Moreover, computer programs for general use, even when they are employed in healthcare (e.g., document preparation, medical information storage, word processing), or computer programs intended for wellness or lifestyle purposes, are not seen as medical devices.⁵⁴

In the EU, there are no specific guidelines for software with self-learning capability, completely autonomous, to be viewed as medical device, nor is there any authority that certifies the conformity of this type of computer program.⁵⁵ Therefore, the COCIR⁵⁶ has stressed that they cannot be placed on the market as a medical device.⁵⁷ The Meddev 2.1/6 Guidelines take into particular account the “predetermined” software as a paradigm. Even so, the Regulation (EU) on medical devices allows health centers to manufacture their own product, which is used to provide the healthcare service, to a group of specific patients, based on the fact that there is no product on the market that can meet its specific needs (Art. 5 para. 5). In these cases, the product manufactured by the healthcare center itself cannot be marketed (*in-house*), and except for the general safety and operating requirements provided in Annex I of the Regulation, the rest of the requirements do not apply. This manufactured *in-house* device may well be a non-predetermined computer program, which modifies itself outside or beyond the boundaries designed by the manufacturer.

intellectual property and advertising”, in *HealthTech. Law and Regulation*, ed. Jelena Madir (Cheltenham: Edward Elgar, 2020), 59.

⁵³ Armin Gärtner, MEDDEV-Leitfaden 2.1/6 für Software als Medizinprodukt am Beispiel PDMF, E-HEALTH.COM., 2017, accessed February 2021, http://www.e-health-com.eu/fileadmin/user_upload/dateien/Downloads/Gaertner_Software_als_Medizinprodukt_end.Pdf.

⁵⁴ More about computer programs as medical devices in: Susana Navas Navarro, “Salud electrónica e Inteligencia Artificial”, in *Salud e Inteligencia artificial desde el Derecho privado*, ed. Susana Navas Navarro (Granada: Comares, 2021), 14-23.

⁵⁵ See: ISO/IEC WD 22989 Artificial Intelligence. Concepts and Terminology; ISO/IEC WD 23053 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML). Concerning the health software, see the standard: IEC 82304-1:2016 General Requirements for Product Safety. Online: iso.org. Accessed February 2021.

⁵⁶ COCIR is the abbreviation for: “The European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry”.

⁵⁷ COCIR, “Artificial Intelligence in EU Medical Device Legislation”, September, 2020, 10, https://www.cocir.org/fileadmin/Position_Papers_2020/COCIR_Analysis_on_AI_in_medical_Device_Legislation_-_Sept_2020_-_Final_2.pdf.

The *High-Level Panel of Experts* has, as it is known, been publishing different reports on future regulation of AI. In *Ethics Guidelines for Trustworthy*,⁵⁸ Artificial Intelligence refers to the “*explainability and transparency of the algorithm*” as one of the properties that make an AI system trustworthy. Hopefully these guidelines will be further developed, in the future, and the application of AI to health will be considered from both an ethical and legal point of view.⁵⁹ This path has already begun with the COCIR Report, in which it recommended that the IEC 62304 standard should be studied and, where appropriate, updated, requiring manufacturers of medical devices to establish an “*algorithm change protocol*” (ACP)⁶⁰ for health products based on AI with learning capability, to establish, from the design, minimizing the risk of bias for vulnerable groups.⁶¹

b) High-risk AI-based systems and health

Almost in parallel with the legislation on medical devices, in relation to AI, and the huge production of data, studies, and reports that have been carried out, as well as resolutions, communications, and other documents of the European authorities have been published, relevant working groups have been built up. Work is intense within the EU, aiming to produce a future regulation of AI,⁶² robotics, and emerging technologies, as well as blockchain and online platforms, among others. In addition, it is worth mentioning the forthcoming publication, of an EU *Data Act* in 2021, as highlighted by the Communication on a European Strategy for Data.⁶³

Particularly, concerning AI, two main reports deserve special attention: firstly, the “*Liability for Artificial Intelligence and other emerging digital technologies*” prepared by the *Expert Group on Liability and New Technologies – New Technologies Formation*, known by the acronym NTF, in November 2019⁶⁴ and, secondly, the report from the European Commission to the European Parliament, the Council and the European Economic and Social Committee, “*On the safety and liability implications of Artificial Intelligence, the Internet of Things and Robotics*”⁶⁵ accompanying the White paper “*On Artificial Intelligence – A European approach to excellence and trust*.”⁶⁶ Likewise, two more documents should be mentioned: the “*Draft Report on Civil Liability Regime for Artificial Intelligence*”⁶⁷ and the “*Civil liability regime for artificial intelligence*” of the research service of the European Parliament,⁶⁸ made public in September 2020. Moreover, the “*Report with Recommendations to the Commission on a civil liability regime for artificial intelligence*” of the European Parliament, published on 5 October 2020, stands out for its importance.⁶⁹ It has been accepted, entirely, in the

⁵⁸ HLEG AI, “Ethics Guidelines for Trustworthy AI”, European Commission, April 8, 2019, 5, <https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>.

⁵⁹ Heinz-Uwe Dettling, “Künstliche Intelligenz”, 640.

⁶⁰ Woodrow Barfield and Ugo Pagallo, *Advanced Handbook on Law and Artificial Intelligence* (Cheltenham: Edward Elgar, 2020): 22.

⁶¹ COCIR, “Artificial Intelligence in EU Medical Device Legislation”, 13-14; 20-22.

⁶² European Parliament Resolution of 12 February 2019 on a comprehensive European industrial policy on artificial intelligence and robotics [2018/2088(INI)].

⁶³ COM (2020) 66 final, 19.2.2020.

⁶⁴ See: [LiabilityforAIandotheremergingtechnologies.pdf](#), accessed February 2021.

⁶⁵ COM (2020) 64 final, 19.2.2020.

⁶⁶ COM (2020) 65 final, 19.2.2020.

⁶⁷ INL 2020/2014, May 2020.

⁶⁸ See <http://www.europa.europa.eu/thinktank>, accessed February 2020.

⁶⁹ 2020/2014(INL) 5.10.2020.

Resolution of the European Parliament, of 20 October 2020, in which a *Proposal for a Regulation on civil liability for the operation of artificial intelligence systems* is made.⁷⁰

On 16 February 2017, the European Parliament adopted a Resolution on “*Civil law rules on Robotics*”⁷¹ with recommendations for the European Commission. In this Resolution, the Commission was asked to prepare a proposal for a future legal instrument containing civil rules in relation to robots’ liability and other AI systems. 2018 was a very active year in this area.⁷² In March, the Commission founded the previously mentioned *Expert Group on Liability and New Technologies* with two formations: NTF (*new technologies formation*) and PLDF (*products liability directive formation*). The NTF should be limited to the non-contractual liability aspects. After analysing the national laws in this regard, focusing on specific cases, and comparing different aspects of these standards, the previously mentioned report presented its conclusions and recommendations. In addition, in April, the Commission published the Staff Working Document on “*Liability for emerging digital technologies*”⁷³ accompanied by the document “*Artificial Intelligence for Europe*.”⁷⁴

In this contribution, when referring to AI, I considered the definition given by the *High-level Expert Group on AI*,⁷⁵ established within the EU, such as: “*AI systems are software (and possibly also hardware) designed by humans that, given a complex objective, act in a physical or digital dimension, perceiving their environment through the acquisition of data, the interpretation of said data, whether structured or not, reasoning, processing the information derived from the data and making the best decision to achieve the aforementioned objective.*” This definition is closely followed by the Resolution of the European Parliament of 20 October 2020 (Art. 3 lit. a).⁷⁶

The medical devices sector is one of those sectors in which the technology used can partly be classified as “*high-risk*,” using the term suggested by the *Resolution of the European Parliament* of 20 October 2020⁷⁷ and by the *White Paper on Artificial Intelligence*. The latter sets out an AI-based system can be considered high-risk if it meets the following two criteria cumulatively.⁷⁸ First of all, this system is used in a sector in which,

⁷⁰ P9_TA-PROV (2020)0276.

⁷¹ P8_TA (2017)0051.

⁷² Actually, in February, the European Parliamentary Research Service (EPRS) published additionally the study “A common EU approach to liability rules and insurance for connected and autonomous vehicles”, accessed February 2021, [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU\(2018\)615635_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf).

⁷³ SWD (2018) 137 final.

⁷⁴ COM (2018) 237 final.

⁷⁵ AIHLEG, “A definition of AI: Main capabilities and disciplines”, April 8, 2019, <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>. Also, see: EU Science Hub, JCR Technical reports, “AI Watch. Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence”, accessed February 2021, <https://ec.europa.eu/jrc>.

⁷⁶ “AI-system means a system that is either software-based or embedded in hardware devices, and that displays behavior simulating intelligence by, inter alia, collecting and processing data, analyzing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals”.

⁷⁷ Art. 3 lit. c: “high risk means a significant potential in an autonomously operating AI-system to cause harm or damage to one or more persons in a manner that is random and goes beyond, what can reasonably be expected; the significance of the potential depends on the interplay between the severity of possible harm or damage, the degree of autonomy of decision-making, the likelihood that the risk materializes and the manner and the context in which the AI-system is being used”.

⁷⁸ White Paper, 16-17.

given the characteristics of the activities provided, significant risks can be expected to occur. Two are the sectors especially taken into account: transport and assistance, in which health services can be comprised. The list with the sectors where technology is considered as high-risk must be updated every six months. Secondly, the AI-based system in that sector must be used in such a way that significant risks are likely to occur. This implies that not every use involves significant risk. Thus, not every technology used in the healthcare field presents the same level of risk. For example, it is not the same in the telematic consultation between a doctor and his patient (*low-risk*) as in the use of a surgical robotised arm that operates remotely and autonomously (*high-risk*).⁷⁹ If the risk involves bodily harm, the person's death, or significant material or moral damage, we normally tackle with high-risk AI-based systems.

If we apply this approach to computer programs considered medical devices, we could affirm that those of risk class III and IIb would be of high-risk, while those of class IIa and I of low/medium risk.⁸⁰

2.3.2. *Some controversial issues regarding civil liability*

In AI-based systems, there is often more than one person who “operates” the technology; for example, the hospital or health center that intervenes on a patient with a surgical robot, but there is also another person or a hospital that provides support services, updates the software, defines the characteristics of the technology or supervises the machine learning system. The first operator is considered, according to the NTF and the European Parliament Resolution of October 20, 2020, as a “frontend operator”⁸¹ while the second is viewed as a “backend operator,”⁸² between which a legal relationship may (or may not) exist.⁸³ When an AI-based system is “used” as a health practitioner “auxiliary,” the degree of autonomy, learning, and decision-making capability of that system should be taken into account. I am not dealing here with the assumption that the robot does not have any type of autonomy, because the human takes the control or autonomy that has been deactivated by the human. Such cases would not differ at all or very little, for the purposes of civil liability, of the handling of any other device, tool, or material used by the healthcare professional. If it causes damages, civil liability rules will be applied. This question should not be problematic. Nor is it controversial (or, at least, it does not seem to me that it should be) the assumption that the AI system makes a diagnosis or proposes a treatment, but the final decision regarding the medical act is taken by the physician or his team. If the decision taken is to follow the criteria established by the software and the medical act based on it entails a series of damages, the liability lies with the subject (or subjects)

⁷⁹ Draft Report, 7.

⁸⁰ Annex VIII Regulation (UE) 2017/745, on medical devices. See: Tom Chakraborti, “Regulation and Governance of HealthTech”, in *HealthTech. Law and Regulation*, ed. Jelena Madir (Cheltenham: Edward Elgar, 2020), 33.

⁸¹ Art. 3 lit. e EU Report (5.10.2020): “frontend operator means any natural or legal person who exercises a degree of control over a risk connected with the operation and functioning of the AI-system and benefits from its operation.”

⁸² Art. 3 lit. f EU Report (5.10.2020): “backend operator means any natural or legal persona who, on a continuous basis, defines the features of technology and provides data and an essential backend support service and therefore also exercises a degree of control over the risk connected with the operation and functioning of the AI-system.”

⁸³ See: *LiabilityforAIandotheremergingtechnologies.pdf*, accessed February 2021.

who make the final decision. It is a liability by own action; not, by someone else's behavior.

On the other hand, if the AI-based system makes the decision autonomously (high-risk technology), whether the person has the power to supervise the system and proceeds to act, for example, through a robotic surgical arm, the issue is not obvious. Here, the analogy could be made with the employer and the employee. In this case, liability for someone else's act would be the appropriate basis for liability, since we must consider the actions of two possible "subjects," firstly, a natural person (healthcare practitioners) or legal person (clinic or hospital) and, secondly, the AI-based system, so that the activity or conduct of each of them is relevant to establish whether there is a case for liability. If, for example, supervision is lacking, the physician or the hospital must be held liable for the damage caused by the AI-based system because they have violated a duty of care. Nevertheless, it also requires a wrong performance on the side of the AI-based system in the same way as if a human acts wrongly, he or she would be regarded as liable.

In the case of AI-based systems, liability for someone else's act could be based on the relationship between the physician and/or hospital and the AI-based system since the former benefits from the activity carried out by the latter. We should keep in mind that the AI-based system I am addressing is more typical of being commissioned or acquired by companies than by individuals. In this case, the liability of the "principal" is based on the behavior of his "auxiliaries" (e.g., Art. 1903 para. 4 Spanish Civil Code). The term "*auxiliary*" covers all those cases in which a person or, in this case, an AI-based system behaves according to the instructions of another that would be the principal regardless of the relationship existing between them. Therefore, there is a "*principal*" (the human or the legal person in question) and an "*auxiliary*" (the AI-based system). However, one of the requirements for applying the principal's liability for his or her auxiliary's acts is the existence of a dependency relationship. The principal is the one who gives the instructions. In the matter at hand, AI-based systems, although, in some cases, may have prior instructions, by virtue of their learning capability and autonomy, when making decisions, act without being subject to the control of the principal that benefits from its activity. There is a lack of dependency which is a characteristic of the principal's vicarious liability for his or her auxiliary's actions. Rather, it would be considered as an independent contractual party.

In this particular regard, it could be thought that only those AI-based systems follow the instructions given by the principal. However, they have freedom in executing the entrusted task and could be subjected, by analogy, to the same principal vicarious liability requirements. Notwithstanding, there would not be "identity of reason" in those cases in which the AI-based system acts, regardless of the instructions given or that, taking as a starting point latterly, because of its self-learning capability, behaves far away from them. In any case, charging the principal with the harmful consequences of the behaviour of the AI-based system he uses is consistent with the idea that whoever enjoys the benefit generated by the AI-based system is the principal.⁸⁴

In accordance with the terminology used by the NTF and in the Resolution of the European Parliament, in which recommendations are made to the Commission to regulate civil liability for damages caused by operating high-risk AI systems of 20

⁸⁴ Ernst Karner, "Liability for robotics: current rules, challenges, and the need for innovative concepts", in *Liability for Artificial Intelligence and the Internet of Things*, eds. Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (Baden Baden: Nomos Verlag, 2018), 120.

October 2020, the principal, who must supervise the system, would be considered the “frontend operator” while the producer of the AI-based system would be the “backend operator.” In the case of eHealth, the “frontend operator” would be the hospital or clinic acting as a “principal,” while the health professional using the AI system would be subjected to the instructions given. Therefore, if the bad performance was that of the health practitioner, the principal (the hospital or the clinic) would be held accountable according to the civil liability rules for someone else’s acts.

Cases of completely autonomous AI-based systems, in which there is no human intervention, remain outside the proposed Regulation because there is no “operator.” If the “backend operator” is considered a manufacturer, the corresponding regulations will be applied. Indeed, Art. 3 lit. d of the previously mentioned report by the European Parliament warns that “operator” includes both front and backend operator, unless the liability of the latter is already covered by Directive 85/374/EEC on products liability,⁸⁵ obviously, because he is considered a “producer.”⁸⁶

3. eHealth and the personalisation of medicine. Patients empowerment

The COVID-19 pandemic is highlighting the importance emerging technologies based on AI and highly sophisticated algorithms as well as the implantation of communication, information technologies and robotics in different areas of our life⁸⁷ can become.⁸⁸ From personal relationships throughout the lockdown, teleworking, online training, *e-commerce* to, significant in the current climate, “*electronic health*,” the application of emerging technologies to health will allow the personalisation of therapeutical and medical treatments, in relation to the specific individual, that is, the healthcare system user.

Technology and, particularly, technology applied to health, means that the patient will not be a mere passive subject regarding his own health. Rather he or she will actively participate in aspects related to it, making decisions together with their physicians. Thus, it is an equal relationship in which the patient and the health professional cooperate. Indeed, at present, citizens in general – and in the health field are not an exception – seek information, primarily, on the internet.⁸⁹ Or they obtain it from the *apps* that they have downloaded, visiting the physician with basic information about their health that, until recently, they lacked.

The term “*patient*” should be subjected to revision. That is, it may not serve to describe the new citizen interested in his or her health. In fact, the patients’ true “autonomy” would precisely take control of everything that concerns his or her health, not simply being a mere recipient of information to agree with. This approach continues to prevail in the regulation about “patient autonomy,” in which he or she is seen mainly as a passive person, who receives information to which he or she “consents”

⁸⁵ OJ L 210, 7.8.1985.

⁸⁶ Annabelle Bruyndonckx *et al.*, “Product Liability: compliance and safety issues”, in *HealthTech. Law and Regulation*, ed. Jelena Madir (Cheltenham: Edward Elgar, 2020), 114-142.

⁸⁷ “What if we could fight coronavirus with artificial intelligence”, EPRS, European Parliamentary Research Service, Author: Mihalios Kritikos, Scientific Foresight Unit (STOA), PE 641.538, Mach 2020.

⁸⁸ As, for example, the algorithm created by the *European Center for Disease Prevention and Control* in relation to the actions to be taken in the event of contagion by COVID-19.

⁸⁹ Nancy P. Gordon and Mark C. Hornbrook, “Differences in access to and preferences for using patient portals and other eHealth technologies based on race, ethnicity, and age: a database and survey study of seniors in a large health plan”, *J Med Internet Res*, v. 18, no. 3 (2016): e50.

(that is “nods”), even if, in practice in many cases, he or she is just “adhering” to it. A “paternalistic” model continues to prevail (even if it is “weak”) based more on the beneficial nature of the medical profession than on the true autonomy of the patient,⁹⁰ although it is intended to present the issue otherwise.⁹¹ Technology permits responsibility to be shared more equitably between physicians and patients.⁹²

This new approach to individual health gives the possibility of supplying a more personalised medicine, almost tailored to each patient. In this regard, standardisation in the health field will gradually disappear to give way to the application of a much more unique medicine, which will have a particular impact on aspects as relevant as the informed consent of the patient/health service user⁹³ and on insurance premiums.⁹⁴

4. Discrimination and eHealth

As I have been highlighting, technology applied to health makes it possible for medicine to focus much more on the specific patient, personalising the treatment with much more precision, than until recently, insofar as the technology permits access to a whole series of data about the patient’s health, easing the provision of a particular health service. The technology used is of a very different range. Some specific type of technology will require a level of knowledge based on the information provided both by healthcare professionals and by the manufacturer, which may lead to certain groups being deprived of it and, consequently, of a certain type of treatment that could improve their quality of life.⁹⁵ This can happen, for instance, in the case of dependent elderly or very elderly people⁹⁶ and of people with specific types of disability. Regarding the first group, in addition to the fact that they may have limited access to technology – maybe they have a mobile phone (not always a *smartphone*) or a tablet –, they tend to focus on very basic functions, and, in many cases, they do not fully understand the way it works. In case of the pandemic caused by COVID-19 with the launch of applications, both in the public and private sector, with different functions (e.g., tracking the contacts of people with a positive diagnosis, entering health data, locating sick people, etc.), and considered one of the most effective means of controlling community contagion, the elderly have been prevented from utilising this means of disease control.⁹⁷ The exclusion of this group of people, to which electronic health comes very late, is clear.

The second social segment I was referring to, is people with disabilities which do not enable them to properly manage and understand the technology applied to improve their health. It should be noted that, for these people, accessing technology

⁹⁰ Ion Arrieta Valero, “El ejercicio razonable de la autonomía del paciente”, *Dilemata*, v. 4, no. 8 (2012): 27-32.

⁹¹ Ana Ylenia Guerra Vaquero, “El paciente como sujeto de derechos. La autonomía de la voluntad como fundamento del consentimiento informado y de las instrucciones previas”, *BAJO PALABRA. Revista de Filosofía*, II Época, no. 12 (2016): 153-162.

⁹² EDPS, Opinion 1/2015, mHealth. Online at: https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf, accessed February 2021.

⁹³ Gunther Eysenbach, “Consumer Health Informatics”, *BMJ* v. 24, no. 320(7251) (2000): 1713-1716.

⁹⁴ Carlos Górriz López, “Inteligencia artificial y seguros”, in *Salud e Inteligencia artificial desde el Derecho privado*, ed. Susana Navas Navarro (Granada: Comares, 2021), 269-301.

⁹⁵ Jelena Madir, “Using?”, 2.

⁹⁶ Eduardo Osuna Carrillo de Albornoz, “La información en el contexto de la atención sanitaria a las personas mayores vulnerables”, in *Autonomía del paciente mayor, vulnerabilidad y e-salud*, eds. M^a. Belén Andreu Martínez and José Ramón Salcedo Hernández (Valencia: Tirant Lo Blanch, 2018), 138-139.

⁹⁷ Council of Europe, “Joint Statement on Digital Contact Tracing”, Alessandra Pierucci and Jean-Philippe Walter, 28.04.2020, www.coe.int/dataprotection, accessed February 2020.

implies getting access to a very effective assistive or supportive system (“assistive technology”)⁹⁸ in order to overcome social barriers with which they cope. In some of these cases, the exclusion could be alleviated with a “universal design,” making the technology accessible to any citizen. The “universality,” “inclusivity” character (“design for all”) of the design, from the conception of the technology (“*by default*”), is fundamental for disabled persons. Universal design⁹⁹ should not prevent that reasonable adaptations should be made, when necessary, to the specific case in order to facilitate the accessibility of the person concerned to the technology in question. In Recital no. 50, by Directive (EU) 2019/882, of the European Parliament and of the Council of April 17, 2019, on the accessibility requirements of goods, products, and services, obviously, dependent persons, who cannot be considered having some kind of disability, can benefit from this universal accessible design.

Other disadvantaged groups such as migrants or those with a low or very low-income level, could also be excluded from accessing technology even if they can get access to public health services.

Another situation that, in my view, should be highlighted, deals with the risk that the data collected in electronic health devices will be crossed with other data (for example, that extracted from user interaction on social networks), allowing the creation of profiles, which lead to automated decision-making harming users significantly. While Art. 22 General Data Protection Regulation¹⁰⁰ requires that the “owner” of the data should be informed about the computational logic that is being used, the truth is, in practice, it can generate invisible discrimination related to health, for instance, concerning a disease suffered by an individual (e.g., AIDS) or regarding his or her disability. These situations can be direct discrimination, but they can also be discrimination by association,¹⁰¹ such as when a person is discriminated against for having a child with a disability, caring for a terminally ill person or infected with COVID-19. In these cases, there is most likely a gender bias¹⁰² also, leading to a “double discrimination,” which is usually “invisible”¹⁰³ for the person discriminated against. Thus, it is extraordinarily important the segregation, in general, of data by sex and, particularly, in the medical field, to the extent that men and women may react differently to treatment due to their not always identical physiology.¹⁰⁴

⁹⁸ Directive (EU) 2019/882, of the European Parliament and of the Council of 04.17.2019, on the accessibility requirements of goods, products and services (OJ L 151/170, 7.6.2019) defines the “technology support” (Art. 3 nr. 37) as follows: “*any item, equipment, service or product system, including programs, that is used to increase, maintain, replace or improve the functional capacities of people with disability, or to alleviate or compensate for deficiencies, activity limitations or participation restrictions.*”

⁹⁹ The Convention on the rights of persons with disabilities, signed in New York on December 13, 2002, (<https://www.un.org/en/>, accessed February 2021) defines “universal design,” in Art. 2, as “*the design of products, environments, programs and services to be usable by all people, to the greatest extent possible, without the need for adaptation or specialized design.*” “Universal design” shall not exclude assistive devices for particular groups of persons with disabilities where is needed.

¹⁰⁰ Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.

¹⁰¹ Sandra Watcher and Brent Mittelstadt, “A right to reasonable inferences: re-thinking data protection law in the Age of Big Data and AI”, *Columbia Business Law Review*, v. 2 (2019): 494 et seq.

¹⁰² OCDE, “Women at the core of the fight against COVID-19 crisis”, accessed February 2021, https://read.oecd-ilibrary.org/view/?ref=127_127000-awfnqj80me&title=Women-at-the-core-of-the-fight-against-COVID-19-crisis.

¹⁰³ Mireille Hildebrandt and Bert-Jaap Koops, “The challenges of ambient law and legal protection in the Profiling Era”, *MLR*, v. 73, no. 3 (2010): 428-460.

¹⁰⁴ Storydata (coord.), *Open Data and Artificial Intelligence. Tools for Gender Equality* (Govern obert:

5. Conclusion. Internet of bodies

The technology applied to health and, particularly, that related to medical devices leads to the “*Internet of Medical Things*”¹⁰⁵ (IoMT), which is linked to the so-called “*Internet of Bodies*” (IoB).¹⁰⁶ When the device connected to the human body is of a medical nature, both IoMT and IoB, in the end, involve “quantifying,” that is, human beings are becoming “data.” In fact, the individual himself, from the different devices that he possesses and/or carries with him incorporated or not in his body,¹⁰⁷ extracts data regarding his own parametrical bioindicators in numerical form. Thus, he quantifies with percentages how much he has slept and the quality of his sleep, blood pressure, heart rate, steps taken, insulin level, etc. This need for quantification has led to the “*quantified self*” movement.¹⁰⁸

The tendency to quantify is widely extended, for example, in the field of online intermediation platforms where classifications, ratings, and other lists are established based on the stars or scores given by individuals. In any service that is provided to us, whether *online* or *offline*, we are asked for a score. We are becoming a society of quantification.¹⁰⁹ The problem is that, although numerical data can give a clearer vision of reality, they also simplify it and can do so to a point where a new reality is built. In short, it is used as a social engineering tool. In the case that I address – the IoB – the implantation of chips, sensors, or other devices (whether medical or not), which collect a multiplicity of data, is leading to the «construction» of a «new» human being that, in some cases, can possess some capacities or abilities beyond those with which he has been genetically and physiologically gifted.¹¹⁰ Whatever it is, individuals’ tendency to “*personalise*” is a common feature of this time.¹¹¹ Therefore, all this amount of data, massively analysed, can drive to developing and publishing tailor-made legal norms (norms’ “personalization”) or, at least, to the personalised “application” of the existing legal norm(s) decided by an algorithm. Hence, it must be noted that the decision adopted cannot significantly harm the holder of the data (*arg. ex Art. 22 GDPR*), especially in the absence of his or her consent.

Generalitat de Catalunya, 2020).

¹⁰⁵ Florence Hudson and Chris Clark, “Wearables and Medical Interoperability: The Evolving Frontier”, *Computer*, v. 51, no. 9 (2018): 86-90.

¹⁰⁶ Andrea M. Matwyshyn, “The Internet of Bodies”, 81-82.

¹⁰⁷ Three generations of technologies related to the human body are already mentioned. The first generation consists of external technology such as *wearables* that we have reported in this work. The second one deals with technology implanted in the human body, such as an artificial pancreas or a cochlear implant. The third has to do with the fusion of the human mind with computers and the Internet, which is known as “*brain-computer interface*” (BCI). About this and other issues, see: Andrea M. Matwyshyn, “The Internet of Bodies”, 94-115.

¹⁰⁸ Steffen Mau, *The Metric Society* (Cambridge: Polity Press, 2019), 99 et seq.

¹⁰⁹ Steffen Mau, *The Metric Society*, 10 et seq.

¹¹⁰ Susana Navas Navarro and Sandra Camacho Clavijo, *El ciborg humano. Aspectos jurídicos* (Granada: Comares, 2018).

¹¹¹ Andreas Reckwitz, *Die Gesellschaft der Singularitäten* (Berlin: Suhrkamp, 20nd ed., 2020), 27 et seq.