IUS et SALUS
RIVISTA DI DIRITTO SANITARIO E FARMACEUTICO

Rivista IUS et SALUS

Roma, 01.05.2020

Artificial Intelligence in Social and Health Services: A New Challenge for Public Authorities in Ensuring Constitutional Rights*

by **Guerino Fares**, *Associate Professor of Public Law and Health Law at Roma 3 University*
Scientific director of "Ius & Salus" journal

ABSTRACT: By taking advantage of the precious opportunities that technological development offers, national health and social services systems can improve their performance by reducing time and costs and simplifying actions and procedures more rationally. There are numerous potential applications of artificial intelligence (AI) to the healthcare and social services sector. They produce benefits for patients, optimizing their treatments, and society, compensating the increasingly higher costs of treating new diseases and meeting increasingly more complex care needs. The use of predictive algorithms and techniques may be extremely valuable in several operational contexts: from the prevention to the diagnosis of diseases, from surgery to rehabilitation, from home-based care for elderly and disabled people to the organisation of social services in households. However, the desirable implementation of AI must respect supreme principles of law and fundamental human rights on which modern democracies and contemporary constitutional orders are based: the principles of equality, equal treatment and access to services; the right to freedom of the individual; the principle of proportionality and the precautionary principle in risk management; the right to self-determination and the right to the protection of personal data; the right to decision making that is not fully automated but may include the contribution of AI managed by a human being under the responsibility of the latter.

* Questo lavoro è destinato al volume a cura del Prof. Martin BELOV, *Information and Technology Revolution and its impact on State, Constitutionalism and Constitutional Law*, London, Hart Publishing, 2020, in corso di pubblicazione.

ABSTRACT: Sfruttando le preziose opportunità offerte dallo sviluppo tecnologico, i sistemi nazionali di erogazione dei servizi sanitari e sociali possono migliorare le loro prestazioni riducendo tempi e costi e semplificando le azioni e le procedure in modo più razionale. Numerose sono le potenziali applicazioni dell'intelligenza artificiale (IA) al settore sanitario e dei servizi sociali. Esse producono benefici sia per i pazienti, perché ne ottimizzano i trattamenti sanitari e assistenziali, sia per la società nel suo complesso, compensando i costi sempre più elevati richiesti dalle terapie per la cura di nuove patologie e soddisfacendo un bisogno di assistenza che diviene sempre più complesso. L'utilizzo di algoritmi e tecniche predittive può essere estremamente prezioso in diversi contesti operativi: dalla prevenzione alla diagnosi delle malattie, dalla chirurgia alla riabilitazione, dall'assistenza domiciliare per anziani e disabili all'organizzazione dei servizi sociali in ambito familiare. L'auspicabile implementazione dell'IA deve, nondimeno, rispettare i principi giuridici supremi e i diritti umani fondamentali su cui si basano le moderne democrazie e gli ordini costituzionali contemporanei: i principi di uguaglianza, parità di trattamento e di accesso ai servizi; il diritto di libertà degli individui; il principio di proporzionalità e il principio di precauzione nella gestione del rischio; il diritto all'autodeterminazione e il diritto alla protezione dei dati personali; il diritto ad un processo decisionale che non sia completamente automatizzato ma può prevedere il contributo dell'IA solo se gestito da un essere umano sotto la responsabilità di quest'ultimo.

1. *The relationship between AI and health and social services: the opportunities offered by the technological development*

The social and healthcare sector is more and more impacted by digital and artificial intelligence systems because of increasing developments of sophisticated machine learning and techniques that are able to find complex patterns in data.

This paper will be focused mainly on the digitalization of public action connected to the big data phenomenon and the algorithmic procedures (e.g., e-health, telemedicine, m-health and smart-phone app for healthcare purposes, robotic surgery).

Meanwhile, the correct management of those technologies based on AI needs an adaptation of the legal framework related to the welfare state, with the aim of guaranteeing citizens' constitutional rights to the most appropriate extent: from the effectiveness of care to equality in patients' access to medical

treatment; from reasonableness of the administrative procedures to the application of data protection regulation.

The paper aims at proposing an analysis of the main constitutional and administrative issues with regard to Artificial Intelligence, especially in the social, healthcare and pharmaceutical sectors: moving from the role of AI and digital technologies in the design and delivery of those types of services[1].

Many different definitions of AI have been given over time. Some people talk about "the science of making machines which do things that would require intelligence if done by men"[2]. Others talk about a "cross-disciplinary approach to understanding, modeling, and replicating intelligence and cognitive processes by invoking various computational, mathematical, logical, mechanical, and even biological principles and devices"[3].

The European Commission is also aware of how important the notion of artificial intelligence is[4], which defines it as follows: "Artificial intelligence (AI) refers to systems that display intelligent behavior by analyzing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications). Many AI technologies require data to improve their performance. Once they perform well, they can help improve and automate decision making in the same domain"[5].

The Commission itself offers clear examples of this innovative tool with enormous potential for public policies: "AI is helping us to solve some of the world's biggest challenges: from treating chronic diseases

[1] "The health sector has been hailed by the Organisation for Economic Co-operation and Development (OECD) as the perfect platform for AI, due to the need for data to improve diagnostics and treatments and because of the volume of data generated by patients and professionals in electronic health records and the Internet of Things. AI can contribute to the improvement of decision-making in the diagnosis and treatment of patients and to the development of new treatments": see EUROPEAN FOUNDATION FOR THE IMPROVEMENT OF LIVING AND WORKING CONDITIONS – EUROFOUND, *Research Report on "Public Services - Impact of digitalisation on social services"* , Luxembourg, 2020, http://eurofound.link/ef19043, p. 14.

[2] J. COPELAND, *Artificial Intelligence: A Philosophical Introduction*, New Jersey, Blackwell Pub, 1993, p. 1.

[3] K. FRANKISH, W.M. RAMSEY (eds.), *The Cambridge Handbook of Artificial Intelligence*, Cambridge, Cambridge University Press, 2014, p. 7. The theory of the algorithm as a process to be applied to numbers is introduced in A.M. TURING, *Rounding-off Errors in Matrix Processes (1948)*, in *Collected Works of A.M. Turing*, vol. II, Amsterdam, 1992.

[4] Other definitions of AI have been formulated: such as, for example, the ability of a digital computer or a computer-controlled robot to perform tasks that are usually associated with the highest intellectual processes characteristic of human beings (the ability to reason either to discover meanings or to learn from past experience); or as a scientific discipline that aims to develop programs or machines (software and /or hardware) that have behavior that would be defined as intelligent if it were exhibited by a human being. Science and experience have also shown that important practical results are achievable in the context of decision-making processes, the understanding of natural language, the recognition of models and images. The common assumption for these processes is that machine can be considered as a child who, gradually educated, develops an adult brain (A. TURING, *Computing Machinery and Intelligence*, Mind, 59 (1950), 433).

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

or reducing fatality rates in traffic accidents to fighting climate change or anticipating cybersecurity threats"[6].

However, all definitions given of IA are dated by now; therefore, they need to be updated with technological progress, considering benefits and risks related to a new superintelligence, defined as "any intellect that greatly exceeds the cognitive performance of humans in virtually all domains of interest"[7].

AI and machine learning are constantly evolving areas of research and practice, and the discussions about transparency, proportionality and accountability are consequently increasing. The availability of computing power and the access to large pools of heterogeneous datasets have allowed researchers to develop even more demanding algorithms to analyse data and search for patterns, correlations and links that may be of significance.

Furthermore, we need specific information about the main issue of AI, namely the "decision paradigm", which is linked, for instance, to the right not to be subjected to a decision based solely on automated processing in order to obtain social benefits.

Administrative procedure automation may set milestones in the interpretation and declination of the measures adopted through them and in the consequent profiles of administrative responsibility. The assignment of decision-making processes to an "algorithm" means that the result derived from this application must be considered as an "administrative IT act". This act must be in compliance with the general principles that govern the administrative activities' system, together with the relevant obligations of transparency and publicity.

The methodology to be used will be to connect the various aspects of a broader topic for the purpose of finding solutions related to the various problems.

In this context, big data plays a very important role in many ways within the health and pharmaceutical sectors and has already transformed various facets of the same sector. These huge datasets are leading to new drug discoveries and improving clinical trials more efficiently. For example, various devices allow researchers to monitor trial participants in real time, and healthcare professionals are enabled to predict and prevent illness in better ways[8].

From personalized medicine to assisted diagnostics to genetic engineering, the possibilities of AI are really endless. However, legal and regulatory challenges remain, especially after the introduction of EU

[6] AI includes tools with all the makings if used in healthcare sector. So much so that on February 19th 2020 the European Commission has approved a set of documents called *Shaping Europe's digital future: European data strategy and AI White paper*, putting in evidence how much the classic areas of European wellbeing, first of all healthcare, will benefit from AI. This package is composed of the "Commission Report on safety and liability implications of AI, the Internet of Things and Robotics", a "White Paper on Artificial Intelligence", the Communication about "A European Strategy for Data", and the Communication about "Shaping a digital future for Europe".

[7] N. BOSTROM, *Superintelligence. Paths, Dangers, Strategies*, Oxford University Press, 2017, 11.

[8] These words are from A.S. BERNE, *Big data in the pharmaceutical sector – between protection and transparency: Opportunities and legal challenges*, in *EPLR*, 2019, no. 1, p. 1.

Regulation no. 2016/679 (the General Data Protection Regulation – GDPR): taking into account that the digitalization of processes can lead to issues regarding the privacy.

Patient-centred health data contributes to patient outcomes whilst reducing wasteful spending in healthcare.

An area where the potential benefits of big data have been particularly significant, but also where data quality constraints have been evident, is healthcare and medical research[9]. The possible sources of this kind of information are the most disparate: Electronic Health Records (EHRs), medical records, medical literature, clinical trials, insurance claims data, pharmacy prescriptions, data entered by patients or recorded on apps or fitness trackers, etc.[10]

In this perspective, the field of emergency medicine is fundamental, considering that there are three main areas of AI use in emergency medicine: AI in predictive modelling, AI in patient monitoring, and AI in emergency department operations[11].

However, the potential benefits could be better quality healthcare, with interventions more precisely tailored to individual patients' circumstances if their medical and other data can be matched to extensive datasets. In fact, big data benefits depend on the quality of the datasets being brought together. Medical professionals are often concerned about the quality of hospital data because the data collection process is out of date and no longer appropriate for big data analysis. In some cases, premature conclusions are being drawn from the data because it is not rich enough. Moreover, the further away the interpretation of the health data is from the person who produced it, the more likely it is to be misinterpreted: this is why it would be appropriate to improve standardization and the way we record things.

In practice, digitalization is a major trend in healthcare, and the mining of health-related data is on the rise. Big data offers the possibility of deriving novel insights to support decision-making processes but also brings together unknowns with regard to data quality and hence the robustness of the evidence generated. It is also possible to distinguish between four different types and origins of health-related data: voluntary (collected through devices and software), obligatory (from insurance and health cards), explored (through patient-originated-research on the internet) and inferred (through assumptions from existing health data).

Some scholars have successfully pointed out that "there are many expectations and hopes for applying AI techniques in the medical field. First of all, the possibility of developing predictive models with obvious advantages in terms of prevention. Secondly, the ability to put in place early diagnosis, in order to guarantee a prompt reaction using the most appropriate care. Finally, the affirmation of chatbot-based

[9] See HOUSE OF COMMONS – SCIENCE AND TECHNOLOGY COMMITTEE, *The Big Data Dilemma. Fourth Report of Session 2015–16*, London, 12 February 2016, p. 23.

[10] See W. NICHOLSON PRICE, *Artificial intelligence in health care: Applications and legal implications*, in *The SciTech Lawyer*, vol. 14, no. 1, 2017, p. 10.

[11] See N. LIU, Z. ZHANG, A.F. WAH HO, M.E. HOCK ONG, *Artificial intelligence in emergency medicine*, in *Journal of Emergency and Critical Care Medicine*, 2018, no. 2, p. 82.

environments promises to guarantee the right information for patients, accompanying them in their care processes. AI could be capable of solving many problems in several e-health contexts. Intelligent virtual assistants, now embedded in smartphones or dedicated home speakers, like Microsoft Cortana and Apple Siri, but increasingly present in people's home devices, such as voice assistants Amazon Alexa or Google Assistant, are supported by systems with powerful AI features. These tools represent today the most advanced and captivating frontier of the use of AI to facilitate everyday life"[12].

The devices for healthcare can provide support for social assistance at the same time, this double utility reflecting the mixed need that part of the population, especially the older one, has.

The term "telecare", as a synonym of "telehealth", explains this concept well. In fact, telecare includes technical devices and assistive technology as well as professional healthcare services to assist, monitor and care for people from a distance[13].

Usually, the general objectives of telecare services are as follows: a) promoting the permanence and inclusion of dependent people in the context where they normally live; b) enhancing and keeping the degree of autonomy and independence of dependent persons at home; c) favouring the safety and trust of dependent persons; d) providing relief for dependent persons and their relatives; e) serving as support for carers living with the dependent person.

Therefore, healthcare and social assistance are two combined factors in the perspective of digitalization as a multitasking process: AI can contribute towards reducing the time spent on customer support and administrative tasks and increasing the involvement of citizens in the policymaking process. AI can also contribute towards better-informed decisions in the design of services and policies; for example, by fine-tuning the allocation of resources for health and social care services in different areas[14]. AI can also allow to pull data from various aspects of a person's assessments and care plans, searching and analysing

---

[12] See P. GUARDA, *"Ok Google, am I sick?": Artificial intelligence, e-health, and data protection regulation*, in *BioLaw Journal*, 2019, no. 1, p. 362, who adds that "particular conditions requiring elaborate treatment plans could benefit from AI tools during specific therapies. Incorporating an artificial intelligence system capable of automatically formulating plans based on specific conditions would provide value to both physicians and patients alike. This is the case of ecosystems designed to innovate the processes of interaction between physician and patient, with an evident impact also on the organizational models that regulate the performance of health services.9 These intelligent systems may look for inconsistencies, errors and omissions in an existing treatment plan or may be used to formulate a treatment based on a patient's specific condition and on accepted treatment guidelines. The intelligent agent can, furthermore, be used for finding information, for example on the Internet, relevant to a particular disease, integrating knowledge about user preferences and needs into such searches, or for automatically interpreting medical images (i.e. X-rays, angiograms, CT scans, etc.), becoming a formidable tool especially with regard to mass screens where the system could signal potentially abnormal images for detailed human attention. Finally, expert systems and decision support systems, programmed to aggregate and store a large amount of data modelled for specific purposes, can be successfully used in the field of medical devices in applications for cardiac monitoring and automated ECG, medical imaging, clinical laboratory analysis, and so on".

[13] Telecare includes a variety of services such as communication, monitoring, consultation, diagnostics and training: see PARLIAMENTS AND CIVIL SOCIETY IN TECHNOLOGY ASSESSMENT – PACITA, *Telecare Technology for an Ageing Society in Europe - Current State and Future Developments*, http://wp6.pacitaproject.eu/wp-content/uploads/2014/02/Telecare-description-web.pdf, Brussels, 2014, p. 9.

[14] EUROPEAN COMMISSION, *Report of the Expert Panel on effective ways of investing in Health (EXPH)*, Luxembourg, 2019, p. 4, http://ec.europa.eu/dgs/health_food-safety/index_en.htm .

unstructured text for key concepts to help social care and health service workers access information relevant to that individual. AI could also allow to reduce costs by enabling care workers to optimise people's health and well-being through offering general practitioners (GPs) preventative options, reducing visits to hospitals and emergency rooms, and driving competition among service providers[15].

It is estimated that telecare in Europe mostly includes lot of technologies: sensors and monitoring devices, detectors, alarm systems, communication devices, video or imaging devices, smartphone apps and specialised medical devices connected to the internet. In some country, videoconferencing and other remote services are available in devices used by people with disabilities, child welfare services and services for families with children[16]. It is also estimated that demand for Technology Enabled Care services will increase with the ageing of the population and care budget constraints[17].

The demographic changes are expected to increase the demand for telecare services thanks to population aging, greater confidence with devices (people is starting to gain confidence at new devices more and more), decreasing device costs and increased portability. Then, other factors work as an incentive to develop the use of AI tools, such as service quality, efficiency, security and inclusion in the perspective of service users. From the technological side, the general increase of wearable devices in all areas of society will increase both acceptance and use of telecare devices. Moreover, the interaction between devices is also predicted to improve over time. They remain, however, as barriers to further use of telecare, the legal, ethical and data protection issues, and the need to train staff and users.

Healthcare and social assistance can be in a mutual dependency relationship also regarding the use of robotics. In fact, the robot can prepare people for their care appointments and encourages them to do

[15] "Technology Enabled Care services are more and more designed to empower individuals to support themselves in their own homes and manage their own health conditions. For example, connected care services are able to detect smoke or gas or a person falling; the aim is ultimately to improve health outcomes. Many products and services are commercially available such as telecare devices, at-home alarms, activity monitoring, bed occupancy sensors (to notify possible falls), to allow users to live independently but receive social assistance when needed. The targets for these products include older people and people with disabilities. Such products enhance users' access to care services while also improving their inclusion since they can live independently instead of staying in hospitals or care homes. Introducing more monitoring services to provide 24/7 remote support via traditional and digital routes will create efficiencies of scale while helping older people to care for themselves. In other cases, the service enables online and video consultations for people with disabilities, child welfare services, psychosocial assistance for children and for families, support for child rights issues and other care services for children and multidisciplinary cooperation. The service combines various technologies for service providers, such as telepresence for consultations and other forms of co-working and information transfer forms for relaying confidential information, and allows communication between professionals and between professionals and users. Virtu.fi also provides services for citizens, such as online bookings, guidance and counselling (including via telepresence), and tools for measuring various personal health indicators. In social services the sectors of greatest development and perhaps of most interest are those related to teleassistance and the management of digital administration related to accessing social services. The traditional method of service delivery is changing, with greater emphasis now on how technology can support people through proactive alert monitoring rather than reactive response calls": see EUROPEAN FOUNDATION FOR THE IMPROVEMENT OF LIVING AND WORKING CONDITIONS – EUROFOUND, *Research Report on "Public Services - Impact of digitalisation on social services"*, p. 16.

[16] In particular regarding the Finnish experience, see T. KAUPPILA, K. KIISKI, M. LEHTONEN, *Sähköhelmenkalastus – Sosiaalihuollon sähköisten palvelujen nykytila ja kehittämistarpeet*, web page, available at http://julkaisut.valtioneuvosto.fi/handle/10024/160653, 2018, p. 25.

[17] see EUROPEAN FOUNDATION FOR THE IMPROVEMENT OF LIVING AND WORKING CONDITIONS – EUROFOUND, *Research Report on "Public Services - Impact of digitalisation on social services"*, p. 17.

things that they can still do themselves, like drinking an extra glass of water on a hot day or going for a walk. At the same time, it can help older people with rehabilitation exercises or taking a medicine or receiving healthcare.

As well data matching and data mining techniques are suitable for a mixed-use, such as to evaluate the eligibility for public benefits or to target sanitary inspections.

The digital technologies can also guarantee mixed advantages, including devices for security alarms and health checks together. Welfare technology reduces pressure on social and healthcare services by decreasing consultations, home nursing services and admissions to hospital. For example, the economic gains could achieve through the use of digitally supported training come from less commuting by therapists and fewer hours of therapy needed due to improvements in service users' condition.

Big data and AI are leading to radical changes in decision-making processes[18]. It would consequently be appropriate to analyse the paradigm shift that is occurring in the field of social and health services, along with its implications for constitutional and administrative law. The application of AI in administrative decisions regarding the sector at issue is very interesting. The overview will continue by reflecting on the radical transformations that are proceeding at great speed, underlining the main challenges that only through interdisciplinary approaches can be effectively addressed. In conclusion, some fundamental principles of a new constitutional and administrative law in the cybernetic era should be proposed.

Digital transformation of health promotion and disease prevention requires targeted oversight and safeguards for its full potential to be harnessed. Moreover, people who would most benefit from mobile health and other such digital tools may be the least likely to have easy access to it. More generally, health promotion and disease prevention pave the way for a more effective and efficient health system[19].

As an eminent Italian scholar has pointed out[20], today a growing number of decisions affecting human liberties are made by algorithms. This evidence raises a vast number of questions concerning the transparency of such tools, the legal and ethical framework for algorithmic decision-making, and the societal and cognitive impacts of such algorithmic automation. Therefore, the big challenge now is, on the one hand, to outline the inherent tension between AI and law and, on the other hand, to examine and critique the standards set by GDPR to provide effective protection for fundamental liberties.

---

[18] See D.A. HASHIMOTO, G. ROSMAN, D. RUS, O.R. MEIRELES, *Artificial intelligence in surgery: promises and perils*, in *Annals of Surgery*, 2018, vol. 268, no. 1, p. 70.

[19] The progress made thanks to AI show how the programs have acquired most of their content for learning, rather than for the original input. As a result, hearing prostheses filtering environmental noise, support for the medical diagnosis of tumors, drafting of therapeutic plans and ECG interpretation are available today (N. BOSTROM, *Superintelligence. Paths, Dangers, Strategies*, Oxford University Press, 2017, 40).

[20] See A. SIMONCINI, *The unconstitutional algorithm: Artificial intelligence and the future of liberties*, in *BioLaw Journal*, 2019, no. 1, p. 63. The author talks about a new doctrine of "precautionary constitutionalism" through which protection of fundamental rights and the rule of law should be granted within the designs of new technologies.

AI uses algorithms. Consequently, first of all it is important to focus the definition of algorithm, starting from the most basic one, as "organized sequence of calculations".

Algorithm is a word that derives from al-Khuwărizmĭ, nickname of the Arab mathematician Muhammad ibn Mŭsà who lived in the 9th century. It is an older concept than that of AI that collects and uses it.

According to a more innovative concept, algorithm is a mathematical system that answers a question or founds the solution to a problem. An algorithm that answers in terms of yes or no is called "decision procedure". An algorithm that answers providing a specific number is called "calculation procedure"[21].

Therefore any entity, public or private, that provides healthcare services can use the algorithm whenever it has to make a decision or answer a question from the patient. Algorithm has growing usefulness as it is used within standardized procedures that must answer a very high number of questions or make a lot of serial decisions. In such cases, algorithm takes a time of execution that is far less than that which a man would need and benefits from a memory much higher than that which is proper to a human being.

Nevertheless, the control of an enormous amount of data by a few companies puts people's confidentiality at risk. In more precise terms, AI allows a profiling of the political preferences of people, which seems to represent a specific risk to the pluralism that must characterize every democratic regime. Therefore, an unknown factor for the democracy's hold and for the freedom of expression on which this structure is based seems to materialize.

With the increase in computational calculation capacity and the connected growth in quantity and quality of data available today, the possibilities for profiling people can in fact be easily expanded to the field of political orientations. As often happens with internet advertising, whereby people are increasingly

[21] Ultimately, the algorithm is a process characterized by two essential requirements: a finite number of steps, on the one hand, and the finalization to a real and concrete result, on the other (*Algorithm*, in *Encyclopaedia Britannica, Micropaedia*, 15th Edition, 1985, https://www.britannica.com/science/algorithm). After algorithm and AI, blockchain technology has entered the economic and legal system since 2008, by offering new opportunities for use to public and private entities also in the health care and welfare services sector. According to the Italian legislation, blockchain uses so-called Distributed Ledger Technologies – DLT (see It. Legislative Decree 14 December 2018 no. 135, Article 8-*ter*). For doctrine, see F. VOTTA, *"Distributed Ledger Technology" and "Blockchain": considerations on the possible evolution of the public administrations digitalization*, in *www.giustamm.it*, 2019, no. 11. As recently clarified by the *Opinion of the European Economic and Social Committee on Blockchain and the EU single market: what next?(own-initiative opinion), (2020/C47/03)*, "Blockchain (hereafter BC) and distributed ledger technology (DLT) has the potential to transform society. BC is a mathematical structure for storing data in a way that limits corruption and fake data". In the meantime, "BC is defined as both a code, i.e. a communication protocol, and a public register, in which all transactions between network participants are recorded one after the other, with a high degree of transparency and in a way that cannot be altered". "BC is a technology for promoting user trust. It makes it possible to share on-line information, agree on and record transactions in a verifiable, secure and permanent way". "This opinion focuses on BC as a technology, which can be applied to a whole host of areas and industries such as energy, finance, food and agriculture, medicine and healthcare, elections and governance". As goal 3 "Good health and wellbeing and the opportunity in sharing patient healthcare records more securely and efficiently". Moreover, "these are self-executing contractual states stored on the blockchain which nobody controls and therefore everyone can trust. Examples are trade clearing and settlement, gift/loyalty coupons, electronic health records, royalty distribution, product provenance, peer-to-peer transactions, lending, insurance, energy credits, and voting". As noticed by European Commission, "in the area of social welfare, blockchain has been used by pension providers in the Netherlands to set up a pension infrastructure that allows tax authorities, employers and employees to monitor the contributions made by individuals in different pensions funds": see EUROPEAN COMMISSION, *Blockchain now and tomorrow: Assessing multidimensional impacts of distributed ledger technologies*, Luxembourg, 2019.

receiving offers corresponding to their tastes, such as information of a political nature – particularly electoral information, the risk is that people are exposed to very limited and specific information based on their presumed preferences. In this way, profiling can more easily include people's political leanings which are more and more influenced by big data.

Moreover, we must consider that AI tools are not perfect machines. In fact, AI also makes mistakes. Therefore, it is impossible to completely delegate to the machine an administrative procedure regarding the assignment of social benefits to the citizens: it is a fault of the system.

The same warning must also be applied in other fields. Let us take the example of hiring procedures. Sometimes the hiring procedure is managed only by the AI system by means of an algorithm and results in choices without any motivation, without the identification of an administrative official who assesses the individual situations or correctly outsources the related provisional decisions.

In an important case-law[22], regarding the hiring procedure precisely, the judge confirmed the plaintiff's perspective according to which the algorithm arranged transfers in one province rather than another, in a type of job rather than another, without taking into account the preferences indicated in the respective transfer requests, without any reason or the slightest transparency[23].

Thanks to these cases promoted by some teachers for the assignment of their place of employment, the concept of algorithm captured the attention of interpreters and operators of the law and, consequently, of scholars.

The administrative judge highlights the pros and cons of applying digital technologies to administrative decisions. In his opinion, the following should be appreciated: a) digitalization is important for improving the quality of services provided to citizens and users; b) the algorithm certainly guarantees the compliance with the efficiency and cost-effectiveness of the administrative action and the good performance of the public administrations; c) the advantages, in managing of repetitive and discretionary activities, achievable by excluding interference due to negligent or malicious conduct by the official as a human being, with the greatest guarantee of impartiality. They raise doubts instead: d) the fact that the technical rule that governs the algorithm is still a general administrative rule, managed by man and not by the

[22] Italian Consiglio di Stato, sez. VI, 13 dicembre 2019 n. 8472 has stated three fundamental principles: a) the possibility for the recipient to be aware of the decision-making processes; b) the non-exclusivity of the automated decision; c) the ban of discriminations due to the algorithmic decision. Similarly, sez. IV, 8 aprile 2019 n. 2270, and Tar Lazio, sez. III-bis,14 febbraio 2017 n. 3769. For doctrine, see S. CRISCI, *Evoluzione tecnologica e trasparenza nei procedimenti "algoritmici"*, in *Law of Internet*, 2019, no. 2, p. 380; G. MANCOSU, *Les algorithmes publics déterministes au prisme du cas italien de la mobilité des enseignants*, in *R.I.I.D.*, 2019, no. 1, p. 75.

[23] For further analysis of the debate about how best to achieve algorithmic transparency, from which several approaches have emerged in order to ensure and demonstrate the data protection compliance of 'black box' big data processing activities such as machine learning, see INFORMATION COMMISSIONER'S OFFICE, *Big Data, Artificial Intelligence, Machine Learning and Data Protection*, Wilmslow, 2017, p. 86; J.A. KROLL, J. HUEY, S. BAROCAS, E.W. FELTEN, J.R. REIDENBERG, D.G. ROBINSON, H. YU, *Accountable algorithms*, in *University Pennsylvania Law Rev.*, 2017, vol. 165, p. 633. The theory of transparency as an antidote to opacity is supported, among others, by F. PASQUALE, *Beyond innovation and competition: the need for qualified transparency in internet intermediaries*, in *Northwestern University Law Rev.*, 2010, vol. 104, no. 1, p. 160.

machine, and as such is subject to general administrative principles (reasonableness, proportionality, publicity, transparency, judicial control, etc.); e) the attempt to back the algorithmic rule out of control of the administrative judges, who are indeed obliged to verify the correctness of the automated procedures in all their phases and components.

In other words, the result of the application of the algorithm has been contested: consequently, IT administrative act was found illegitimate due to the irrationality of its results compared to the provisions of law.

Public administrations must also be able to exploit the significant potential of the digital revolution[24]. In this context, the use of computer algorithms for making decisions that affect the public and private spheres must be justifiable in terms of efficiency and neutrality. In many fields, algorithms promise to become the tool used to correct the distortions and imperfections that typically characterize cognitive processes and the choices made by human beings. These aspects, in particular the limits of human beings, have been highlighted in recent years by an impressive literature of behavioural economics and cognitive psychology. In this context, the decisions made by the algorithm thus take on an appearance of neutrality, the result of aseptic, rational, data-based calculations.

What should be clear is that without human control, the defects of an automated device may produce effects that are contrary to the expected ones: complication instead of simplification, partiality of results instead of completeness, and irrationality of outcomes instead of equity and plausibility[25]. Then, the more the activity to be performed is discretionary in nature, the more the limits of the automated procedure will become evident[26].

2. *The European regulatory framework: promoting the use of AI*

EU competencies in health protection have been increasing throughout the years, although without affecting the powers of the Member States that remain responsible for the organisation and funding of health and social care.

Reaffirming the greater adequacy and incisiveness of its actions in certain fields, the European Union has acquired competence in social and health matters that is cross-sectoral and horizontal. As such, it is capable of justifying its influence on any other policy with the objective of "ensuring a high level of human health protection" (Article 168 TFEU).

[24] D.K. CITRON, F. PASQUALE, *The scored society: due process for automated predictions*, in *Washington University Law Rev.*, 2014, no. 89, p. 1, discusses "technological due process".

[25] See R.C. LAWLOR, *What computers can do: analysis and prediction of judicial decisions*, in *American Bar Association Journal*, 1963, no. 49, p. 337; R. KEOWN, *Mathematical models for legal prediction*, *2 Computer L.J.*, (829) 1980, p. 6.

[26] See M. BOVENS, S. ZOURIDIS, *From street-level to system-level bureaucracies: how Information and Communication Technology is transforming administrative discretion and constitutional control*, in *Public Administrative Review*, 2002, p. 66.

In particular, through its actions, the EU can complete the measures adopted by individual Member States: promoting public health and disease prevention, encouraging cross-border cooperation in their services and stimulating the technological innovation of national welfare systems.

Therefore, through a considerable set of soft-law acts, the EU has supported the implementation of e-health projects, among them the realisation of health information networks, the use of electronic health records and digital health records, telemedicine services and portable monitoring systems.

Most recently, building on Articles 16 and 114 TFEU, in addition to Article 168 TFEU, the European Commission adopted a set of acts aimed at promoting the creation of a digital single market in the health and care sectors. The objective of these initiatives is to enhance digital health data to provide targeted and personalised treatments to citizens, making them active participants in the management of their health, as well as in a more efficient and effective use of the available resources.

The contents of the "*European Commission, State of Health in the EU – Companion Report 2017*"[27] are very interesting and can be summarized as follows:

• Patient-centred care and patient empowerment require general knowledge about self-care and self-management but also "soft skills" such as communication and teamwork. Indeed, soft skills become increasingly important in conjunction with (and not separate from) the digital transformation of health and care, as patient-centredness and patient empowerment are facilitated by, for instance, e-health, mobile health (mHealth) and individual access to electronic patient records;

• The spread of digital technology is currently revolutionizing traditional clinical practice. Indeed, the expansion of eHealth is leading to new ways of care delivery, requiring a new mix of skills, such as information or interpretation for detailed genetic assessment so as to improve diagnosis and treatment;

• The implementation of the next stage of development in e-health infrastructure, such as electronic medical records in primary care, e-prescriptions and patient registries, will not only contribute to longer-term efficiency of health-care spending but will also enhance the quality and continuity of care for patients. A digital strategy is necessary;

• Technology is also a strong driver of patient empowerment: tailored apps and smart portable devices provide effective support for healthy lifestyles and for involving the patient directly in the management of chronic conditions. Finally, strongly related to the Digital Single Market Strategy, advanced information and communication technologies will allow for the creation of large and interconnected databases of medical and health data. At the same time, new technologies are a key driver of health spending and its projected growth. It is therefore crucial to carefully evaluate the cost-effectiveness of new technologies and assess what works and does not work for patients and providers. In order to reap the benefits of

[27] The text of the Report 2017 is available at the following link: https://ec.europa.eu/health/sites/health/files/state/docs/2017_companion_en.pdf.

technology and effectively enhance the quality of care, it requires adequate training of the health workforce, as well as a supportive environment in terms of professional culture, incentives and organizational arrangements.

A comprehensive set of actions within the digital transformation of health and care, part of the Digital Single Market Strategy, has been provided in a specific Commission Communication[28].

In particular, the 2017 Commission Communication on the mid-term review of the Digital Single Market Strategy recognizes an advanced data infrastructure with citizens' secure access to their electronic health records and patient empowerment through interaction with health-care providers as key features of the digital transformation of health and care.

The subsequent "*European Commission, State of Health in the EU – Companion Report 2019*"[29] should be noted for its importance, and its highlights are worthy of reporting:

• Building on the 2018 Commission Communication enabling the digital transformation of health and care in the Digital Single Market, the new Report looks at its potential for health promotion and disease prevention. Digital solutions, such as apps, wearable technology and online fora, hold great potential for health promotion and disease prevention, with best practice examples emerging across the EU. These innovative approaches help raise awareness and empower citizens to take control of their healthy behaviour and lifestyle choices. Digital solutions should, however, always be seen as part of a broader, comprehensive health promotion and disease prevention strategy;

• Digital platforms and environments could become a new health promotion setting, requiring targeted oversight and safeguards, with a particular focus on stepping up digital health literacy. A host of associated barriers and risks require consideration at the European level, with a bearing on – inter alia – interoperability, privacy and reimbursement criteria. Policy efforts should also take into account digital health literacy so that mHealth can be used appropriately and by all. Harnessing the potential of digital solutions for health promotion and disease prevention will depend on an openness to these innovative technologies combined with a critical understanding of their success factors;

• A good health promotion strategy includes digital tools, services and platforms having great potential when it comes to health promotion and disease prevention. Such digital solutions, be it apps, wearable technology or online fora, may empower people to enjoy a healthy lifestyle and prevent them from developing illnesses. Some mHealth tools even highlight early symptom or disease indicators, provide feedback to health workers and assist in patient adherence to treatment programs. These digital solutions

[28] See the 2017 Commission Communication on the mid-term implementation review of the Digital Single Market Strategy, Brussels, 5 October 2017, COM(2017) 228, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1496330315823&uri=CELEX:52017DC0228.

[29] The text of the Report 2019 is available at the following link: (https://ec.europa.eu/health/sites/health/files/state/docs/2019_companion_en.pdf.

also open up new inter-sectoral avenues to health determinants, such as transport, urban planning and the environment.

In other words, apps, wearable technology and online fora can all empower people to enjoy a healthy lifestyle and prevent them from developing illnesses.

However, digital solutions may give rise to new or increased inequalities between people who do and who do not have the skills to harness their potential. Similarly, varying levels of national or regional support for the rollout of digital health solutions can have an impact on who is given the possibility of benefiting from these tools, thus exacerbating inequalities. Employing digital solutions to strengthen health and well-being will require equal digital opportunities, widespread digital literacy, strong digital security and well-designed, effective tools, services and platforms[30]. EU Member States are required to exchange experiences, transfer best practices and develop common approaches to support the uptake of mHealth solutions for better health promotion, disease prevention and chronic disease management.

No less significant is the 2018 "*Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society*"[31].

This Communication:

• stresses that health information portals, smartphones and mHealth apps can empower citizens to take a more active role in looking after their health and changing their health behaviours. It also recognizes that the uptake of digital solutions for health and care remains slow and varies greatly across Member States and regions, so that it is very important to promote a uniform level common to all countries;

• underlines that the WHO also acknowledges that mHealth can improve access to health information and promote positive changes in health behaviours to prevent the onset of acute and chronic diseases. In particular, the organization sees the use of mHealth tools as a good opportunity for increasing awareness to bring about changes in the key risk factors for non-communicable diseases and for increasing patient, family and community involvement.

The same Communication takes charge of resolving the problems represented by the presence of diversified national models and non-interoperable technologies. For this purpose, it offers support to Member States in terms of funding and actions aimed at promoting, on the one hand, the political cooperation and exchange of best practices across the different national health and care systems and, on

[30] See the 2019 OECD report "How's Life in the Digital Age? Opportunities and Risks of the Digital Transformation for People's Well-being", https://www.oecd.org/publications/how-s-life-in-the-digital-age-9789264311800-en.htm.

[31] The Communication is available at the following link: https://ec.europa.eu/digital-single-market/en/news/communication-enabling-digital-transformation-health-and-care-digital-single-market-empowering.

the other hand, the sharing of genomic data or other health data needed for the progress of research and personalised medicine.

As rightly pointed out, thanks to this act, "[artificial intelligence is hereby introduced, for the first time, in the European documents that expressively address the digital health with reference to health data, as an essential technology that, operating on such data, opens new care perspectives, new forms of disease prevention and personalised treatments]"[32].

Ultimately, health information portals, smartphones and mHealth apps can help citizens to take a more active role in looking after their health and changing their health behaviours.

However, the regulatory European framework within which the new AI technologies in the field of health and social care should be placed is not well-defined yet.

Currently, the framework is composed of some legislation focused on another primary matter but that are applicable also to the sector at issue on the basis of the possible intersections with it: for example, the legislation on medical devices, electronic identification, the security of networks and information systems as well as the protection of personal data.

In other respects, the only specifically and directly relevant act is the European Parliament Resolution of 16 February 2017 with recommendations on Civil Law Rules on Robotics. The Resolution is not limited to dealing with the dimensions regarding the civil liability for damage. It also provides valuable information on the principles that should drive the introduction and use of robotic technologies with social benefits for elderly and disabled people and national health services[33].

As discussed in the next paragraph, privacy issues, consent and access to personal data are some of the main issues identified in implementing digitalisation strategies and using digital technologies in social services, therefore some mitigating measures are needed.

The difficulties of ensuring privacy could affect the development of digital services. This risk is higher when the trust of the service user is lacking: because in some cases in an illegal way the State kept the data of users; or medical data has been stolen from devices that are connected to a records system or used to send targeted advertising messages and even to blackmail patients.

---

[32] *See* E.A. FERIOLI, *Artificial Intelligence in social and health services: a new challenge to the role of public institutions in Italian welfare?* in *BioLaw Journal*, 2019, no. 1, p. 168.

[33] E. MACRÌ, A. FURLANETTO, *Robots between myth and reality interacting with people in social environments and hospitals. An approach through risk management and law*, in *Riv. It. Med. Leg.*, 2017, no. 3, p. 1045, which points out the first strong position adopted by a European authority on the need to introduce effective rules in the matter of robots and artificial intelligence, has highlighted all the legal, ethical and economic contradictions related to the massive introduction of such technologies in daily life. Regarding the main liability issues of a cutting-edge robotic surgery application, *see* G. GUERRA, *Comparative law, and robotics: reflections on American "litigation" regarding robotic surgery*, in *Dir. Inf.*, 2016, no. 2, p. 157, who argues that further studies on a tight relationship between law and the brain sciences is basically important in order to reach an authentic interpretation of new robotic functions and their legal implications. For an in-depth examination of the interaction between robots and human beings and its ethical and legal effects, s*ee* A. BERTOLINI, *Human-robot interaction and deception*, *in Oss. Dir. Civ. Comm.*, 2018, no. 2, p. 645.

Therefore, in principle, strong data protection safeguards should accompany increased use and analysis of data to ensure that the user consents to the use of their data and that data are anonymised where possible[34].

3. *AI tools and the protection of constitutional rights: a case analysis.*

As aforementioned, artificial intelligence (AI) has for a long time had a number of applications in the health sector, giving rise to many advantages in terms of, inter alia, tests, robotic surgery, remote diagnosis or medical care for elderly people and vulnerable groups: it is clear, then, that the promotional approach adopted by the same European Commission on several occasions has underlined the benefits in terms of cost reduction related to the digital transformation of healthcare and social assistance.

Looking at these dynamics, the interpreter dutifully takes on the task, primarily ethical rather than legal, of subjecting the new devices to the assessment of compatibility with the system of guarantees and of the inviolable human rights constitutionally enshrined: personal freedom and its specific facets (Article 5 ECHR; Article 13 et seq. Italian Constitution); the right to the protection of personal data (last protected by the Regulation (EU) 2016/679 – GDPR); and the right to good administration (Article 41 – Charter of Fundamental Rights of the European Union).

The last-mentioned right requires, in particular, that the decisions taken by a substantially public entity be adequately justified. This leads to the affirmation that although human intelligence can be supported by an artificial one, it cannot be entirely replaced by the latter (see Article 22 GDPR)[35].

In the medical field, the risk of violation of above-mentioned Article 22 perhaps is lower than in other sectors. As more advanced AI applications are used in the medical field, the human being's contribution is not entirely excluded.

---

[34] See LOCAL GOVERNMENT ASSOCIATION – LGA, *Transforming social care through the use of information and technology, London*, 2017. For the healthcare sector, it has been recommended appropriate training and skills development in privacy and security measures for processing personal health data. An adequate training and skills development are required for social services as well. It is a challenge for staff to ensure that data is collated, shared and used in a way that reassures service users that their data is protected; therefore, it is vital that training is provided to improve skills in this area. For further details see OECD, *Recommendation of the Council on Health Data Governance*, Paris, 2019.

[35] For more details on this general ban, *see* G. NOTO LA DIEGA, *Against the dehumanization of decision-making –algorithmic decisions at the crossroads of intellectual property, data protection, and freedom of information*, in *JIPITEC*, vol. 9, 2018, no. 3, p. 17; S. WACHTER, B. MITTELSTADT, C. RUSSELL, *Counterfactual explanations without opening the black box: automated decisions and the GDPR*, in *Harvard Journal of Law and Technology*, 2018, no. 31(2), p. 841; DATA PROTECTION WORKING PARTY, *Guidelines on Automated Individual Decision-making and Profiling for Purposes of Regulation 2016/679*, 6 February 2018. Regarding the healthcare sector, see E. BEGOLI, T. BHATTACHARYA, D.F. KUSNEZOV, *The need for uncertainty quantification in machine-assisted medical decision making*, in *Nature Machine Intelligence*, 2019, vol. 1, no. 1, p. 20. As noted by another author, although a rule any algorithmic decision, which has a significant effect on individual, is prohibited, nevertheless the scope of this provision is still narrow, since it refers to fully automated decision-making, and may be easily circumvented by including a merely formal human intervention in the decision process, with no influence on the outcomes of that process: see P. SAVONA, *Administrative Decision-Making after the Big Data Revolution*, in *www.federalismi.it*, no. 19/2018, p. 32.

An example is provided by telemedicine, which is meant as a way of supplying healthcare services through innovative information and communication technology (ICT) capable of mitigating circumstances in which the health professional and the patient, or even two professionals, are not in the same location[36].

Therefore, in such cases, the human operator still has the main role together with the responsibility for the interpretation of symptoms and reports so that the technical progress is not exposed to the risk of failure and biases of calculation systems that end up breaching the most relevant freedoms of the individual, among which the right to the protection of health is paramount according to the International, European and Member States laws.

At most, regarding to the informed consent, the problem arises of making the information's content clear when explaining the purposes of the processing. This is due to the fact that the group of the users of personal data could depend on the specific arrangement followed: telemonitoring and telerehabilitation usually involve the operator and the patient, while teleconsultation extends the scope by making possible the contact between a remote facility and a specialised centre.

Another example is minimally invasive surgery. In this field, automated tools (such as the Da Vinci, Prebot, Star or Watson robots) perform surgeries under the control of the operator whose contribution is therefore preserved.

Obviously, we should not disregard the importance of the predictive values of any algorithm that is able to forecast complex phenomena and to rapidly and simultaneously collect and process big quantities of data[37]: advancing a diagnosis, calculating the probability of the onset of a disease or the statistically relevant factors regarding the incidence and spread of an epidemic represent beneficial achievements for the future of human beings.

At the same time, the support of the analysis of cases not otherwise easily solvable or the performance of a service with low technical complexity should not hide the fact that it is not possible to delegate everything to machines to the extent that the human being is completely excluded from the basic choices, and his/her dignity is voided.

---

[36] Regarding the general framework see EUROPEAN COMMISSION, *Communication Com(2008)689 on telemedicine for the benefit of patients, healthcare systems and society*, 4 November 2008, whose aim is to support Members States in achieving large-scale and beneficial deployment of telemedicine services, by building confidence in and acceptance of this new technology, taking into account that the level of telemedicine spread must be measured both on the demand side (citizens) and on the supply side (healthcare facilities). Therefore, Member States are warmly invited to assess and adapt their national regulations enabling wider access to telemedicine services, by addressing issues such as accreditation, liability, reimbursement, privacy and data protection.

[37] J.M. BALKIN, *The Three Laws of Robotics in the Age of Big Data*, in *Yale Law School Faculty Scholarship Series n. 5159*, 2017, available at the following link: http://digitalcommons.law.yale.edu/fss_papers/5159, talks about the "society of the algorithm".

The mark of the natural person and, in this case, of the health operator cannot be suppressed: in fact, in considering the scope of any AI, the right to substantiation and review of the automated decision – and not only the logics applied to take it – has increasingly been taking root.

It has been pointed out that even if the medical action does not benefit from a specific constitutional guarantee in terms of the obligation to state the reasons, "[it is possible to doubt the total legitimacy of a medicine that bases its decisions on computer operations for which none can ensure understanding and control]"[38].

In other words, the outcomes of robotic procedures must be in compliance with the legislative provisions and with the purposes therein admitted; in addition, the arrangements and rules that are the bases for the setting of a procedure must be clear and *ex post* verifiable.

Some very salient issues are the rights to freedoms and the right to self-determination in particular: it is the right that is expressed through informed consent and that authorises third parties, for example, to subject the consenting person to a medical action or to personal data processing for various purposes.

From digital clinical records to paperless prescriptions and electronic health records, new problems emerge regarding the protection of a patient's information from interference that is undue and not authorised by the data owner.

The regulation of these cases suggests following the personalistic model that, on the one hand, enhances the relationships between patients and health professionals and, on the other hand, prefers a patient-focused approach to treatment in which the informed consent provided by the patient is a core element.

In the various scenarios described above – (i) computer-based storage and processing of data regarding people's health status in e-health forms, (ii) predictive or probabilistic analysis of the patient's clinical situation on the basis of algorithms in telemedicine, and (iii) setting and execution of robotic surgery – the protection levels and the response instruments used to prevent the possible breach of human fundamental rights and guarantees should be shaped with regard to the circumstances in these scenarios.

In sectors in which subjective rights and constitutional values should be considered, the employment of cutting-edge technologies requires, in general, a careful updating, if not a real reshaping, of the regulatory principles of the sectors affected by scientific progress.

With regard to e-health, the most important type is represented by the electronic health record, which collects digital or digitalized data and documents regarding patients' health.

bringing together patient's health and social-health digital or digitalised data.

In the context of the computerisation of health data to which Member States may introduce further conditions and limitations (see Article 9, Par. 4, GDPR), the electronic health record has been subject,

[38] See C. CASONATO, *Constitution and Artificial Intelligence: an organizer for the next future*, in *BioLaw Journal*, 2019, no. 2, 718.

since the very beginning to a set of restrictions concerning the establishment, subsequent inputting and access that is guaranteed only to the patient and the authorised health staff.

The electronic health record also requires the data subject's consent. In various Member States, including Italy, this consent has not been expressly retracted, not even after Article 75 of the Privacy Code – in its new formulation *post* Legislative Decree no. 101/2018 and in compliance with the provisions of Article 9 of the same GDPR – eliminated the necessity of consent for data processing for treatment and diagnosis purposes.

Regarding telemedicine and robotic surgery, the most relevant aspects are: principles of and rights to proper functioning in terms of quality of data and process; the responsible programming and execution of surgeries; the justification of the choices made and the possibility of contesting them before a judge[39]; equality and equal access to the new opportunities provided by technology; and the protection of dignity and freedom of self-determination of the individual.

The final topic which remains to be dealt with came to the fore in social and mass media chronicles after various governments expanded the range of measures required to face the health emergency caused by the spread of the virus known as Covid-19.

There are issues concerning the announced "launch" of the apps for contact tracing. These tools have valuable potential for tracking the spread of the virus, but their compatibility with the supreme principles of modern constitutional orders have yet to be verified[40].

---

[39] A. SORO, *Democrazia e potere dei dati*, Milano, Baldini+Castoldi, 2019, p. 181, highlights how, in the case of entirely automated decisions based on a contract or consent, the recipient has a power no longer merely preventive but also responsive that results in the right to: a) obtain human action on the process by the owner; b) express his/her opinion; and c) contest the adopted decision. Similarly, with regards to the use of AI in the procedural field, it is worth mentioning the significant comments by D. PAVLI, *Partly dissenting opinion in CEDU Judgment, second section, 4 September 2019, Application no. 39757/15, Einarsson and others v. Iceland*: "Emerging practice in the Council of Europe area is in line with this general approach. Thus, courts in at least two jurisdictions (the United Kingdom and Ireland) have approved in recent years the use of technology-assisted review, employing a form of artificial intelligence known as predictive coding, for the purposes of electronic disclosure in high-stakes civil litigation. The rationale would apply with equal force in criminal cases of comparable complexity. Again, the underlying premise for the use of such advanced technology is, of course, that both sides are granted the fullest possible access to begin with. And, secondly, that criminal-law frameworks and investigative practices are organized in such a way as to facilitate adequate access for the defense at the appropriate (that is, early) stage of proceedings".

[40] As stated in the Circular of the Italian Ministry of Health of 25 March 2020 – "[Updating of the organizational guidelines for hospital and territorial services during the Covid-19 emergency]", considering that the systemic use of the emerging technologies (data analytics, artificial intelligence) and of telemedicine (teleconsultation, telecare) in other countries in the world has already proven to give very effective contributions to monitoring of and containing the infections from Coronavirus SARS-CoV-2, it is appropriate to select the technological solutions of telecare for home-based patients (both for Covid-19-related diseases and for other diseases, including chronic ones), the best technologies and solutions for continuous tracing, alerting and prompt control of the level of exposure of people to the risk and, subsequently, of the epidemic's evolution across the territory. This is to allow the Ministry of Health and the Istituto Superiore di Sanità, in collaboration with the World Health Organization, to evaluate the best digital solutions available with respect to telemedicine and home-based care apps and technology-based tools and strategies for the "active" monitoring of the infection risk and to coordinate at the national level the adoption and use of these technological solutions in order to improve the results in terms of monitoring and contrast of the spread of Covid-19.

In the framework of the AI-health protection relationship, there is vital interest in exploring any abstractly useful proposal to support the policies aimed at contrasting the spread of the pandemic. Policies regarding the use of the technology with purposes of monitoring and prevention of infections should be precisely delineated.

The health, social and economic emergency related to the recent and rapid large-scale spread of the coronavirus obliges policymakers and those responsible for institutions and the care of people to verify the effectiveness and sustainability of the measures that can be adopted for the eradication of the disease and the overcoming of its many negative effects in citizens' lives.

Some rightly point out that if the aim is to decisively take the path back to normality, it seems impossible to disregard the use of tracing systems that monitor movements and personal contacts, mainly by using specific apps that can be installed on users'/patients' smartphones.

Indeed, it seems impossible to renounce mechanisms that allow concerned people to be informed about the presence of people who tested positive or that facilitate the identification of asymptomatic people who should be subjected to quarantine.

In the debate, there is also strong defence of the following scheme. Citizens going outside should know if there are virus-positive individuals among those whom they have been in contact; once at home, they should know if they in turn have been infected; if they have symptoms but are not able to go to a hospital or first aid facilities because of restrictions by authorities, they should receive prompt and adequate diagnoses and treatment care by the operators who receive their phone requests[41].

Given these circumstances, apps can complement the other measures – swabs and protective devices (gloves, masks, etc.) – capable of containing the spread of the virus and limiting its reproduction capacity.

The identification of infected individuals, their isolation and retrospectively reconstructing their interpersonal contacts should be considered as the basic steps in the operational chain.

From the perspective of safeguarding of human fundamental rights, which have to be balanced with the effectiveness of the instrument adopted, it is necessary to be aware that to identify the legal basis legitimising the use of an app, mandatory or voluntary, the app's specific functionality should be considered as a dependent variable.

In this regard, the potential of an app is limitless, as demonstrated by experience: mass screening; the provision to users of useful telephone numbers or updated information and insights about the epidemic's trend; the regular detection and control of clinical parameters; geolocalization; remote medical support;

[41] In the list of the recommendations contained in the Circular of the Italian Ministry of Health of 27 March 2020 for the management of immunosuppressed patients during the Covid-19-emergency, it should be pointed out in particular the following: g) activate, whenever possible, telemedicine examinations, except for clinic and/or treatment needs, to prevent as more as possible the access to hospital first aid facilities.

remote monitoring of virus-positive and/or isolated patients; the transmission of alerts or warnings to individuals who present suspicious symptoms or who have been in contact with infected patients; verifications of compliance with the measures of social distancing and obligation to stay at home; and the transmission of information to police forces in order to facilitate the execution by them of institutional purposes. All these objectives are abstractly compatible with the multifunction purposes of an app designed for contact tracing. And, in all likelihood, the app could perform a variety of other functions.

The app is one of the significant examples of devices instrumentally intended for tracing health and pharmaceutical products, able to dialogue with IT company systems and to interface with clinical records, or to drive the dynamics of home-based care or guide the correct administration of drugs and treatments, or to perform predictive analyses about patients' health status, or even to rationalise the expenditure processes for the supply and storage of materials purchased.

In its evolution, the multilevel legal order has been including the development of protections in the case of the processing of health data with the use of computer technologies. The purpose is to make the processing of sensitive data lawful.

Among others, examples are provided by the following rules:

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

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

At the national level, many legal orders have established similar and very significant rules. The Italian privacy code, for example, provides that: a) the measure to safeguard the processing of health, genetic and biometric data must take account of the scientific and technological developments in the sector addressed by the same measures; b) the principles of the continuous application of protection measures to data regarding health must always be expressly safeguarded; c) the data subject's consent is still required for

the processing operations related to the use of medical apps through which autonomous controllers collect personal data, as well as health data, for purposes other than telemedicine or when, regardless of the purpose of the application, the data subject's information can be accessed by subjects other than the health professionals or other individuals bound to professional secrecy; and d) sensitive data that could reveal a person's health status can be processed only through organizational arrangements such as encoding or encryption techniques that make the data subject not identifiable.

As mentioned above, the legal basis for the lawfulness of the processing should consider the specific characteristics of the assessed device's purposes. The prediction of virus-positive cases and/or the prevention of infection outbreaks may require measures that limit personal freedoms for the benefit of public health.

Given the sensitivity of the matter and the legal and social effects of contact tracing through an app, it seems reasonable to affirm that the functional characteristics of the app be validated at its origin and controlled during its employment by the policymaker who provides or promotes its adoption and who subsequently must manage it, guiding the use of it by the masses responsibly.

The topic of health apps was addressed during the application of legislation prior to the EU Regulation 2017/745 on medical devices. This earlier legislation concerned software embedded in a device or constituting a medical device regardless of the technological support used.

In general, in regulating a single application of AI, the assessment of the impact on privacy is crucial, so it is important to put the need for personal data protection at the centre of the humans-science and freedoms-technological progress relationships.

The specific informed consent as a tool can, however, prove to be a restriction that limits in a disproportional way the concrete benefits achievable by AI: the sharing and processing of a huge quantity of data – as shown in the example of precision medicine or scientific research based on the use of genetic data and samples stored in biobanks[42] – may generate considerable treatment benefits for people, provided that a rigid imposition of the voluntary scheme does not substantially frustrate its potential[43].

If so, then the consent required for the creation, inputting and updating of an electronic health record may not be vital in the case of apps like the ones at issue.

In the case of electronic health record, the consent means as such to accept the purposes of a data processing likely to essentially affect the personal sphere of the consenting subject.

In the case of apps for contact tracing, the debate is mainly about public health purposes. In this perspective, the legislative act may represent the lawfulness condition of the processing, especially if the

[42] See J.E. LEE, *Artificial Intelligence in the future biobanking: current issues in the biobank and future possibilities of artificial intelligence*, in *Biomedical Journal of Scientific & Technical Research*, 2018, vol. 7, no. 3, p. 1.

[43] See C. CASONATO, *Artificial intelligence and constitutional law: first considerations*, in *D.P.C.E.*, 2019, special booklet, p. 108.

collected data is processed in a basically anonymous and aggregated form, as well as if its confidentiality and integrity are preserved across the transmission procedure through the relative infrastructures.

Therefore, alternatives to the consent-centred perspective are not absent. Indeed, the ability to ensure the effective anonymity of data goes beyond the outreach of the GDPR (see Recital 26) and the urgent and absolute obligation of ensuring the maximum level of privacy. The enactment of a legal act authorising the data processing for public interest reasons in the field of public health [Articles 6, 9, Paragraph 2, lett. *i*), Art. 23, Par. 1, lett. *e*), Recitals 41, 46 and 50] is a sufficient justification for the processing.

Furthermore, the consent, in addition to being technically unnecessary, sometimes may also prove to be counterproductive[44]: suffice it to say that providing for its acquisition at all costs corresponds to the exercise of the rights under Article 7 GDPR, among which is the right to the withdrawal of the same consent, with the risk of deleting the data previously collected and enhanced, which would have easily deducible detrimental effects at the expense of the planned public health purposes.

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

Nevertheless, it should be clear that if privacy consent may not be necessary in cases such as the one at issue, the voluntary aspect seems not likely to be attenuated in the overall architecture of a contact-tracing policy via smartphones, but quite the contrary.

At this point, the above-mentioned legal basis for personal data processing is no longer relevant. What is relevant, upstream, is the legal basis of any obligation to participate in the mass screening. Such an obligation, from time to time and depending on the features of each app, can be detected in the constitutional provisions that legitimise mandatory health treatments and limits to personal freedom and to the freedom of movement, stay and meeting people.

The assumed obligatory nature of joining the contact-tracing project might undermine its success anyway, given that the achievement of a minimum but high threshold of participants (for example, 70%? 80%?) seems essential for this purpose.

The difficulty of enforcing such an obligation, although formally justified and theoretically complemented by sanctions, would lead to the highly predictable circumstance that a project that has an inspiring rationale not accepted or shared by the target people may be easily obstructed. People may avoid downloading the app, switch off their mobile devices, deactivate the network connections, enable the airplane mode, or simply not carry it. It is also not certain that all eligible individuals for the project would have a smartphone.

[44] See P. QUINN, *The anonymization of research data – a pyric victory for privacy that should not be pushed too hard by the EU data protection framework?* in *European Journal of Health Law*, 2017, no. 24, p. 14.

With reference to the effectiveness of the operation, the initial input should logically originate from the reporting of the doctor who, having correctly detected and interpreted the symptoms, shall be required to record the infection case in order to initiate the contact chain that allows identification of the areas with a potentially higher risk.

Therefore, the preferable and most successful approach seems to be encouraging the free and voluntary participation of the citizen in installing and using the app, perhaps by providing incentives for this purpose. Such incentives could include data anonymity and a guarantee of non-reidentification; excluding the processing of such data for secondary and different purposes, e.g., police controls; the assurance that this data will be deleted at the end of the program; a commitment to respecting the privacy of the participant's family; the adoption of technologies compatible with data encryption (e.g., Bluetooth); the assurance that data will be stored in the user's device rather than an external facility; the prior definition of actions to be taken in the case of data breach or of risk that data is unlawfully processed; the promise of an appropriate privacy protection training of the staff that will use the concerned equipment; scientific evidence of the real effectiveness of the initiative in an epidemiological perspective; prohibiting the transfer of the owned data outside the European Union; renunciation of processing genetic data; and various material rewards (e.g., phone top-up, fiscal bonuses or other measures that do not breach the principles of equality, equal treatment and non-discrimination in the access to essential provisions and services or basic economic provisions).

It is not conceivable to reserve access to information channels or special treatment programs only to those who join the app program, or to provide swabs or protection devices only to the participants. It may be possible to allow the program volunteers a higher freedom of movement and participation in public life – including the use of services that are not considered essential and are particularly prohibited because of the spread of the virus – precisely because of the tracing done by those managing the system.

Throughout this program, only data strictly needed to fulfil the intended purposes will be collected, reducing as much as possible the risk of improper uses or possible external attacks to a system that, in any transmission between its various users (patient, doctor, health facility, data manager), is able to make the app user's IP address not intelligible and, in any case, not associable to the user's personal details.

Focusing on the confidence element also means building trust regarding the fact that the public subject is responsible for the entire range of management, storage, ownership and responsibility reports of the processing of the data collected. This should be done upon an appropriate exploration of the different competencies among State and Regions in this specific matter.

At the same time, a stable and balanced mix of personal freedoms and social aspects, of rights of individuals and need of solidarity for anyone, and of the individual and collective dimensions of the right to health protection represents the most solid foundation for an effective emergency legislation.

Ultimately, if the aim is to promote an extensive public health program inspired by noble prevention, diagnosis and care purposes, it is necessary to boost citizens' confidence that by cooperating with the management of the emergency system, a civic duty is carried out, and personal and egoistic interests are served. Such a program can be enhanced by fair incentives, and the risks of abuses and aggression should be curtailed.

The element of citizens' confidence in institutions remains the keystone of the system, as shown by other experiences (e.g., the electronic health record example)[45]. Otherwise, if based on an obligation to participate, the initiative would be unsuccessful and compromised since there is not a legal and especially practical basis for such an obligation.

In addition, the confidence in the proposing authority could lead the patient to urge the connection and updating of the clinical record and electronic health record with Covid information, or to request, through the inputting of the required data, a feature that provides local assistance, along with the assurance of self-distancing.

In conclusion, to defeat t Covid-19, it is necessary to take a further step forward in the universe of potential offered by new technologies, expertly regulate the law-science relationship and take on responsible risk management.

In a context where the evolution of the epidemic and the setting up of treatments addressing the disease are unknown factors, the backward mapping of the contacts by those who have been infected is increasingly essential.

First, it is necessary to detail the functions that such a software must guarantee, taking into account three primary criteria for contact tracing: 1) who (detection of the health status); 2) where (geolocalization); and 3) with whom (relationships with others).

Actions intended to really mitigate and prevent the spread of infection cannot disregard the identification of the relations with potential risk, defining the most exposed areas and subjects (in terms of symptoms, pre-existing diseases, age, and others) and aiming to provide indications about the behaviours to adopt (asking for a test, staying in self-isolation, etc.).

Tracing the interrelations between individuals at risk, wherever they happen (means of transport, in shops and retail establishments, companies and public places, etc.), allows us to optimally define the sanitisation operations necessary and places to be made inaccessible.

The legal basis depends, however, on the type of app and the function that it develops.

The principle of self-determination finds a set of multi-faceted forms.

[45] The gained experience in blockchain technologies also shows how important the element of trust is: if in a public registry a series of data are annotated with a high degree of transparency and in a non-modifiable form, therefore the data processing is made safe and the trust of the participants in the validation process is growing. In this way, blockchain technology ensures the security of digital transaction operations and the legal regulation reduces the level of risks in artificial intelligence.

On one hand, there is the informed consent to the health treatment that facilitates the joint realisation of the patient's right to health protection and to personal freedom.

On the other hand, the informed consent to personal data processing does not necessarily correspond to the purpose of the data subject's health protection, since it might be used for other objectives.

The case of an app to be used for contact tracing does not properly identify the first type of consent, since the issue does not concern coercive health treatments in the strict sense. At most, it concerns a call for detection of parameters and data that are useful for the reconstruction of the clinical status for any voluntary treatment measures aimed at the solution of the health problem.

The same applies to the second type of consent (the privacy consent), which can be terminated upon the assurance that data is managed so that anonymity is ensured and/or on the basis of a legislative act that, inspired by the fulfilment of primary public health purposes, provides measures for the suitable protection of citizens' fundamental rights.

A third type of consent is highly relevant, or better yet, an expression of willingness should be encouraged through incentives for boosting awareness that participation in the prevention and contrast program is right, effective and guaranteed to keep the basic principles of our legal order.

Respect of the intangible legal principles means following the paths of equality, proportionality, temporariness, recognition of protections versus any abuse, identity safeguards, privacy and recognizing the human being's dignity.

In order for the monitoring system results to be acceptable to the public, it is necessary, among others, to screen and make the flow of the collected data impermeable to the public security authority.

A software credibly aiming at supporting the anticipation of the end or weakening of restrictions, thanks to the pandemic containment measures, is not particularly suitable for purposes having a high impact on the personal freedom that would require legal restraints (i.e., other and more guaranteed instruments like the reasoned acts of the judicial authority).

The processing of personal data belonging to particular categories according to the definitions in Art. 9 GDPR *per se* gives rise to problems of compatibility with the constitutional framework; in view of this, further uses for the purposes of the police or for the investigations of crimes or general responsibilities are absolutely not recommended, just because they are of doubtful constitutionality.

At the same time, incentives for the downloading of the app are admissible upon compliance with the standards of reasonableness and proportionality. Therefore, basically, a reasonable and constitutionally lawful incentive cannot have the exercise of the right to freedom as a counterpart.

A correct scaling of the incentives strengthens the voluntary basis and the personalistic principle by providing a valid alternative for the hard path of mandatory participation in the tracing program.

A radical renouncement of fundamental freedoms is not a viable objective, and it should not be sacrificed in the name of a massive assessment of individuals' infection risk.

The humanization of processes is undoubtedly required: it is necessary to convey to the citizens the message that on the other side of the device, there is not merely an algorithmic calculation but a doctor or another health operator in person who is available for dialogue and personal support in their case; at the same time, citizens must be ensured that their sensitive data will be capable of being reidentified only if they test positive for the virus. Unnecessary information (subjective limits) or information no longer required over time (time limits) should be deleted. In any case, care should be taken to prevent individuals other than the health professionals taking care of a patient's clinical path from knowing the patient's identity (subjective limits).